VERBAND DER INTERNETWIRTSCHAFT

1. Auflage 2020

GDPR Playbook

Praxistipps zur Umsetzung der DS-GVO

Vorwort

Liebe Leserinnen und Leser,

mit der Datenschutzgrundverordnung wurde erstmals ein einheitliches Datenschutzrecht für den gesamten EU-Raum geschaffen.

Bis zum 25. Mai 2018 mussten Unternehmen, die personenbezogene Daten von EU-Bürgern erfassen und verarbeiten, ihre Systeme und Prozesse an die neuen Regelungen der Datenschutzgrundverordnung (DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG-neu) anpassen. Gerade kleine und mittelständische Unternehmen hat dies vor große Herausforderungen gestellt. Denn diesen Unternehmen fehlt häufig Personal und Know-how, um den Vorgaben der DSGVO gerecht zu werden.

Aus Ermangelung an Rechtsprechung und Erfahrungswerten zur DSGVO waren viele Unternehmen verunsichert. Zwar wurden im Vorfeld Merkblätter und Orientierungshilfen der einzelnen Aufsichtsbehörden veröffentlicht. Allerdings besteht teilweise selbst bis zum heutigen Zeitpunkt keine Einigkeit unter den einzelnen Aufsichtsbehörden im Hinblick auf die Umsetzung datenschutzrechtlicher Vorgaben.

Viele Unternehmen wissen daher nach wie vor nicht, wie bestimmte Vorgaben der DSGVO umzusetzen sind. Dies betrifft z.B. die Frage, ob in bestimmten Fällen Einwilligungen eingeholt werden müssen oder ob die Verarbeitung auf ein berechtigtes Interesse gestützt werden kann.

Unser GDPR Playbook soll Ihnen dabei helfen, diese Unsicherheiten abzubauen. Sie finden darin Anregungen und Hilfestellungen, wie Sie in Zukunft weiterhin rechtskonform personenbezogene Daten verarbeiten können. Dabei haben wir uns speziell auf die Interessengebiete unserer Mitgliedsunternehmen fokussiert. Behandelt werden

datenschutzrechtliche Themen aus den Bereichen Cloud, E-Mail-Marketing, Onlinemarketing, Konzerndatenschutz und Blockchain samt Praxisbeispielen und konkreten Hilfestellungen. Im vorliegenden GDPR Playbook haben wir das gebündelte Expertenwissen aller Beiträge unserer Whitepaper-Reihe „Datenschutz und DSGVO" für Sie zusammengestellt. An dieser Stelle ein herzliches Dankeschön an die Juristinnen und Juristen und weiteren Know-how-Träger, die uns als Gastautoren bei der Realisierung unterstützt haben, und ihr Expertenwissen zu unterschiedlichen Teilaspekten der DSGVO und deren Umsetzung verständlich und praxisnah beleuchten.

Viel Spaß bei der Lektüre!

Mit freundlichen Grüßen

Clarissa Benner, LL.M.
Rechtsanwältin (Syndikusrechtsanwältin)

Inhalt

Autoren

Matthias Bendixen
Rechtsanwalt
Rickert Rechtsanwaltsgesellschaft mbH
www.rickert.net

Klaus M. Brisch, LL.M.
Partner, Global Head of Technology
DWF Germany Rechtsanwaltsgesellschaft mbH
www.dwf.law

Kirstin Dauber
Ass.iur.
Rickert Rechtsanwaltsgesellschaft mbH
www.rickert.net

Dr. Jens Eckhardt
Rechtsanwalt
Fachanwalt für Informationstechnologierecht
Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV)
Derra, Meyer & Partner, www.derra.eu

Eva Focken
Rechtsanwältin
Fieldfisher (Gemany) LLP.
www.fieldfisher.com

Sibel Kocatepe, LL.M.
Wissenschaftliche Mitarbeiterin
WILDE BEUGER SOLMECKE Rechtsanwälte
www.wbs-law.de

Jan Philip Lutterbach
Rechtsanwalt
Rickert Rechtsanwaltsgesellschaft mbH
www.rickert.net

Christian Schmoll
Rechtsanwalt, Fachanwalt IT-Recht
g3s Rechtsanwälte, www.g3s.legal
CIPP/E, CIPM
FIP, Datenschutzbeauftragter, www.dp.institute

Christian Solmecke, LL.M.
Rechtsanwalt und Partner
WILDE BEUGER SOLMECKE Rechtsanwälte
www.wbs-law.de

Nico Winter, LL.M.
Associate
DWF Germany Rechtsanwaltsgesellschaft mbH
www.dwf.law

GDPR Playbook

Praxisorientierte Umsetzung von Informationspflichten

Christian Schmoll

Die Informationspflichten der DSGVO stellen die Unternehmen vor große Herausforderungen. Eine allzu eng am Gesetzeswortlaut orientierte Umsetzung führt dabei oft zu wenig praktikablen Ansätzen und eher zu weniger als zu mehr Transparenz in der Datenverarbeitung.

In diesem Beitrag werden die Anforderungen der DSGVO an die Information der Betroffenen dargestellt und anschließend zahlreiche Tipps für eine praxisorientierte Umsetzung gegeben.

1. TRANSPARENZ

Wer weiß was wann und warum über mich?

Transparenz ist eines der wesentlichen Grundprinzipien des Datenschutzes. Jedermann soll immer darüber informiert werden, welche Daten zu seiner Person für welche Zwecke erhoben, verarbeitet und gespeichert werden. Der Grundgedanke dabei ist, dass ich mein Recht auf informationelle Selbstbestimmung nicht wirksam ausüben kann, wenn ich nicht weiß, wer was wann und warum über mich weiß.

Transparente Datenverarbeitung

Die Datenschutzgrundverordnung (DSGVO) sieht dementsprechend umfangreiche Verpflichtungen zu transparenter Datenverarbeitung vor. Der Verantwortliche muss den Betroffenen zum einen bereits bei Erhebung der Daten darüber informieren, welche Daten er zu welchem Zweck verarbeitet (die sogenannten „Informationspflichten"). Zum anderen sieht die DSGVO auch das Recht vor, jederzeit Auskunft darüber zu erhalten, welche Daten ein Verantwortlicher über mich verarbeitet und speichert und diese unter anderem auch berichtigen oder löschen zu lassen (die sogenannten „Betroffenenrechte").

Die Informationspflichten sind einer der wenigen Bereiche, bei denen die DSGVO in den Unternehmen tatsächlich zu erheblichen zusätzlichen Anforderungen geführt hat. Die Umsetzung der Informationspflichten dürfte die Aufgabe sein, die in den

Unternehmen den meisten Aufwand und die meisten Kopfschmerzen verursacht.

Informations-Overkill

Bei der Umsetzung der rigiden gesetzlichen Vorgaben zu den Informationspflichten knirscht es zwischen Theorie und Praxis oft recht heftig. Eine buchstabengetreue Umsetzung der Informationspflichten führt in der Praxis oft zu wenig sinnvollen und formalistischen Lösungen.

Die Betroffenen werden an jeder Ecke mit ausufernden Datenschutzinformationen im schlimmsten Juristenjargon zugeschüttet, die nicht zu der erwünschten Transparenz der Datenverarbeitung führen, sondern genau zum Gegenteil - der Overkill an Datenschutzinformationen führt dazu, dass die Betroffenen diese ausblenden und überhaupt nicht mehr wahrnehmen.

Es wird von den Betroffenen sicher nicht als begrüßenswerte Stärkung ihres Rechtes auf informationelle Selbstbestimmung wahrgenommen, wenn beispielsweise der Handwerker ihnen am Telefon vor einer Terminvereinbarung am Telefon erst einmal 10 Minuten seine Datenschutzerklärung vorlesen muss. Aus genau solchen Datenschutz-Exzessen resultiert die vielfach geäußerte Kritik am „Bürokratiemonster DSGVO".

Klare und einfache Sprache

Verständlich und in klarer und einfacher Sprache sollen die Informationen laut DSGVO erfolgen. In der Praxis sieht das oft ganz anders aus. Eine Analyse der Bayerischen Rundfunks zeigt plastisch, dass die untersuchten Datenschutzerklärungen der meistgenutzten Internetdienste durch die Bank sprachlich deutlich anspruchsvoller sind als „Der Tod in Venedig" von Thomas Mann, ein Klassiker der deutschen Literatur, der aber sicherlich nicht aufgrund seiner klaren und einfachen Sprache geschätzt wird.

Neben der sprachlichen Komplexität der Datenschutzerklärungen macht auch die schiere Länge sie größtenteils ungenießbar. Den Vogel schießt in der Analyse des Bayerischen Rundfunks die Datenschutzerklärung des Onlinehändlers Zalando ab, mit der sich der Betroffene mehr als 90 Minuten befassen darf, wenn er sie einmal von vorne bis hinten durchlesen möchte.

Hier sind praxisorientierte Lösungen gefragt, die tatsächlich zu mehr Transparenz in der Datenverarbeitung führen und die sich gleichzeitig auch im Alltag praxisorientiert umsetzen lassen, ohne zu Kopfschütteln und Unverständnis bei den Betroffenen zu führen.

2. WIE, WANN UND WO SIND DIE INFORMATIONEN ZU ERTEILEN?

Die Informationen sind gemäß Art. 12 DSGVO in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Es sollte also zumindest der Versuch unternommen werden, die Datenschutzerklärung nicht wie eine juristische Doktorarbeit klingen zu lassen.

Zweistufige Informationen

Die zu erteilenden Informationen sind fast immer ziemlich umfangreich. Es bietet sich dabei an, mit einem zweistufigen Ansatz zu arbeiten:

- **Auf einer ersten Stufe**, im unmittelbaren Umfeld der Datenerhebung, werden kurz und prägnant nur die wirklich wesentlichen Informationen zu der beabsichtigten Datenverarbeitung dargestellt (Basisinformationen)
- **Auf einer zweiten Stufe**, im Regelfall in der Datenschutzerklärung auf der Webseite des Verantwortlichen, folgen dann die ausführlichen Informationen, beispielsweise zu den Betroffenenrechten, gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten und so weiter

Am Beispiel einer Gewinnspielpostkarte sähe das wie folgt aus:

Auf der ersten Stufe, direkt auf der Postkarte, werden kurz und übersichtlich folgende Basisinformationen mitgeteilt:

- Wer erhebt die Daten (Verantwortlicher)
- Welche Daten werden erhoben (so das nicht ohnehin offensichtlich ist, was bei einer Gewinnspielpostkarte, in der ich lediglich meinen Namen und meine Kontaktdaten eintragen kann, der Fall sein dürfte)
- Wozu werden die Daten erhoben (soweit das nicht auch ohnehin offensichtlich ist – was bei einer Gewinnspielpostkarte ebenfalls der Fall sein dürfte, so die Daten nicht über die Teilnahme am Gewinnspiel hinaus für Werbemaßnahmen verarbeitet werden sollen)
- Auf welcher Rechtsgrundlage werden die Daten erhoben

Für alle weiteren Informationen auf einer zweiten Stufe, beispielsweise über die beabsichtigte Dauer der Speicherung und zu den Betroffenenrechten, wird auf eine ausführliche Datenschutzerklärung auf der Webseite des Verantwortlichen verwiesen.

Auf dieser ersten Stufe sollten dabei zumindest die Informationen erteilt werden, die für die Entscheidung des Betroffenen, seine Daten preiszugeben oder eben nicht, von wesentlicher Bedeutung sind. Alles, womit der Betroffene im jeweiligen Kontext nicht rechnet und nicht rechnen muss, was also aus Datenschutzsicht ein Stolperstein sein könnte, muss auf der ersten Stufe klar und deutlich auf den Tisch gelegt werden. Auf der zweiten Stufe, in den nachgelagerten ausführlichen Datenschutzinformationen auf der Webseite, dürfen sich keine Überraschungen mehr verstecken.

Dieser zweistufige Ansatz ermöglicht es, den Informationsverpflichtungen der DSGVO pragmatisch und effizient nachzukommen. Gleichzeitig erhöht diese Herangehensweise auch die Wahrscheinlichkeit, dass die Betroffenen zumindest die wesentlichen Datenschutzinformationen zur Kenntnis nehmen. Das „weniger" auf der ersten Stufe führt hier insgesamt eindeutig zu einem „mehr" an Transparenz.

Medienbruch bzw. Linklösung

Bei der zweistufigen Information ist auch ein „Medienbruch" zulässig. Die ausführlicheren Informationen der zweiten Stufe können beispielsweise auf der Webseite des Verantwortlichen zur Verfügung gestellt werden oder es kann ein Informationsschreiben zur Verfügung gestellt werden, das der Betroffene beispielsweise an der Kasse einsehen oder abholen kann oder das ihm bei Bedarf postalisch zugesandt wird.

Im Beispiel der Gewinnspielpostkarte würde dann, nach den wesentlichen Basisinformationen der ersten Stufe, für die ausführlichen Informationen der zweiten Stufe auf die Datenschutzerklärung auf der Webseite verwiesen.

Diese sogenannte „Linklösung" (manchmal neudeutsch auch als „layered approach" bezeichnet) ist von den meisten Aufsichtsbehörden zwischenzeitlich ausdrücklich anerkannt worden und wird auch im Working Paper 260 der Artikel-29-Datenschutzgruppe[1] („Leitlinien für Transparenz")[2] vorgeschlagen.

Bildsymbole

Es kann dabei auch mit Bildsymbolen gearbeitet werden, um einen Überblick über die Datenverarbeitung zu vermitteln. Die Verwendung solcher Bildsymbole ist eine hervorragende Möglichkeit, um die wesentlichen Informationen der ersten Stufe kurz und prägnant zu übermitteln.

[1] Die Artikel-29-Datenschutzgruppe war ein unabhängiges Beratungsgremium der EU-Kommission, bestehend aus Vertretern der nationalen Datenschutzaufsichtsbehörden und der EU-Kommission. Sie wurde mit der DSGVO vom Europäischen Datenschutzausschuss abgelöst.

[2] https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp260rev01_de.pdf

Die DSGVO sieht dabei auch die Möglichkeit vor, dass die Europäische Kommission standardisierte Bildsymbole vorgibt, die dann einheitlich verwendet werden können. Solche standardisierten Bildsymbole wären äußerst begrüßenswert und würden die Informationsvermittlung erheblich erleichtern, wurden jedoch von der Europäischen Kommission bisher leider noch nicht vorgegeben.

Kinder

Richten sich die Datenschutzinformationen auch oder insbesondere an Kinder, sind sie kindgerecht zu verfassen, also in einer so klaren und einfachen Sprache, dass ein Kind sie verstehen kann.

Sprache

In welcher Sprache bzw. welchen Sprachen die Datenschutzinformationen zur Verfügung gestellt werden müssen, hängt davon ab, an welche Zielgruppe sich das jeweilige Angebot richtet.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) führt in einer Auslegungshilfe[3] aus, dass ein Onlineshop, der in verschiedenen europäischen Sprachen angeboten wird, auch die Datenschutzerklärung in den verschiedenen Landessprachen vorhalten sollte. Wenn ein Onlineshop, der sich an Kunden in ganz Europa wendet, einheitlich nur auf Englisch angeboten wird, kann man nach Ansicht des BayLDA davon ausgehen, dass ein Nutzer, der sprachlich dazu in der Lage ist, den Bestellvorgang im Onlineshop auf Englisch durchzuführen, auch eine englischsprachige Datenschutzerklärung verstehen kann. Eine Übersetzung ist dann nicht zwingend erforderlich.

Erreichbarkeit

Die Datenschutzinformationen müssen leicht zugänglich sein. Für eine Webseite bedeutet das, dass sie nicht nur auf der Startseite verlinkt werden sollten, sondern von jeder Unterseite aus erreichbar sein müssen. Sie sollten zudem stets über einen eindeutigen Link mit der Bezeichnung „Datenschutz" oder „Datenschutzerklärung"

[3] https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Informationspflichten_Sprache.pdf

oder ähnlichem erreichbar sein. Es ist nicht ausreichend, die Datenschutzinformationen beispielsweise unter dem Link zum Impressum zur Verfügung zu stellen.

Bei einer App sollten die Datenschutzinformationen schon direkt im App-Store vor der Installation abrufbar sein und nicht erst, wenn die App bereits installiert wurde und beispielsweise alle Kontaktdaten aus dem Telefonbuch auf den Server das Anbieters hochgeladen hat.

Der Hinweis auf Videoüberwachung sollte überall dort, wo ich den Bereich, der überwacht wird, betreten kann, gut sichtbar angebracht werden.

All-In-One-Datenschutzerklärung

Es muss nicht für jede einzelne Datenerhebung und für jeden einzelnen Datenverarbeitungsvorgang eine separate spezifische Datenschutzerklärung zur Verfügung gestellt werden. Es bietet sich vielmehr an, eine umfassende zentrale Datenschutzerklärung „All-In-One" auf der Webseite zur Verfügung zu stellen, in der die verschiedenen Datenerhebungen und Verarbeitungsvorgänge im Unternehmen im Detail dargestellt werden. Gerade wenn man für die Datenschutzinformationen einen zweistufigen Ansatz verfolgt und nach den Basisinformationen auf der ersten Stufe auf die ausführlichen Informationen der zweiten Stufe verweist, können und sollten die verschiedenen Datenerhebungen und Verarbeitungsvorgänge übersichtlich gegliedert in einer zentralen Datenschutzerklärung auf der Webseite zusammengefasst werden.

Es darf sich bei der Datenschutzerklärung dann aber nicht um einen nichtssagenden generischen „One-Size-Fits-All"-Text handeln, sondern es müssen sauber getrennt und übersichtlich strukturiert die verschiedenen Bereiche bzw. Betroffenengruppen dargestellt werden.

Beispiel:
Auf dem Tresen eines Handwerksbetriebes steht ein Schild *„Wir, die XYZ GmbH, erheben Ihre Daten ausschließlich zur Erfüllung des Vertrages. Ausführliche Informationen zur Datenverarbeitung und zu Ihren Rechten finden Sie unter www.xyz.de/datenschutz"*. An der Eingangstür klebt zudem ein Hinweis auf Videoüberwachung (mit Zweck/Rechtsgrundlage, Speicherdauer, verantwortliche Stelle und ebenfalls wieder einem Verweis auf www.xyz.de/datenschutz). In der Datenschutzerklärung unter www.xyz.de/datenschutz finden sich dann, sauber getrennt und strukturiert, Informationen zur Datenverarbeitung (1.) beim Besuch der Webseite; (2.) bei Vertragserfüllung als Kunde; (3.) im Rahmen der Videoüberwachung; (4.) bei Stellenbewerbungen und so weiter.

In eine Information muss nicht eingewilligt werden

Sinn und Zweck der Datenschutzinformationen ist es, den Betroffenen darüber zu informieren, welche Daten von wem zu welchen Zwecken verarbeitet werden. Diese Information muss dem Betroffenen zur Verfügung gestellt werden, sie muss jedoch vom Betroffenen nicht bestätigt werden und der Betroffene muss auch nicht ausdrücklich einwilligen.

So ist es beispielsweise, auch wenn man es in vielen Onlineshops auch größerer Anbieter allenthalben sieht, definitiv nicht erforderlich, dass im Rahmen des Kaufvorgangs die Datenschutzerklärung ausdrücklich akzeptiert wird bzw. dass in die Datenschutzerklärung „eingewilligt" wird. Es kann rechtlich sogar äußerst problematisch sein, eine Einwilligung hineinzuformulieren, wo keine Einwilligung erforderlich ist. Bei einer Änderung der Datenschutzinformationen kann man in diesem Fall unter Umständen vor dem durchaus unangenehmen Problem stehen, eine erneute Einwilligung in die neue Datenschutzerklärung einholen zu müssen.

Im Rahmen der Rechenschaftspflicht kann es sinnvoll sein, sich die Erteilung der Informationen bestätigen zu lassen (ausführlicher dazu weiter unten). Es muss dabei

jedoch sauber formuliert werden, dass es sich eben nicht um eine Einwilligung handelt, sondern dass lediglich bestätigt wird, dass die Datenschutzinformationen erteilt wurden.

> **Beispiel für das Wording beim Checkout im Onlineshop:**
> *[ ] Es gelten die AGB und die Datenschutzerklärung von XYZ, von denen ich Kenntnis genommen habe.*

Wann sind die Datenschutzinformationen zu erteilen?

Wenn Daten direkt beim Betroffenen erhoben werden, müssen die Informationen unmittelbar bei der Erhebung der Daten zur Verfügung gestellt werden (Art. 13 Abs. 1 DSGVO). Eine nachträgliche Information ist bei der sogenannten Direkterhebung nicht zulässig.

Eine nachträgliche Information von Betroffenen, deren Daten vor Inkrafttreten der DSGVO erhoben wurden, ist und war dementsprechend auch nicht erforderlich.

Wenn die Daten eines Betroffenen nicht direkt von dem Betroffenen zur Verfügung gestellt wurden, sondern wenn der Verantwortliche sie aus anderen Quellen erhoben hat (sogenannte Dritterhebung), muss der Betroffene innerhalb einer „angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats" informiert werden (Art. 14 Abs. 3 DSGVO). Die Monatsfrist ist dabei nicht pauschal als Regeldauer anzusetzen, sondern als absolute Maximalfrist, wenn eine frühere Information sich unter Berücksichtigung der spezifischen Umstände nicht oder nur mit unangemessenem Aufwand bewerkstelligen lässt.

Wenn Daten bei einem Dritten erhoben wurden, um mit dem Betroffenen zu kommunizieren, müssen die Datenschutzinformationen spätestens zum Zeitpunkt der ersten Mitteilung an den Betroffenen erteilt werden.

Wenn man also beispielsweise bei einem Adressbroker Postadressen erwirbt, um postalische Werbung zu versenden, müssen die erforderlichen Datenschutzinformationen zumindest im ersten Anschreiben enthalten sein. Auch hier ist natürlich wieder der zweistufige Ansatz bzw. layered approach zulässig. Im Werbebrief können dabei kurz und prägnant lediglich die Basisinformationen erteilt werden. Im konkreten Fall sollten also mindestens der Verantwortliche, die Herkunft der Daten (Adresshändler), der Zweck der Verarbeitung, die Rechtsgrundlage der Verarbeitung (das überwiegende berechtigte Interesse) und das Recht auf Widerspruch (sowohl gegenüber dem Verantwortlichen wie auch gegenüber dem Adresshändler) dargestellt werden. Für alle weiteren Informationen kann dann auf die Datenschutzerklärung auf der Webseite verwiesen werden.

Rechenschaftspflicht

Die DSGVO folgt dem Ansatz, dass man stets umfassend nachweisen können muss, dass man die Anforderungen der DSGVO eingehalten hat. Man ist also quasi schuldig bis zum Beweis der Unschuld. Um dieser sogenannten Rechenschaftspflicht nachzukommen, muss im Unternehmen umfangreich dokumentiert werden.

Bezogen auf die Informationspflichten und das Transparenzgebot bedeutet das, dass der Verantwortliche immer nachweisen können muss, dass die nach Art. 13 und 14 DSGVO erforderlichen Informationen ordnungsgemäß erteilt wurden.

Es ist darauf hinzuweisen, dass nicht nachgewiesen werden muss, dass der Betroffene die Informationen auch tatsächlich zur Kenntnis genommen hat. Der Verantwortliche muss die Informationen lediglich erteilen, ob der Betroffene sie dann auch tatsächlich liest ist nicht mehr Sache des Verantwortlichen.

Der Nachweis der ordnungsgemäßen Zurverfügungstellung der Informationen kann zum einen erbracht werden, indem man sich von jedem Betroffenen immer im Einzelfall bestätigen lässt, dass ihm die Informationen zur Verfügung gestellt wurden. Diese Herangehensweise kann man beispielsweise im Onlineshop wählen, indem man sich im Checkout-Prozess mittels Checkbox bestätigen lässt, dass die

Datenschutzerklärung zur Verfügung gestellt und zur Kenntnis genommen wurde (auch wenn die tatsächliche Kenntnisnahme nicht zwingend erforderlich ist).

In den meisten Fällen dürfte die ausdrückliche Bestätigung der Zurverfügungstellung jedoch wenig praktikabel sein und zu ausufernder Bürokratie führen. Es bietet sich daher an, den Prozess der Informationserteilung zu dokumentieren – also das „wie" der Information. Es kann mittels einer solchen Prozessdokumentation dann nachgewiesen werden, dass strukturell sichergestellt ist, dass jeder Betroffene informiert wird. Zusätzlich muss auch noch das „was" detailliert dokumentiert werden, also welche Informationen zu welchem Zeitpunkt erteilt wurden. Hier ist eine saubere Versionskontrolle erforderlich, um stets zweifelsfrei darlegen zu können, welche Version der Datenschutzerklärung zu welchem Zeitpunkt auf der Webseite zur Verfügung gestellt wurde.

Eine solche Prozessdokumentation im Rahmen eines umfassenden Datenschutzmanagementsystems (DSMS) erfüllt dann ebenfalls die Anforderungen der Rechenschaftspflicht.

Ausnahmen von der Informationspflicht

Bei der Direkterhebung beim Betroffenen kann auf die Information des Betroffenen nur verzichtet werden, wenn der Betroffene bereits über die Information verfügt. Es ist dabei nicht zwingend erforderlich, dass er zuvor bereits vom Verantwortlichen ausdrücklich informiert wurde. Auch wenn beispielsweise der Verantwortliche und der Zweck der Datenverarbeitung ganz offensichtlich sind, ist eine formelle Information zu diesen Punkten entbehrlich.

> **Beispiel:**
> *Ruft ein Betroffener bei einem Handwerker an, um einen Termin zu vereinbaren, verfügt der Betroffene ganz offensichtlich schon über die Informationen zum Verantwortlichen. Er hat den Handwerker ja schließlich angerufen. Auch der Zweck der im Rahmen der Terminvereinbarung am Telefon erhobenen Daten ist für den Betroffenen offensichtlich. Eine ausdrückliche nochmalige Information*

zu diesen ganz offensichtlichen Punkten erübrigt sich. Nach Ansicht des BayLDA[4] ist es in diesem Falle ausreichend, wenn die sonstigen Informationen im Rahmen einer Auftragsbestätigung per E-Mail mittels eines Links auf die Datenschutzerklärung auf der Webseite oder auch erst bei Wahrnehmung des Termins bereitgestellt werden. Dies gilt natürlich nicht, wenn die Daten zu sonstigen, unter Umständen für den Betroffenen unerwarteten Zwecken verwendet werden sollen. Beabsichtigt der Handwerker beispielsweise, die Mobilfunknummer des Betroffenen zur Kommunikation via WhatsApp zu verwenden, so ist der Betroffene über diesen Umstand unbedingt zu informieren.

Auch wenn der Betroffene bereits informiert wurde und zu einem späteren Zeitpunkt lediglich zusätzliche Daten erhoben werden, sich aber am Zweck der Datenverarbeitung und auch an den sonstigen Parametern nichts geändert hat, ist eine nochmalige Information nicht erforderlich und würde eine überflüssige Förmelei darstellen.

Bei der Dritterhebung, wenn Daten also nicht direkt beim Betroffenen erhoben werden, sondern aus anderen Quellen stammen, kann auf die Information des Betroffenen verzichtet werden, wenn die Erteilung der Information unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

Beispiel:
Im Bereich des Social Media Listening, bei dem öffentlich zugängliche Daten aus den sozialen Netzwerken (Facebook, Twitter, Instagram etc.) beispielsweise für Zwecke der Marktforschung erhoben werden, ist eine direkte Information der potentiell betroffenen Milliarden Nutzer der sozialen Netzwerke nicht oder nur mit unverhältnismäßigem Aufwand möglich. So sich die Datenerhebung beim Social Media Listening anhand des konkreten Anwendungsfalls auf ein berechtigtes Interesse des Verantwortlichen stützen lässt, kann die Information sämtlicher Betroffenen unter Umständen alleine schon aufgrund der Masse an potentiell Betroffenen entbehrlich sein.

[4] https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_InformationspflichtenTelefon.pdf

Auch bei Daten, die dem Berufsgeheimnis unterliegen, kann eine Information unterbleiben. Werden beispielsweise personenbezogene Daten an einen Rechtsanwalt weitergereicht, um eine Klage vorzubereiten, müssen weder der Mandant, der die Daten an den Rechtsanwalt übermittelt, noch der Rechtsanwalt den Betroffenen und potentiellen Beklagten informieren.

Folgen eines Verstoßes

Bei einem Verstoß gegen die Informationspflichten droht ein Bußgeld – und die möglichen Bußgelder der DSGVO sind potentiell erheblich. Die transparente Datenverarbeitung und ordnungsgemäße Erfüllung der Informationspflichten wird von der DSGVO als wesentlich für die Freiheitsrechte der Betroffenen angesehen und die DSGVO sanktioniert Verstöße daher mit dem höchstmöglichen Bußgeldrahmen, nämlich mit bis zu 20 Millionen Euro oder mit 4% des globalen Jahresumsatzes des Unternehmens bzw. der gesamten Unternehmensgruppe.

3. ÜBER WAS MUSS INFORMIERT WERDEN?

Nach der ausführlichen Übersicht über das „wie" der Informationserteilung nachfolgend eine kurze Übersicht über den erforderlichen Inhalt der Datenschutzinformationen.

a) Verantwortlicher

Der vollständige Name des Verantwortlichen, seine ladungsfähige Postanschrift und eine E-Mail-Adresse müssen angegeben werden. Wenn der Verantwortliche nicht in der EU niedergelassen ist, müssen auch sein Vertreter in der EU (gem. Art. 27 DSGVO) und dessen Kontaktdaten angegeben werden.

b) Datenschutzbeauftragter

Wenn ein Datenschutzbeauftragter bestellt ist, unabhängig davon ob auf Basis von Art. 37 DSGVO oder von § 38 BDSG, müssen dessen Kontaktdaten angegeben

werden. wobei eine generische E-Mail-Adresse wie datenschutz@xyz.de ausreicht. Die Nennung des Namens des Datenschutzbeauftragten ist nicht erforderlich.

c) Verarbeitungszwecke und Rechtsgrundlage

Die Zwecke der Datenverarbeitung und die jeweilige Rechtsgrundlage müssen benannt werden. Die Daten dürfen, dem Grundsatz der Zweckbindung folgend, nur für hier angegeben Zwecke verarbeitet werden. Eine nachträgliche Zweckänderung ist schwierig und aufwändig. Daher sollte bei der Definition der Zwecke sorgfältig vorgegangen werden. Eine zu enge Zweckbestimmung kann sich zu einem späteren Zeitpunkt schnell als unnötiges Korsett erweisen. Die Zweckbestimmung darf andererseits auch kein völlig nichtssagender generischer Allgemeinplatz sein.

Wenn als Rechtsgrundlage das überwiegende berechtigte Interesse des Verantwortlichen (Art. 6 Abs. 1 lit. f) DSGVO) dient, ist auch das berechtigte Interesse konkret anzugeben. Ein schematischer Verweis auf ein berechtigtes Interesse alleine ist hier nicht ausreichend.

> **Beispiel für ein Kontaktformular auf der Webseite:**
> *Wir verarbeiten die von Ihnen in das Kontaktformular eingegebenen Daten und ergänzend Ihre IP-Adresse und den Zeitpunkt der Kontaktaufnahme auf Basis eines berechtigten Interesses gem. Art. 6 Abs. 1 lit. f) DSGVO. Wir möchten den Besuchern unserer Webseite durch die Bereitstellung des Kontaktformulars eine einfache und direkte Kontaktaufnahme mit uns ermöglichen.*

d) Empfänger

Es muss auch über „Empfänger oder Kategorien von Empfängern" der Daten informiert werden. „Empfänger" sind dabei nicht nur Dritte, so dass neben anderen Verantwortlichen auch gegebenenfalls gemeinsam Verantwortliche und vor allem auch Auftragsverarbeiter zu benennen sind.

Ob in jedem Fall die Angabe der bloßen „Kategorien von Empfängern" ausreichend ist oder ob man, wenn die konkreten Empfänger bekannt sind, diese auch konkret im Einzelfall zu benennen hat und nur auf Kategorien ausweichen darf, wenn die Empfänger konkret noch nicht bekannt sind, ist umstritten.

Die Idee der Informationspflichten ist es, es dem Betroffenen zu ermöglichen, sich ein umfassendes Bild von der beabsichtigten Datenverarbeitung zu machen. Dafür kann oftmals die Angabe von Kategorien von Empfängern ausreichend sein. Es wird dem Betroffenen beispielsweise meist herzlich egal sein, an welche Bank seine Daten für die Zahlungsabwicklung weitergegeben werden oder auf den Servern welches Webhosters die Webseite liegt (wenn seine Daten die EU verlassen, ist er darüber ohnehin separat aufzuklären, siehe weiter unten). Die Angabe von Kategorien kann das Transparenzbedürfnis des Betroffenen im Regelfall ausreichend befriedigen, so sich die Kategorien nicht in nichtssagenden Allgemeinplätzen erschöpfen. Die Angabe der Kategorie „Auftragsverarbeiter" ohne nähere Präzisierung dürfte beispielsweise nicht ausreichend sein. Eine konkrete Angabe der Empfänger kann hinsichtlich einer transparenten Datenverarbeitung unter Umständen aus sogar kontraproduktiv sein (Stichwort „Informations-Overkill"), wenn dem Betroffenen beispielsweise eine lange Liste von Empfängern mit identischer Funktion präsentiert wird (beispielsweise Versanddienstleister bei einem Onlineshop). Auch wenn der Betroffene alle naslang über Änderungen von Empfängern informiert werden muss, beispielsweise bei einem regelmäßigen Austausch von Auftragsverarbeitern einer bestimmten Kategorie, ist es unter Transparenzaspekten zielführender, mit der Angabe konkreter Kategorien zu arbeiten.

e) Übermittlung in Drittländer

Auch über eine beabsichtigte Übermittlung in „unsichere" Drittländer außerhalb der EU bzw. ohne Angemessenheitsbeschuss der EU-Kommission, ist zu informieren. Zudem ist darüber zu informieren, mit welchen Mitteln ein angemessenes Datenschutzniveau beim Empfänger sichergestellt wird. Es wird sich dabei meist um das EU - US Privacy Shield oder die EU-Standardvertragsklauseln handeln. Es ist dann auch noch darauf hinzuweisen, wie der Betroffene detaillierte Informationen

dazu erhalten kann, beispielsweise durch einen Link auf die Privacy Shield-Zertifizierung (https://www.privacyshield.gov/list) oder indem gegebenenfalls die Zurverfügungstellung einer Kopie der EU-Standardvertragsklauseln auf Anfrage angeboten wird.

f) Dauer der Speicherung

Die Dauer der Speicherung der Daten ist so konkret wie möglich anzugeben. Wenn eine konkrete Zeitspanne noch nicht benannt werden kann, beispielsweise weil initial noch nicht klar ist, wie lange die Daten für den konkreten Zweck tatsächlich erforderlich sind, sind zumindest die Kriterien für die Festlegung der Speicherdauer zu definieren.

> **Beispiel:**
> *Wir löschen Ihre Daten, die im Rahmen Ihrer Anfrage erhoben wurden, sobald diese für den Zweck der Erhebung nicht mehr erforderlich sind, d.h. wenn der konkrete Sachverhalt, der Ihrer Anfrage zu Grunde liegt, abgeschlossen ist. Sofern es im Zusammenhang mit Ihrer Anfrage zu einem Vertragsverhältnis gekommen ist, unterliegen wir den gesetzlichen Aufbewahrungsfristen und löschen Ihre Daten nach Ablauf dieser Fristen.*

g) Betroffenenrechte

Es ist über das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung sowie Datenübertragbarkeit hinzuweisen (Art. 15 bis 20 DSGVO). Zu den Betroffenenrechten kann für alle Verarbeitungen einheitlich informiert werden.

> **Beispiel:**
> *Sie haben das Recht, jederzeit Ihre nachfolgend aufgelisteten Betroffenenrechte (gem. Art. 15 bis 20 GDSVO) auszuüben. Bitte kontaktieren Sie uns hierfür unter den oben angegebenen Kontaktdaten des Verantwortlichen oder wenden Sie sich unter den oben angegeben Kontaktdaten an unseren Datenschutzbeauftragten.*

Sie haben folgende Rechte:

- *Auskunft über Ihre bei uns gespeicherten Daten und die Details der Verarbeitung (Art. 15 DSGVO);*
- *Berichtigung unrichtiger personenbezogener Daten (Art. 16 DSGVO);*
- *Löschung Ihrer bei uns gespeicherten Daten (Art. 17 DSGVO);*
- *Einschränkung der Datenverarbeitung (Art. 18 DSGVO);*
- *Datenübertragbarkeit (Art. 20 DSGVO).*

h) Widerspruchsrecht bei berechtigtem Interesse

Wenn die Verarbeitung auf einem berechtigten Interesse beruht, ist der Betroffene über sein Recht auf Widerspruch gegen die Verarbeitung zu informieren.

Das Recht auf Widerspruch besteht grundsätzlich nur, wenn bei dem Betroffenen eine „besondere Situation" vorliegt. Nur bei der Verarbeitung für Direktwerbung kann der Betroffene jederzeit Widerspruch einlegen.

Beispiel:

Soweit wir Ihre Daten, wie in dieser Datenschutzerklärung erläutert, zur Wahrung unserer überwiegenden berechtigten Interessen verarbeiten, können Sie dieser Verarbeitung mit Wirkung für die Zukunft widersprechen. Kontaktieren sie uns dazu bitte unter den oben angegebenen Kontaktdaten.

Dieses Widerspruchsrecht steht ihnen grundsätzlich nur bei Vorliegen von Gründen zu, die sich aus ihrer besonderen Situation ergeben (Art. 21 Abs. 1 DSGVO). Nach Ausübung Ihres Widerspruchsrechts werden wir Ihre personenbezogenen Daten nicht weiter zu diesen Zwecken verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die ihre Interessen, Rechte und Freiheiten überwiegen, oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Erfolgt die Verarbeitung zu Zwecken der Direktwerbung, können Sie Ihr diesbezügliches Widerspruchsrecht jederzeit ausüben (Art. 21 Abs. 2 DSGVO) und wir werden Ihre personenbezogenen Daten dann, unabhängig von den Gründen des Widerspruchs, nicht weiter zu Zwecken der Direktwerbung verarbeitet.

Der Hinweis auf das Widerspruchsrecht sollte gesondert hervorgehoben und von anderen Informationen getrennt erfolgen, beispielsweise abgesetzt von der sonstigen Datenschutzerklärung im Fettdruck.

i) Widerruf der Einwilligung

Eine Einwilligung kann der Betroffene jederzeit widerrufen – und auf dieses Widerrufsrecht ist er auch ausdrücklich zu informieren. Die Information über das Widerrufsrecht sollte dabei nicht nur formelmäßig in der Datenschutzerklärung erfolgen, sondern auch bereits direkt bei der Einholung der Einwilligung (also auf der ersten Stufe).

Beispiel

Einige Datenverarbeitungsvorgänge sind nur mit Ihrer ausdrücklichen Einwilligung möglich. Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Dazu reicht eine formlose Mitteilung per E-Mail an uns unter den oben angegebenen Kontaktdaten. Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

j) Beschwerde bei der Aufsichtsbehörde

Auch über das Recht, sich jederzeit bei einer Datenschutzaufsichtsbehörde beschweren zu können, ist zu informieren. Auch dieser eher formalen Informationspflicht kann wieder problemlos mit einer Standardformulierung nachgekommen werden.

Beispiel:

Ihnen steht des weiteren ein Beschwerderecht bei der zuständigen Daten-

schutzaufsichtsbehörde zu. Eine Liste der Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich finden Sie unter: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

k) Automatisierte Entscheidungsfindung und Profiling

Werden Verfahren der automatisierten Entscheidung oder andere Profiling-Maßnahmen eingesetzt, kann dies erhebliche Auswirkungen für den Betroffenen haben. Über den Einsatz solcher Verfahren ist dementsprechend detailliert zu informieren, einschließlich einer Beschreibung des verwendeten Algorithmus. Es ist auch darüber zu informieren, dass solche Verfahren nicht eingesetzt werden.

Beispiel:

Eine automatisierte Entscheidungsfindung einschließlich eines Profiling wird von uns nicht durchgeführt.

l) Nur bei Direkterhebung: Verpflichtung zur Bereitstellung personenbezogener Daten

Der Verantwortliche muss den Betroffenen darüber informieren, ob die Bereitstellung seiner personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben, für einen Vertragsschluss erforderlich ist oder eine sonstige Verpflichtung besteht und welche Folgen eine Nichtbereitstellung hätte.

Beispiel:

Die Bereitstellung personenbezogener Daten ist weder gesetzlich noch vertraglich vorgeschrieben, Sie sind auch nicht verpflichtet, personenbezogene Daten bereitzustellen, allerdings ist die Angabe personenbezogener Informationen für einen Vertragsabschluss insofern erforderlich, als bestimmte Angaben zwingend erforderlich sind, um einen Vertrag abschließen (und durchführen) zu können.

m) Nur bei Dritterhebung: Kategorien und Quelle der personenbezogenen Daten

Werden personenbezogene Daten nicht beim Betroffenen direkt erhoben, muss

der Betroffene über die verarbeiteten Datenkategorien und über die Herkunft bzw. Quelle der Daten informiert werden und auch darüber, ob es sich dabei um eine öffentlich zugängliche Quelle handelt.

4. VORLAGEN, BEISPIELE UND FAQS

Es gibt keine allgemeingültigen Muster, weil jede Datenverarbeitung spezifisch beschrieben werden muss und jede Datenverarbeitung unterschiedliche Funktionen hat. Es gibt jedoch zahllose hervorragende Vorlagen, Beispiele und Generatoren, die als Basis für die Erstellung eigener individueller Datenschutzinformationen dienen können. Einige davon sollen hier erwähnt werden, ohne konkrete Empfehlungen auszusprechen oder einen Anspruch auf Vollständigkeit zu erheben.

a) Webseite

Für die Datenschutzinformationen rund um die Webseite gibt es zahlreiche Generatoren im Internet, bei denen man nach Abarbeitung eines mehr oder weniger umfangreichen Fragenkatalogs eine fertige Datenschutzerklärung für die Webseite erhält, oft auch direkt mit HTML-Code zur direkten Einbindung.

Diese Datenschutzinformationen beziehen sich im Regelfall jedoch nur auf die Datenverarbeitungen rund um die Webseite. Alle sonstigen Informationen der „zweiten Stufe", also beispielsweise zur Datenverarbeitung im Rahmen der Dienstleistungen des Verantwortlichen, zur Nutzung und Speicherung von Kundendaten in einem CRM, zum Umgang mit Bewerberdaten und so weiter sind jeweils individuell zu erstellen und zu ergänzen.

- Das Institut für Informations-, Telekommunikations- und Medienrecht der Uni Münster von Prof. Dr. Thomas Hoeren stellt eine Musterdatenschutzerklärung für Websitebetreiber zur Verfügung: https://www.itm.nrw/lehre/materialien/musterdatenschutzerklaerung/
- Rechtsanwalt Dr. Thomas Schwenke stellt einen für die Privatnutzung kostenlosen Datenschutzgenerator zur Verfügung: https://datenschutz-generator.de

b) Mitarbeiterinformationen

Im Arbeitsverhältnis werden meist große Mengen zum Teil auch sensibler Daten verarbeitet. Zudem gibt es im Bereich des Mitarbeiterdatenschutzes zahlreiche Beschwerden bei den Aufsichtsbehörden und die Aufsichtsbehörden prüfen verstärkt in diesem Bereich.

Daher kommt einer korrekten und umfassenden Information der Mitarbeiter über die Verarbeitung ihrer Daten im Rahmen des Beschäftigungsverhältnisses besondere Bedeutung zu. Neue Mitarbeiter sind zudem auch auf die Vertraulichkeit (früher auf das „Datengeheimnis") zu verpflichten. Beides sollte möglichst im Rahmen einer Datenschutzschulung vor oder unmittelbar bei Aufnahme der Tätigkeit erfolgen. eco stellt seinen Mitgliedsunternehmen hierfür auf Anfrage gerne eine Vorlage zur Verfügung.

c) Eventfotografie

Das Thema „Fotografie und Datenschutz" ist ein weites Feld, auf das hier nicht im Detail eingegangen werden kann. Es lässt sich grundsätzlich sagen, dass Eventfotografie auf Basis eines berechtigten Interesses des Veranstalters nach wie vor zulässig sein kann. Stützt man das Anfertigen der Fotos auf sein berechtigtes Interesse, läuft man nicht Gefahr, dass die Betroffenen ihre zuvor erteilte Einwilligung widerrufen und man gezwungen ist, den widerrufenden Abgebildeten auf Fotos zu suchen, um ihn unkenntlich zu machen etc.

Es ist jedoch eine Information der Veranstaltungsteilnehmer erforderlich. Die Veranstaltungsteilnehmer sind dabei darüber zu informieren, zu welchem Zweck die Fotos verwendet werden sollen und wo die Fotos wie lange veröffentlicht werden sollen (Print? Webseite? Soziale Medien?). Es ist zudem auf das Widerspruchsrecht der Veranstaltungsteilnehmer hinzuweisen.

Ausführliche Informationen zur Erstellung und Veröffentlichung von Fotos hat das Bayerische Landesamt für Datenschutzaufsicht hier veröffentlicht: https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Bilder_und_Verein.pdf

d) Videoüberwachung

Auf eine (nur in engen Grenzen zulässige) Videoüberwachung durch ein Unternehmen muss auf gut sichtbaren Hinweisschildern hingewiesen werden. Ein Muster für ein solches Hinweisschild mit den wesentlichen Informationen findet sich hier: https://www.lda.bayern.de/media/muster/video_infoblatt.pdf

Die Datenschutzkonferenz hat zudem ein Kurzpapier mit ausführlicheren Informationen zur Videoüberwachung und den entsprechenden Informationspflichten veröffentlicht:
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf

GDPR Playbook

Onlinemarketing unter der DSGVO

– Berechtigte Interessen als Rechtsgrundlage für die Datenverarbeitung zu Werbezwecken

Eva Focken

Eineinhalb Jahre nach dem Inkrafttreten der DSGVO bestehen nach wie vor Unklarheiten darüber, ob und wie Nutzerdaten zur Aussteuerung automatisierter Online-Werbemittel genutzt werden dürfen.

In diesem Beitrag widmen wir uns der Frage, wie es aktuell um die einwilligungsfreie Platzierung von (Tracking-)Cookies nach § 15 Abs. 3 TMG steht, und ob die damit verbundene Datenverarbeitung zum Zwecke der Aussteuerung verhaltensbezogener Online-Werbung auf berechtigte Interessen (Art. 6 Abs. 1 Buchst. f DSGVO) gestützt werden kann.

1. VERHALTENSBEZOGENE WERBUNG UND COOKIES

Das Tracking des Nutzerverhaltens im Netz ist für Unternehmen eine wichtige Informationsquelle, um Online-Werbemittel zielgerichtet und effektiv zu platzieren.

Hierzu wird das Nutzerverhalten analysiert, um Interessen und Vorlieben des Nutzers einzuschätzen. Das Ausspielen von Werbung auf Basis solcher Analysen nennt sich verhaltensbasierte Online-Werbung oder, branchentypisch in Englisch, Behavioral Targeting. Die Methode basiert darauf, dass mittels verschiedener Technologien – oft Cookies – Geräte von Nutzern markiert, ihr Verhalten und Interaktionen im Netz erfasst, analysiert und zum Teil auch als (geräteüber-greifendes) Nutzerprofil zusammengeführt werden. Die gesammelten Informationen können Rückschlüsse auf Produktinteressen, Kaufabsichten, Hobbies, aber auch auf Familienstand oder Einkommen zulassen. Ein wertvolles Knowhow, das es Unternehmen ermöglicht, Werbemittel auf das Verhalten der Internetnutzer effektiv und passgenau auszurichten.

Der Rechtsrahmen für die Einbindung solcher (Tracking-)Cookies war in Deutschland vom sog. „Opt-Out"-Ansatz geprägt (§ 15 Abs. 3 Telemediengesetz – TMG).

Diese Norm erlaubt(e) der deutschen Online-Werbeindustrie unter bestimmten Voraussetzungen (Pseudonymisierungspflicht, Transparenz, Widerspruchsmöglichkeit) Nutzungsdaten zu Werbezwecken ohne Einwilligung zu verwenden.

Auch wenn § 15 Abs. 3 TMG immer noch existiert ist es mittlerweile fraglich, ob sich Unternehmen noch auf ein „Opt-Out" verlassen können. Jüngere Entscheidungen des Europäischen Gerichtshofs lassen es als zumindest sehr zweifelhaft erscheinen, dass es sich bei der Norm um eine richtlinienkonforme Umsetzung des Art. 5 Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikation handelt (Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation in der Fassung vom 25. November 2009 – Richtlinie 2009/136/EG). Denn schon im Jahr 2009 galt im Grundsatz ein „informed opt-in". Eine Widerspruchslösung, wie sie § 15 Abs. 3 TMG vorsieht, käme nach Art. 5 Abs. 3 S. 2 der **Richtlinie** nur noch in Betracht, wenn die Speicherung von Nutzungsdaten für die Leistungserbringung unbedingt erforderlich ist (siehe unten).

Eine endgültige Klärung, wie mit dem § 15 Abs. 3 TMG in Deutschland zukünftig zu verfahren ist, steht allerdings noch aus. Daran hat auch das viel diskutierte planet49-Urteil des Europäischen Gerichtshofs nichts geändert.

§ 15 Abs. 3 TMG und die Verwirrung um das planet49-Urteil des EuGH

Um es vorwegzunehmen: Der Europäische Gerichtshof (EuGH) hat in seinem planet49-Urteil entgegen einiger Veröffentlichungen weder entschieden, dass für das Setzen von Cookies immer eine Einwilligung erforderlich ist, noch welche Rechtsgrundlage(n) für den Einsatz von Cookies Anwendung finden. Musste er auch gar nicht, denn es war nicht Gegenstand des Verfahrens. Der EuGH hatte sich ausschließlich mit konkreten Fragen nach dem „wie" zu befassen, d.h. den Anforderungen an eine wirksame Einwilligung nach Art. 5 Abs. 3 der **Richtlinie** sowie Art. 6 Abs. 1 Buchst. a), 7 DSGVO. Der EuGH stellte im konkreten Fall fest, dass

• vorangekreuzte Check-Boxen keine wirksame Einwilligung gemäß Art. 5 Abs. 3 der **Richtlinie** bzw. Art. 6 Abs. 1 Buchst. a), 7 DSGVO darstellen (s.a. Erwägungsgrund 32 der DSGVO).

• die Anforderungen an eine Einwilligung beim Setzen von Cookies gelten, losgelöst, ob diese Cookies personenbezogene Daten erfassen oder nicht, und

• Nutzer über das Setzen von Cookies, ihre Funktionsweise und Speicherdauer transparent zu informieren sind (Art. 12, 13 DSGVO).

Aus dem planet49-Urteil lässt sich also weder eine allgemeine Cookie-Einwilligungspflicht, noch eine Auseinandersetzung mit der (Fort-)Geltung des § 15 Abs. 3 TMG für die deutsche Werbeindustrie ableiten.

Opt-In oder Opt-Out – Wie geht es jetzt weiter?

Der Ball liegt – zumindest für das planet49-Verfahren – beim zuständigen Bundesgerichtshof (BGH). Dass dieser an der Anwendbarkeit des § 15 Abs. 3 TMG festhalten wird, ist aufgrund der aktuellen Entwicklungen auf europäischer und nationaler Ebene allerdings nicht zu erwarten.

Spannend gestaltet sich in diesem Zusammenhang auch die Folgefrage, auf welche Rechtsgrundlage das Setzen von Cookies in Deutschland sodann zu stützen wäre. Art. 5 Abs. 3 der **Richtlinie** kommt keine unmittelbare Wirkung zu, ein Abschluss des Gesetzgebungsverfahrens um die e-Privacy-Verordnung ist auch noch nicht in Sicht.

Die deutschen Datenschutzbehörden gehen davon aus, dass § 15 Abs. 3 TMG unter der DSGVO nicht mehr anwendbar ist und zielen auf Art. 6 DSGVO. Ein möglicher Ansatz unter der DSGVO wäre, in Anlehnung an Art. 5 Abs. 3 der **Richtlinie** für sog. nicht unbedingt erforderliche Cookies (vgl. Art. 5 Abs. 3 S.1 der **Richtlinie**) sich auf die Einwilligung gemäß Art. 6 Abs. 1 Buchst. a) DSGVO zu stützen, für sog. unbedingt

erforderliche Cookies (vgl. Art. 5 Abs. 3 S. 2 der **Richtlinie**) auf berechtigte Interessen gemäß Art. 6 Abs. 1 Buchst. f) DSGVO.

Da sich der EuGH im planet49-Verfahren zu der Frage der Erforderlichkeit von Cookies nicht äußern musste, wird auch der Maßstab „unbedingt erforderlich" zu diskutieren sein. Neben Cookies, welche für die Bereitstellung der vom Nutzer angefragten Leistung unerlässlich sind (z.B. Warenkorb-Cookies im Webshop oder Cookies, die die Cookie-Einwilligung speichern), deutet die aktuelle Positionierung der französischen Datenschutzbehörde (CNIL) darauf hin, dass zumindest First-Party-Analyse-Cookies unter bestimmten Voraussetzungen als unbedingt erforderlich gelten. Anders fallen hingegen erste Beurteilungen für die Einbindung von Third-Party-Cookies zu Analyse, Werbe- und Profiling-Zwecken aus (vgl. die britische Datenschutzbehörde - ICO).

Auch wenn das Ergebnis abzuwarten ist, wird Unternehmen empfohlen, die weiteren Entscheidungen und Entwicklungen auf nationaler und internationaler Ebene zu beobachten. Dies betrifft neben der ausstehenden BGH-Entscheidung insbesondere die ebenfalls verkündeten Bestrebungen des Bundeswirtschaftsministeriums Änderungen am Telemediengesetz vorzunehmen.

Wer kein Risiko eingehen möchte , sollte seine aktuellen Cookies-Praktiken neben § 15 Abs. 3 TMG am Maßstab des Art. 5 Abs. 3 S. 2 der **Richtlinie** prüfen und im Bedarfsfall eine explizite Cookie-Einwilligung auf der Webseite vorsehen, welche die Anforderungen des EuGH entsprechend berücksichtigt.

Wo immer automatisierte Verarbeitungen von Nutzerdaten „im Hintergrund" laufen, gelten (auch) die Spielregeln der DSGVO

Die Verarbeitung von Cookie-basierten Nutzerdaten zum Zwecke der Aussteuerung verhaltensbezogener Werbung umfasst eine Vielzahl an Datenverarbeitungsvorgängen, z.B.

- die Analyse und Auswertung von Nutzerverhalten,
- die Erstellung (pseudonymer) Nutzerprofile und ggf. die Verknüpfung mit anderen Datensätzen (z.B. Kundenprofil),
- die Aussteuerung von Online-Werbemitteln an ausgewählte Zielgruppen sowie
- die Einschränkung der Ausspielung von Online-Werbemitteln an einzelne Nutzer (sog. Frequency Capping).

Auf welche Rechtsgrundlage sich ein Unternehmen für diese Datenverarbeitungsvorgänge stützen kann, richtet sich vornehmlich nach Art. 6 der DSGVO. Neben der Einwilligung, die sich aufgrund ihrer Anforderungen nicht immer als „Königsweg" auszeichnet, spielt insbesondere das berechtigte Interesse gemäß Art. 6 Abs. 1 Buchst. f) DSGVO als Rechtsgrundlage für die Datenverarbeitung zu Werbezwecken eine besondere Rolle.

Welche Schritte und Erwägungen mit Blick auf die aktuelle Behördenpraxis zu berücksichtigen sind, ist nachfolgend dargestellt.

2. BERECHTIGTE INTERESSEN IM BEREICH TARGETING (ART. 6 ABS. 1 BUCHST. F) DSGVO)

Die automatisierte Aussteuerung von Online-Werbemittel an ausgewählte Zielgruppen dient der effizienten Aussteuerung von Werbemitteln und damit der Absatzförderung. Direktwerbung ist auch in den Augen des Gesetzgebers ein berechtigtes Interesse:

> *Erwägungsgrund 47, S. 7 der DSGVO:*
>
> *„[...] Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."*

Das bedeutet jedoch nicht, dass bereits aufgrund Erwägungsgrund 47 der DSGVO für die Verarbeitung von Nutzerdaten zur Aussteuerung verhaltensbezogener Werbung Art. 6 Abs. 1 Buchst. f) DSGVO greift. Vielmehr erfordert dieser Erlaubnistatbestand eine Prüfung der tatsächlichen berechtigten Unternehmensinteressen sowie eine Abwägung der gegenläufigen Interessen im konkreten Fall.

Dazu hat neben der Datenschutzkonferenz (siehe Anhang I) vornehmlich die britische Datenschutzbehörde ICO hilfreiche Handreichungen und ein Muster für die Durchführung einer solchen Prüfung (sog. **„Legitimate Interests Assessment" /"LIA"**) zur Verfügung gestellt. Das LIA umfasst dabei im Wesentlichen drei Prüfbereiche:

I. Die Identifizierung der (wirtschaftlichen) Unternehmensinteressen für die konkreten Verarbeitungsaktivitäten, sog. „Purpose Test“

II. Die Prüfung und Festlegung, ob bzw. dass die konkreten Verarbeitungsaktivitäten für die Erreichung der Unternehmensinteressen erforderlich und angemessen sind, sog. „Necessity Test“

III. Die tatsächliche Abwägung der gegenläufigen Interessen, sog. „Balancing Test“

I. Die Identifizierung der (wirtschaftlichen) Unternehmensinteressen für die konkreten Verarbeitungsaktivitäten, sog. „Purpose Test“

Mit der Aussteuerung verhaltensbezogener Werbung und der damit verbundenen Datenverarbeitungen muss das Unternehmen berechtigte Interessen verfolgen.

Beispiel:
Die Analyse des Surfverhaltens eines Internetnutzers, um diesem Nutzer gezielt bestimmte Online-Werbung anzuzeigen, kann bspw. dem wirtschaftlichen Interesse dienen, die Reichweite des beworbenen Produktes zu steigern, Streuverluste zu vermeiden und die Wettbewerbsfähigkeit am Markt aufrechtzuerhalten.

Für den konkreten Einzelfall sollte sich das Unternehmen i.R.d. „Purpose Test“ insbesondere mit folgenden Fragestellungen auseinandersetzen:

- Wer profitiert von dieser Datenverarbeitung (inkl. Dritte, z.B. Werbepartner)?
- Welche (wirtschaftlichen) Auswirkungen wären mit der Beendigung dieser Datenverarbeitung für das Unternehmen verbunden?
- Welche Maßnahmen hat das Unternehmen getroffen, um die Einhaltung der einschlägigen Gesetze und Branchenrichtlinien sicherzustellen?

II. Die Prüfung und Festlegung, ob bzw. dass die konkreten Verarbeitungsaktivitäten für die Erreichung der Unternehmensinteressen erforderlich und angemessen sind, sog. „Necessity Test"

Wurde ein berechtigtes Interesse ermittelt, müssen die mit der Aussteuerung verhaltensbezogener Werbung verbundenen Datenverarbeitungen zur Verwirklichung der vorgenannten Interessen erforderlich sein und kein milderes, gleich effektives Mittel zur Verfügung stehen.

> **Beispiel:**
> *Die Erforderlichkeit der Verarbeitung von Nutzerdaten zum Zwecke der Aussteuerung verhaltensbezogener Werbung kann bspw. dann vor Herausforderungen stehen, wenn mittels Nutzung aggregierter oder anonymer Datensätze die vom Unternehmen verfolgten Interessen gleichermaßen erreicht werden können (z.B. Contextual Targeting).*

Für den konkreten Einzelfall sollte sich das Unternehmen i.R.d. „Necessity Test" insbesondere mit folgenden Fragestellungen auseinandersetzen:

- Sind die Datenverarbeitung(en) für die Verwirklichung der vorgenannten Interessen erforderlich und nicht nur nützlich?

- Kann das Unternehmen den Zweck ggf. auch mittels Verwendung weniger eingriffsintensiven Informationen erreichen (z.B. Nutzung aggregierte oder anonyme Datensätze)?

- Ist der Inhalt und Umfang der Datenverarbeitungen verhältnismäßig und angemessen?

III. Die tatsächliche Abwägung der gegenläufigen Interessen, sog. „Balancing Test“

Zentraler Punkt des LIA ist der sog. „Balancing Test“: Hier müssen die Interessen des Unternehmens an den Datenverarbeitungen mit den Freiheiten und Rechten des Betroffenen abgewogen werden. Den wirtschaftlichen Interessen des Unternehmens steht regelmäßig der Schutz der personenbezogenen Daten des Betroffenen, sein Recht auf Privatsphäre und informationelle Selbstbestimmung, sowie der Schutz vor wirtschaftlichen Nachteilen gegenüber.

Das Unternehmen muss an dieser Stelle also darlegen und nachweisen, dass es sich mit den relevanten Datenverarbeitungen und ihren Auswirkungen für den Einzelnen tatsächlich auseinandergesetzt hat. Dabei stellen die vernünftigen Erwartungen des Betroffenen (sog. ‚reasonable expectations‘) und die Eingriffsintensität der Datenverarbeitungen wesentliche Faktoren dar, die in die jeweilige Gewichtung der gegenläufigen Interessen einfließen.

> **Beispiel:**
> *Im Rahmen der „reasonable expectations“ wird man u.a. vertreten können, dass die Anzeige verhaltensbezogener digitaler Werbeformate auf frei zugänglichen Webseiten und Plattformen heutzutage keinen unerwarteten oder überraschenden Charakter hat, auch wenn die betroffenen Personen mit der Technologie im Hintergrund nicht konkret vertraut sind.*

Für den konkreten Einzelfall sollte sich das Unternehmen i.R.d. „Balancing Test" daher insbesondere mit folgenden Fragestellungen auseinandersetzen:

- **Eingriffsintensität der Datenverarbeitung**
  - Welche Arten von personenbezogenen Daten werden verarbeitet?

  - Sind Dritte in die Datenverarbeitungen eingebunden und welche (vertraglichen) Absicherungen bestehen mit diesen Dritten?

  - Sind technische und vertragliche Maßnahmen (ggf. mit Drittanbietern) getroffen worden, um sicherzustellen, dass weder Daten von Minderjährigen oder sonstige Nutzerdaten verarbeitet werden, die als besonders sensibel gelten bzw. einen Rückschluss auf besondere Kategorien personenbezogener Daten zulassen (z.B. sexuelle Orientierung)?

- **Reasonable expectations**
  - Wie ist die „Beziehung" zum Betroffenen? Liegt beispielsweise zwischen dem Unternehmen und dem Betroffenen ein direktes (z.B. Kauf im Online-Shop) oder indirektes Verhältnis vor (z.B. Platzierung eigener Cookies auf Webseiten Dritter)?

  - Wie und in welchem Umfang wird der Betroffene über die Datenverarbeitungen informiert? Welche Transparenzmaßnahmen hat das Unternehmen getroffen?

  - Ist davon auszugehen, dass der Betroffene mit der Nutzung seiner Daten zu den benannten Zwecken rechnet?

  - Werden dem Betroffenen wirksame Kontrollrechte eingeräumt?

- **Risikominimierende Maßnahmen**
  - Welche potentiellen Risiken bestehen für die Betroffenen im Rahmen der Datenverarbeitung(en)?

  - Welche konkreten (technischen/ vertraglichen) Maßnahmen hat das Unternehmen getroffen, um die potentiellen Risiken zu vermeiden bzw. so gering wie möglich zu halten?

  - Wie lange werden die relevanten personenbezogenen Daten gespeichert?

Fazit

Ob die Interessenabwägung im konkreten Einzelfall zugunsten des Unternehmens ausfällt, hängt von der Intensität der Datenverarbeitung und den Möglichkeiten zur Risikobegrenzung ab. Werbetreibende Unternehmen sollten sich deshalb der von Ihnen genutzten (Dritt-)Technologien bewusst sein, die weiteren rechtlichen Entwicklungen im Auge behalten und jedenfalls die Risiken adressieren, die in ihrer Einflusssphäre liegen (Transparenz gegenüber und Wahlmöglichkeiten für den Nutzer).

Letztlich kann aber gerade beim Einsatz von aktueller Werbetechnologie hundertprozentige Rechtssicherheit kaum erreicht werden, bevor die Datenschutzbehörden eine europaweit einheitliche Handhabung abgestimmt haben.

GDPR Playbook

E-Mail Marketing im Licht der DS-GVO

Dr. Jens Eckhardt

1. EINLEITUNG

Die Datenschutz-Grundverordnung (DS-GVO) hat zum 25.05.2018 EU-weit das dahin geltende Datenschutzrecht abgelöst und damit ein in der EU grundsätzlich einheitliches Datenschutzrecht geschaffen.

Durch die einheitliche Geltung in allen EU-Mitgliedstaaten ist das EU-weite E-Mail-Marketing erleichtert worden. Aus deutscher Sicht bedeutet das auch, dass Vorgaben, die in Deutschland bisher strenger waren als in den anderen EU-Mitgliedstaaten, jedenfalls formal entfallen. Beispielsweise gab es keine dem § 7 Abs. 3 UWG entsprechende datenschutzrechtliche Regelung im BDSG-alt und im TMG, sodass hier stets eine Unsicherheit bestand.

Bei der rechtlichen Bewertung ist zu unterscheiden zwischen der datenschutzrechtlichen Zulässigkeit der Zusendung von E-Mail-Werbung einerseits und einer Auswertung des Lese-/Öffnungsverhaltens anderseits sowie einem Profiling zur Entscheidung über das Ob, Wie und den Inhalt einer Werbe-E-Mail. Auch wenn diese drei Aspekte aus Anwendersicht verbunden sind, so ist für die datenschutzrechtliche Bewertung dennoch eine Trennung geboten.

2. ANWENDUNGSBEREICH: WER MUSS DIE DS-GVO BEACHTEN? FÜR WELCHE DATEN GILT DIE DS-GVO?

Die DS-GVO gilt für die automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO). Eine automatisierte Verarbeitung darf beim E-Mail-Marketing ohne Weiteres angenommen werden.

Die für das E-Mail-Marketing verwendeten Daten, insbesondere die E-Mail-

Adresse, werden daher typischerweise ein personenbezogenes Datum sein und zur Anwendung des Datenschutzrechts führen. Die Abgrenzung wird relevanter, wenn es um das Messen des Lese-/Öffnungsverhalten und das Profiling geht, da dies leichter umzusetzen wäre, soweit das Datenschutzrecht nicht zur Anwendung kommen sollte.

Entscheidend dafür ist, dass es um personenbezogene Daten geht. Als personenbezogene Daten definiert Art. 4 Nr. 1 DS-GVO:

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;"

Beim E-Mail-Marketing werden diese Voraussetzungen typischerweise gegeben sein. Die DS-GVO ist damit zu beachten.

Die DS-GVO gilt aber nicht (mehr) für anonymisierte Daten, wie sich aus Erwägungsgrund 26 Satz 5 DS-GVO entnehmen lässt. Gerade für die Zulässigkeit von Profiling und Analyse im Rahmen von Smart Data ist das entscheidend, wenn diese nicht die Anforderungen der DS-GVO erfüllen.

Für die Grenzziehung lassen sich aus Erwägungsgrund 26 DS-GVO ebenfalls weitere Anhaltspunkte entnehmen: Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem

Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Hieraus kann zweierlei geschlossen werden: Einerseits ist die Schwelle zur Anonymisierung nicht leicht überschritten. Andererseits lässt sich das nicht abstrakt beurteilen, sondern es muss im konkreten Einzelfall entschieden werden.

Erwägungsgrund 26 DS-GVO enthält noch eine weitere wichtige Aussage: Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. In ihrem Art. 4 Nr. 5 definiert die DS-GVO dann auch den Begriff Pseudonymisierung. Das bedeutet: Auch für pseudonymisierte Daten gilt grundsätzlich die DS-GVO.

Allein der Umstand, dass E-Mail-Marketing im B2B (Business to Business) betrieben wird, ändert hieran nichts. Entscheidend ist auch dann allein, ob personenbezogene Daten verwendet werden.

Werden personenbezogene und nicht personenbezogene Daten gemeinsam verarbeitet, dann muss der Schutz am „schwächsten Glied" ausgerichtet werden und das Datenschutzrecht beachtet werden.

Kurzum: Das Datenschutzrecht gilt für alle Informationen, die einem Menschen zugeordnet werden können. Die Pflichten nach der DS-GVO treffen denjenigen, der über die Verarbeitung der Daten entscheidet. Auch für das E-Mail-Marketing gelten typischerweise die datenschutzrechtlichen Pflichten.

3. VERANTWORTLICHER, AUFTRAGSVERARBEITER UND JOINT CONTROLLERSHIP

Die DS-GVO bezeichnet denjenigen, der über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, als „Verantwortlicher" (Art. 4 Nr. 7 DS-GVO). Er ist der primäre Adressat der Pflichten der DS-GVO. Das ist typischerweise das werbungbetreibende Unternehmen.

Wenn Dienstleister, Partner oder sonstige Dritte eingesetzt werden, dann stellt sich die Frage, wie diese nach der DS-GVO einzuordnen sind:

- Der Dritte kann eigenständig Verantwortlicher sein. Das ist er bspw. wenn er zwar Daten erhält, aber allein und eigenständig über die Zwecke und Mittel der Verarbeitung der erhaltenen personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Für die Übertragung der Daten an den Dritten bedarf es dann einer Rechtsgrundlage nach Maßgabe des Art. 6 DS-GVO.

- Entscheidet hingegen der Verantwortliche allein darüber, wie der Datenempfänger die Daten verarbeitet - sprich über Zweck und Mittel -, dann kann (und sollte grundsätzlich) der Datenempfänger nach Maßgabe des Art. 28 (und 29 DS-GVO) DS-GVO als Auftragsverarbeiter eingebunden werden.

  Zu beachten ist, dass der Abschluss einer Vereinbarung nach Maßgabe des Art. 28 DS-GVO Voraussetzung für die datenschutzrechtliche Behandlung als Auftragsverarbeitung ist. Mit anderen Worten: Ohne Vereinbarung nach Art. 28 DS-GVO keine Auftragsverarbeitung. Dann bedarf die Übertragung einer Rechtsgrundlage nach Art. 6 DS-GVO.

- Entscheiden der Verantwortliche und der Dritte gemeinsam über den Zweck und die Mittel der Verarbeitung, dann ist – so Art. 4 Nr. 7 DS-GVO - von einer gemeinsamen Verantwortlichkeit in Bezug auf die so gemeinsam festgelegten Verarbeitungsschritte auszugehen (auch bezeichnet als Joint Controllership).

Für die gemeinsame Verarbeitung (einschließlich der Übertragung) der Daten bedarf es dann einer Rechtsgrundlage nach Maßgabe des Art. 6 DS-GVO. Darüber hinaus müssen die Verantwortlichen hinsichtlich der gemeinsam festgelegten Verarbeitung(en) zwingend die Vorgaben des Art. 26 DS-GVO umsetzen.

Die Pflicht zum Abschluss der Vereinbarung nach Art. 26 DS-GVO ist – anders als bei der Auftragsverarbeitung – nicht Voraussetzung einer Joint Controllership sondern die Rechtsfolge. Ob eine Joint Controllership vorliegt oder nicht, bestimmt sich nach Art. 4 Nr. 7 DS-GVO.

Der EuGH hat in den letzten Jahren durch drei Entscheidungen die Abgrenzung konkretisiert (Urt. v. 05.06.2018, C-210/16 – Stichwort „Facebook-Fanpage; Urt. v. 10.07.2018, C-25/17 – Stichwort „Zeugen Jehovas"; Urt. v. 29.07.2019, C-40/17 – Stichwort „Fashion ID"). Vor allem durch die Entscheidung „Fashion ID" (Urt. v. 29.07.2019, C-40/17) sind Kriterien herausgearbeitet worden. Entscheidend ist aber auch, dass der EuGH in der Entscheidung „Fashion ID" herausgestellt hat, dass es in einem einheitlichen Ablauf vor- und nachgelagerte Verarbeitungen geben kann, die nicht zwingend eine Joint Controllership sein müssen, nur weil in Bezug auf einen Teil der Verarbeitungsschritte eine solche vorliegt. Beispielsweise muss nicht zwingend auch die Erhebung von Daten eine Joint Controllership sein, nur weil die Auswertung im Rahmen einer Joint Controllership erfolgt.

Eine Auftragsverarbeitung und eine Joint Controllership können grundsätzlich zu einer gemeinsamen Haftung auf Schadensersatz führen (vgl. Art. 82 DS-GVO). Nicht datenschutzkonforme Ausgestaltungen unter den Beteiligten (bspw. fehlende oder unvollständige Vereinbarung nach Art. 26 DS-GVO) können zu Bußgeldern führen.

Kurzum: Die Zusammenarbeit mit anderen Unternehmen erfordert eine klare Beschreibung und Abgrenzung der Rollen, um eine datenschutzrechtliche Bewertung und damit datenschutzkonforme Gestaltung der Zusammenarbeit zu ermöglichen.

4. EINORDNUNG DER ANFORDERUNGEN AN DAS E-MAIL-MARKETING IN DEN GESAMTKONTEXT DER DS-GVO

Über die Zulässigkeit der Verarbeitung personenbezogener Daten hinaus sieht die DS-GVO umfassende Dokumentations-, Transparenz- und Organisationspflichten vor. Dies wird teilweise auch als Paradigmenwechsel im Datenschutzrecht im Vergleich zum bis zur DS-GVO geltenden Datenschutzrecht bezeichnet. Die Missachtung dieser zusätzlichen Pflichten macht zwar das E-Mail-Marketing nicht zwingend unzulässig, kann aber zu drakonischen Bußgeldsanktionen führen.

Diese Anforderungen lassen sich am leichtesten so begreifen:

- Die Zulässigkeitsanforderungen werden durch Dokumentations- und Transparenzpflichten flankiert.

- Die Handlungspflichten werden durch Organisationspflichten flankiert.

Im Extremfall kann das dazu führen, dass zwar das E-Mail-Marketing zulässig ist, aber dennoch ein Bußgeld ausgesprochen wird, weil bspw. eine Transparenz- oder Dokumentationspflicht missachtet wurde.

Der Sinn und Zweck der zusätzlichen Dokumentations- und Transparenzpflichten wird wohl vor allem in zwei Aspekten bestehen: Der Verantwortliche soll dazu gezwungen werden, sich hierdurch mit der Verarbeitung datenschutzrechtlich auseinanderzusetzen (Stichwort: Selbstkontrolle). Die Überprüfung und Kontrolle „von außen" wird dadurch ebenfalls wesentlich erleichtert.

Kurzum bedeutet das für ein rechtskonformes E-Mail-Marketing: Über die reine Zulässigkeitsfrage hinaus sind weitere Pflichten zu erfüllen, um „DS-GVO-compliant" zu sein.

Diese weiteren Pflichten nach der DS-GVO gelten nicht nur für das E-Mail-Marketing, aber eben auch für das E-Mail-Marketing. Das sind insbesondere und in Schlagworten:

- Der Verantwortliche muss die Einhaltung der in Art. 5 Abs. 1 DS-GVO genannten sechs Grundsätze der DS-GVO nachweisen können (sog. Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO). Dazu gehören insbesondere die Rechtmäßigkeit, die Transparenz, die Zweckbindung, die Datenminimierung und Löschregelungen.

  Zu betonen sind vor allem die Pflichten zur Datenminimierung (nur die erforderlichen Daten dürfen verarbeitet werden) und die Löschpflicht (Daten müssen zu festgelegten Daten gelöscht werden). Hier drohen und sind bereits Bußgelder verhängt worden.

  Die Datenschutzaufsichtsbehörde Berlin hat einen Verstoß gegen die Pflicht zur Datenlöschung zum Gegenstand eines Bußgeldbescheids gemacht (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (zuletzt geprüft: 20.01.2020)). Das macht deutlich, dass diese Pflicht nicht zu vernachlässigen ist.

- Der Verantwortliche trifft nach Art. 12 DS-GVO geeignete Maßnahmen, um der betroffenen Person alle Informationen im Rahmen der proaktiven Transparenzpflichten und im Rahmen der Rechte der betroffenen Personen (u. a. Auskunft, Löschung, Recht auf Vergessenwerden, Datenportabilität) unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.

- Der Verantwortliche setzt nach Art. 24 DS-GVO unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie

der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

- Es muss die Einhaltung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nach Art. 25 DS-GVO beachtet werden.

Die Datenschutzaufsichtsbehörde Berlin hat einen Verstoß gegen die Pflicht zum Datenschutz durch Technikgestaltung zum Gegenstand eines Bußgeldbescheids gemacht (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (zuletzt geprüft: 20.01.2020)). Das macht deutlich, dass auch diese Pflicht nicht zu vernachlässigen ist.

- Jeder Verantwortliche führt nach Art. 30 Abs. 1 DS-GVO ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält die in Art. 30 Abs. 1 DS-GVO genannten Angaben. Auftragsverarbeiter haben zusätzlich nach Art. 30 Abs. 2 DS-GVO ein Verzeichnis für ihre Tätigkeiten als Auftragsverarbeiter zu führen.

- Die Pflichten zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO sind weit umfangreicher als nach bisherigem Datenschutzrecht und nicht deckungsgleich mit der IT-Sicherheit.

- Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden diese der Aufsichtsbehörde (Art. 33 DS-GVO) und den betroffenen Personen (Art. 34 DS-GVO).

- In Bezug auf jede Verarbeitung muss geprüft werden, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO zu erfolgen hat.

  Diese wird bei einem einfachen Versenden von E-Mail-Werbung typischerweise keine Rolle spielen. Werden komplexe Analysen oder Aufbereitungen eingesetzt, kann eine solche Prüfung erforderlich werden.

Kurzum: Die DS-GVO-Compliance im E-Mail-Marketing erfordert mehr als die Prüfung der Zulässigkeit der Zusendung. Gerade die Nichtbeachtung „flankierender Pflichten" kann zur (bußgeldbewehrten) „Stolperfalle" werden. Hierzu zählen insbesondere die Prüfung der Grundsätze nach Art. 5 DS-GVO, die Transparenzpflichten nach Artt. 12, 13, 14 DS-GVO sowie das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO.

5. DS-GVO-KONFORME DATENGENERIERUNG

Für die Zulässigkeit des E-Mail-Marketing ist sowohl das Datenschutzrecht als auch das Wettbewerbsrecht zu beachten. § 7 UWG regelt unter welchen Voraussetzungen eine E-Mail-Werbung zulässig ist. Diese Regelungen im UWG werden auch nicht durch die DS-GVO geändert oder gar aufgeboben.

Nach § 7 UWG ist E-Mail-Werbung zulässig, wenn die vorherige ausdrückliche Einwilligung des Inhabers der E-Mail-Adresse gegeben oder die Voraussetzungen der Ausnahme des § 7 Abs. 3 UWG vorliegen ist (hierzu nachfolgend Ziffer 5.5).

5.1 Nebeneinander von UWG und DS-GVO

Die DS-GVO verdrängt in Bezug auf E-Mail-Marketing nicht die Vorgaben in § 7 Abs. 2 Nr. 3, Abs. 3 UWG. Die vereinfacht zusammengefasste Begründung: Diese Regelungen beruhen auf Art. 13 Datenschutzrichtlinie 2002/58/EG. Die Vorgaben der Datenschutzrichtlinie 2002/58/EG werden gemäß Art. 95 DS-GVO nicht durch die Regelungen der DS-GVO verdrängt. Die Verweise der Datenschutzrichtlinie 2002/58/EG auf die allgemeine Datenschutzrichtlinie 95/46/EG gelten gemäß Art. 94 DS-GVO als Verweise auf die DS-GVO. Das hat beispielsweise zur Konsequenz, dass die Anforderungen an eine Einwilligung im Sinne des § 7 Abs. 2 Nr. 3 UWG der DS-GVO zu entnehmen sind. Praktische Konsequenz: Wenn nach § 7 UWG eine Einwilligung erforderlich ist, gilt das auch für das Datenschutzrecht.

5.2 Einwilligungsbasierte E-Mail-Werbung: Inhalt der Einwilligung

Eine Einwilligung nach Maßgabe des Art. 6 Abs. 1 Satz 1 lit. a DS-GVO ist für die rechtmäßige Verarbeitung von personenbezogenen Daten erforderlich, wenn und weil nach § 7 Abs. 2 Nr. 3 UWG eine Einwilligung erforderlich ist. Die inhaltliche Anforderungen an eine Einwilligung ergeben sich aus Art. 4 Nr. 11 DS-GVO. Diese Definition gilt auch für das vorliegende E-Mail-Marketing.

Eine Einwilligung ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (Art. 4 Nr. 11 DS-GVO).

Die Einwilligung hat durch eine eindeutige bestätigende Handlung zu erfolgen. Aus Erwägungsgrund 32 DS- GVO ergibt sich, dass das durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen soll, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer

personenbezogenen Daten signalisiert; Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen hingegen keine Einwilligung dar.

Daraus ergibt sich, dass konkret beschrieben werden muss, wer mit welchem Inhalt werben wird. Das bedeutet:

- Aus der Einwilligung selbst oder aus dem Gesamtkontext muss sich eindeutig ergeben, welches Unternehmen zur werblichen Ansprache berechtigt ist. Das erfordert jedenfalls den vollständigen Unternehmensnamen. Sollen weitere Unternehmen berechtigt sein, müssen auch diese genannt sein.

- Aus der Einwilligung muss sich auch ergeben, zu welchem Inhalt die Werbung erfolgt. Wenngleich die Anforderungen nicht überstrapaziert werden dürfen, so muss für den Einwilligenden doch erkennbar und eingrenzbar sein, um was es gehen wird.

- Aus der Einwilligung muss sich auch ergeben – wenn es nicht aufgrund der Gesamtumstände ohnehin klar ist – mit welchem Medium geworben wird.

Die Anforderungen an die Konkretisierung der Einwilligung haben sich in einer Reihe von deutschen Gerichtsentscheidungen zu § 7 UWG konkretisiert. Dem BGH genügte zunächst in seiner Entscheidung vom 14.03.2017 die Formulierung „Mit der Angabe seiner persönlichen Daten erklärt der Nutzer sein Einverständnis, dass er von F. M. Limited und den hier genannten Sponsoren Werbung per E-Mail an die vom Nutzer angegebene E-Mail-Adresse erhält. Der Nutzer kann der werblichen Nutzung seiner Daten durch F. M. Limited jederzeit durch eine E-Mail an Info@f...-m...com widersprechen" nicht (BGH, VI ZR 721/15, ZD 2017, 327, 329. m. Anm. Eckhardt). Denn – so der BGH - es bleibe offen, für welche Produkte und Dienstleistungen diese werben. Aus ihren Firmen allein könne nicht auf die zur zukünftigen Bewerbung anstehenden Produkte geschlossen werden. Bereits zeitlich zuvor aber auf derselben Linie hatte das OLG Frankfurt a. M. in seinem Urteil vom

28. 7. 2016 darauf abgestellt, dass „eine Konkretisierung des Inhalts wie folgt nicht den Anforderungen genügen solle" (OLG Frankfurt a. M., 28. 7. 2016 – 6 U 93/15, ZD 2017, 33, 34): „Media und Zeitschriften"..., „Vermögenswirksame Leistungen"..., „Altersvorsorge"..., „Finanzen und Versicherungen"..., „Telekommunikationsprodukte bzw. -angebote" (verschiedene Anbieter) und die pauschale Beschreibung der Geschäftsbereiche „E-Mail Werbung für Unternehmen" (zahlreiche Anbieter) und „Versandhandel" sowie „Zusendung von Newslettern des Portals. ...com/de mit unterschiedlichen Produktangeboten wie bspw. Kleidung, Reisen, Rabatte". Die Messlatte war damit recht hoch gelegt.

Zu Beginn des Jahres 2018 kam der BGH dann jedoch recht überraschend zu dem Ergebnis, dass die Begriffe „individueller Kundenberatung" und „neue Angeboten und Services" eine hinreichende Konkretisierung des Inhalts der Werbung darstellen können und eine nähere Konkretisierung gerade nicht erforderlich sei (BGH, Urt. v. 1. 2. 2018 – III ZR 196/17, K&R 2018, 245 ff. mit Anm. Eckhardt). Der BGH führte die Anforderungen auf ein Normalmaß zurück. Dem OLG Frankfurt a. M. genügte dementsprechend beispielsweise die Angabe „Strom & Gas" unter Bezugnahme auf die Verwenderin dieser Formulierung für eine Konkretisierung (Urt. v. 27.6.2019, Az. 6 U 6/19, ZD 2019, 507 ff. mit Anm. Eckhardt).

5.3 Einwilligungsbasierte E-Mail-Werbung: Weitere Anforderungen an die Einwilligung

Die DS-GVO sieht in Artt. 7 und 8 DS-GVO weitere Anforderungen an eine Einwilligung. Aus Art. 7 DS- GVO ergeben sich folgende weitere Anforderungen an die Einwilligung:

- Das werbende Unternehmen muss die Einwilligung – also die Einhaltung der Anforderungen der DS-GVO nach Art. 4 Nr. 11 DS-GVO – beweisen können (Art. 7 Abs. 1 DS-GVO).In der Praxis bedeutet das, dass – wie bisher auch – ein Double-Opt-In-Verfahren eingesetzt werden sollte.

Hinweis: Auch das Double-Opt-In-Verfahren muss DS-GVO-konform gestaltet werden. Das bedeutet neben Prüfung der Zulässigkeit der Speicherung der Daten hierfür vor allem die Beachtung der Informationspflicht nach Art. 13 DS-GVO auch in Bezug auf das Double-Opt-In-Verfahren.

• Wird die Einwilligung zusammen mit anderen Erklärungen erteilt, muss die Abfrage der Einwilligung von den anderen Erklärungen klar zu unterscheiden sein. Hier bieten sich Absetzungen und Hervorhebungen an. Die Abfrage muss dabei in verständlicher und leicht zugänglicher Form und in klarer und einfacher Sprache erfolgen (Art. 7 Abs. 2 Satz 1 DS-GVO). In Art. 7 Abs. 2 Satz 2 DS-GVO steht der Satz: „Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen." Die Bedeutung ist nicht eindeutig. Die Regelung könnte so verstanden werden, dass jeder Verstoß gegen die DS-GVO oder Art. 7 DS-GVO die Einwilligung unwirksam machen würde. Das würde aber zu weit gehen. Aus der englischen Textfassung der DS-GVO ergibt sich jedoch, dass dieser Satz nur Auf Art. 7 Abs. 2 Satz 1 DS-GVO bezogen ist.

• Der Einwilligende muss vor der Erteilung der Einwilligung auf sein Recht zum Widerruf der Einwilligung hingewiesen werden; er hat das Recht eine Einwilligung jederzeit für die Zukunft zu widerrufen (Art. 7 Abs. 3 DS-GVO). Damit dürfen die Daten dann nicht mehr entsprechend der Einwilligung verarbeitet werden.

Der Verstoß gegen diese Hinweispflicht macht die Einwilligung aber nicht unwirksam. Denn die Anforderungen an eine wirksame Einwilligung sind in Art. 4 Nr. 11 DS-GVO festgelegt. Dass ein Verstoß gegen Art. 7 DS-GVO nicht stets zur Unwirksamkeit der Einwilligung führt, ergibt sich daraus, dass der Gesetzgeber diese Konsequenz in Art. 7 Abs. 2 DS-GVO nicht explizit geregelt hat.

- Die Freiwilligkeit der Einwilligung muss auch bei einer Verbindung der Einwilligung mit anderen Leistungen bestehen bleiben (Art. 7 Abs. 4 DS-GVO) (hierzu siehe unten Ziffer 5.4 (Freiwilligkeit und Kopplung)).

Art. 8 DS-GVO sieht besondere Anforderungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft vor. Ein solcher Dienst der Informationsgesellschaft ist eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535: jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. E-Mail-Marketing fällt damit typischerweise nicht in den Anwendungsbereich von Art. 8 DS-GVO.

Wenn Art. 8 DS-GVO Anwendung finden sollte, dann wären Einwilligungen von Personen bis zum vollendeten 16. Lebensjahr unwirksam; für diese müssten die gesetzlichen Vertreter einwilligen. Wenn Art. 8 DS-GVO nicht anwendbar ist, kommt es bei Minderjährigen auf die Einsichtsfähigkeit an, die von der Art der Verarbeitung abhängt und ab etwa 14 Jahren gegeben sein kann. Der Unterschied besteht also in einem Zeitfenster von rund 2 Jahren.

Soweit aus Art. 8 DS-GVO darüber hinaus teilweise abgeleitet wird, dass Maßnahmen ergriffen werden müssten, um sicherzustellen bzw. zu prüfen, dass der Einwilligende über 16 Jahre ist, findet das im Wortlaut keinen ausreichenden Ausdruck.

5.4 Freiwilligkeit und Kopplung

Aus Erwägungsgrund 42 DS-GVO ergibt sich, dass die Freiwilligkeit nur gegeben ist, wenn der Einwilligende eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Das erfordert aber nicht, dass er eine Leistung auch ohne Einwilligung in Werbung kostenfrei erhalten können muss. Denn er hat auch dann eine freie Wahl, wenn er auf die Leistung verzichtet. Anderenfalls wäre die Privatautonomie des Anbieters

unangemessen beeinträchtigt. Denn de facto würde die Regelung ihm dann die Angebotsgestaltung vorschreiben. Jedenfalls Gestaltung bei denen die Einwilligung die Gegenleistung für eine dann kostenfreie Leistung ist, scheitern nicht an der Vorgabe.

Art. 7 Abs. 4 DS-GVO sieht vor: Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Schon der Wortlaut macht deutlich, dass es sich nicht um ein starres Kopplungsverbot handelt. Denn die Kopplung wird gerade nicht verboten. Sie fordert, dass eine solche Kopplung bei der Bewertung, ob eine Einwilligung freiwillig ist, berücksichtigt wird. In der Sache geht die Regelung damit von der Zulässigkeit von Kopplungen aus. Es ist also ein Konzept möglich, bei dem eine Einwilligung die Gegenleistung für eine Leistung ist.

Aus Erwägungsrund 43 DS-GVO ergeben sich weitere Anhaltspunkte für die Bewertung der Freiwilligkeit einer Einwilligung. In besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, soll eine Einwilligung keine gültige Rechtsgrundlage liefern. Allein der Umstand, dass eine Einwilligung als Gegenleistung einer Leistung oder mit einer Leistung gekoppelt wird, begründet kein solches Ungleichgewicht.

Die Einwilligung gilt nach Erwägungsgrund 43 DS-GVO auch nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist. Ob eine solche Einwilligung angebracht oder erforderlich ist, darf nicht allein aus der subjektiven Perspektive der betroffenen Personen bewertet werden. Nach der DS-GVO sind solche Aspekte objektiv zu bewerten (vgl. Erwägungsgrund 76 DS-GVO). Damit ist es eben nicht grundsätzlich ausgeschlossen, eine Werbe- Einwilligung an die Erbringung einer Leistung zu koppeln oder damit zu verbinden.

Das OLG Frankfurt bejahte in seinem Urteil vom 27.6.2019 die Zulässigkeit einer Kopplung einer Gewinnspielteilnahme an eine Einwilligung in Direktwerbung. Von einer wettbewerbsrechtlichen Perspektive ausgehend führt es aus, dass besondere Umstände hinzutreten müssten, damit eine Unfreiwilligkeit gegeben sei (Urt. v. 27.6.2019, Az. 6 U 6/19, ZD 2019, 507 ff. mit Anm. Eckhardt). Das Gericht geht davon aus, dass es für die Freiwilligkeit darauf ankomme, dass der Verbraucher selbst entscheiden könne und müsse, ob ihm die Teilnahme die Preisgabe seiner Daten „wert" sei. Art. 7 Abs. 4 DS-GVO wird durch das OLG Frankfurt aber nicht thematisiert, obgleich es die DS-GVO anwendet (Urt. v. 27.6.2019, Az. 6 U 6/19, ZD 2019, 507 ff. mit Anm. Eckhardt).

Wenngleich die Entscheidung im Ergebnis richtig ist, erscheint die Argumentation zu sehr aus wettbewerbsrechtlicher Sicht gewonnen zu sein. Das Wettbewerbsrecht und das Datenschutzrecht unterscheiden sich nämlich systematisch darin, dass nach dem UWG die Unzulässigkeit begründungsbedürftig ist, während nach der DS-GVO die Zulässigkeit zu begründen ist. Daher fragt das OLG Frankfurt auch, ob die „Schwelle" zur Unzulässigkeit überschritten ist, während datenschutzrechtlich zu begründen wäre, warum die „Schwelle" unterschritten ist. (siehe Anmerkung Eckhardt zu OLG Frankfurt a.M., Urt. v. 27.6.2019, Az. 6 U 6/19, ZD 2019, 507 ff.).

Der Oberste Gerichtshof in Österreich (OGH) kam hingegen in seinem Urteil vom 31.08.2018 (Az. 6 Ob 140/18h) zu dem Ergebnis, dass bei einer Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss grundsätzlich davon auszugehen sei, dass die Erteilung der Einwilligung nicht freiwillig erfolge, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen sollten. Leider unterblieb in der Entscheidung des OLG Frankfurt a.M. eine Auseinandersetzung mit dieser Entscheidung des OGH (siehe Anmerkung Eckhardt zu OLG Frankfurt a.M., Urt. v. 27.6.2019, Az. 6 U 6/19, ZD 2019, 507 ff.).

Kurzum: Eine Einwilligung in E-Mail-Werbung darf an die Erbringung an eine Leistung und insbesondere als Gegenleistung für eine Leistung vorgesehen werden. Allerdings muss eine Bewertung erfolgen, ob aufgrund der Gesamtumstände aus weiteren Gründen die Kopplung dazu führt, dass die Einwilligung unfreiwillig ist. Die sich widersprechende Rechtsprechung macht aber auch deutlich, dass das noch nicht abschließend geklärt ist.

5.5 E-Mail-Werbung gegenüber Bestandskunden ohne Einwilligung

E-Mail-Werbung ist nach § 7 Abs. 3 UWG auch ohne Einwilligung zulässig, wenn

1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,

2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,

3. der Kunde der Verwendung nicht widersprochen hat und

4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Diese Regelung kommt nur gegenüber Bestandskunden zur Anwendung. Sie ist inhaltlich auf eigene ähnliche Produkte beschränkt. Auch wenn diesbezüglich eine gewisse Großzügigkeit greifen sollte, so ist sie gegenüber der Einwilligung begrenzt. Darüber hinaus muss entsprechend dieser Vorgabe die Information der Bestandskunden erfolgen. Wer zu beweisen hat, ob ein Widerspruch erfolgt ist oder nicht, wird im Einzelfall problematisch werden können.

Datenschutzrechtlich wird die Verwendung der E-Mail-Adresse zu diesen Zwecken nach Art. 6 Abs. 1 Satz 1 lit. f. DS-GVO zulässig sein. Denn die Vorgabe in § 7 Abs. 3 UWG beruht auf Art. 13 der sog. ePrivacy-Richtlinie (Richtlinie 2002/58/EG). Es ist also Zulässigkeitsvorgabe des EU-Gesetzgebers, die im Rahmen der Bewertung nach Artt. 6 Abs. 1 Satz 1 lit. f. DS-GVO nicht konterkariert wird; wenn nicht sogar, die Vorgabe in § 7 Abs. 3 UWG aufgrund von Art. 95 DS-GVO vorrangig ist.

Die weiteren in dieser Guideline angesprochenen Pflichten der DS-GVO müssen aber auch in diesem Fall eingehalten werden.

6. PERSONALISIERUNG DER WERBUNG UND „MESSEN" DER NUTZUNG

Für die Personalisierung und das „Messen" der Nutzung von E-Mail-Werbung kommen die Einwilligung und gesetzliche Zulässigkeitsregelungen in Betracht. Die DS-GVO sieht keinen generellen Vorrang der Einwilligung vor einer gesetzlichen Zulässigkeitsregelung vor. In Art. 4 Nr. 4 enthält die DS-GVO zwar eine Definition des Begriffs „Profiling". Die DS-GVO enthält aber keine Spezialregelung für ein Profiling im Kontext von Marketing.

Als Rechtsgrundlage kommt damit die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht.

Die Personalisierung und das „Messen" ist danach nicht grundsätzlich ausgeschlossen, sondern bedarf eine Bewertung im Einzelfall. Maßgabe dabei nach Erwägungsgrund 47 DS-GVO die vernünftigen Erwartungen der betroffenen Person bei der Interessenabwägung. Die Erwartungshaltung der betroffenen Person bestimmt sich insbesondere auch durch die Informationen, die ihr durch den Werbetreibenden, insbesondere bei der Erhebung der Daten nach Art. 13 DS-GVO, gegeben werden. Wird also – was ohnehin gesetzlich verpflichtend ist – der betroffenen Person die Personalisierung und das „Messen" transparent gemacht, wird eher von einer Zulässigkeit auszugehen sein.

Wird eine Verarbeitung auf diese Interessenabwägung gestützt, muss die betroffene Person auf das Recht, dieser Verarbeitung von Daten zu widersprechen, hingewiesen werden (Art. 21 Abs. 4, Art. 13 Abs. 2 lit. b DS-GVO).

Die bisher im deutschen Recht durch § 28 Abs. 3 BDSG-alt (Spezialregelung für Werbung im BDSG-alt) und § 15 Abs. 3 TMG (Spezialregelung für Online-Profile) bestehenden weitergehenden Beschränkungen sind mit dem Anwendungsbeginn der DS-GVO am 25.05.2018 entfallen. Das BDSG-alt ist außer Kraft getreten und § 15 Abs. 3 TMG greift aufgrund des Anwendungsvorrangs der DS-GVO nicht mehr (vgl. auch EuGH, Urt. v. 01.10.2019, Az. C-673-17, Verbraucherzentrale Bundesverband e.V. / Planet49 GmbH). Es gelten damit in Deutschland auch die „Spielregeln", wie sie in der gesamten EU gelten.

Art. 22 DS-GVO trägt die Überschrift „Automatisierte Entscheidungen im Einzelfall einschließlich Profiling". Entgegen dem Anschein durch die Überschrift ist dies keine generelle Regelung des Profilings, sondern nur eines speziellen Profilings. Das Profiling zu Marketingzwecken fällt typischerweise nicht hierunter.

7. PROAKTIVE INFORMATIONSPFLICHTEN

Die DS-GVO sieht in Artt. 13 und 14 umfassende proaktive Transparenzpflichten vor. Bei der E-Mail- Werbung ist Art. 13 DS-GVO relevant, weil die Daten direkt beim Einwilligenden (und nicht aus Drittquellen) erhoben werden. Die Regelung gilt zusätzlich zu den inhaltlichen Anforderungen an eine Einwilligung.

Vermeiden Sie zwei „Stolperfallen":

- Diese Informationspflicht gilt auch, wenn eine Einwilligung eingeholt wird. Mit anderen Worten: Neben dem Text der Einwilligung muss zusätzlich über den Pflichtinhalt des Art. 13 DS-GVO informiert werden. Die Pflicht zur Information besteht auch neben den Informationen, die nach § 7 Abs. 3 UWG zu geben sind.

- Die Informationspflicht besteht für jede Verarbeitung: Zusendung der E-Mail, Double-Opt-In-Verfahren, „Messung" des Verhaltens, Profiling usw. Ausgehend vom Zweck der jeweiligen Verarbeitung muss nach Art. 13 DS-GVO informiert werden.

Nach Art. 13 Abs. 1 DS-GVO ist der betroffenen Person Folgendes mitzuteilen:

- Der Namen und die Kontaktdaten des Verantwortlichen sowie – Sitz in einem Drittstaat (vgl. Art. 27 DS-GVO)- sowie ggfs. seines Vertreters
Bspw. Muster GmbH, Musterstraße 18, 0000 Musterstadt, muster@....

- sofern einer benannt ist - die Kontaktdaten des Datenschutzbeauftragten
„Der Datenschutzbeauftragte ist unter der vorgenannten Anschrift und datenschutzbeauftragter@.... erreichbar."

- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen,

sowie die Rechtsgrundlage für die Verarbeitung;
Hinweis: Dieser Zweck ergibt sich bereits aus dem Text der Einwilligung oder dem Hinweis nach § 7 Abs. 3 UWG. Die Rechtsgrundlage ist dann entweder die Einwilligung nach Art. 6 Abs. 1 Satz 1 lit. a DS-GVO oder § 7 Abs. 3 UWG i.V.m. Art. 6 Abs. 1 Satz 1 lit. f DS-GVO.

- wenn die Verarbeitung auf der Interessenabwägung (Art. 6 Absatz 1 lit. f DS-GVO) beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.
Hier müssen auch Auftragsverarbeiter genannt werden, wenn sie eingesetzt werden

- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie weitere Angaben zu Datenschutzniveau im Drittstaat.

Nach Art. 13 Abs. 2 DS-GVO sind zusätzlich folgende weitere Informationen zur Verfügung zu stellen, „die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten":

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
Hinweis: Die Verarbeitung erfolgt im Fall der Einwilligung bis zum Widerruf und im Fall gesetzlicher Grundlage bis zum Widerspruch zur Zusendung von E-Mail-Werbung.

- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung

oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
Hinweis: Auch wenn die Informationspflicht nach Art. 13 DS-GVO für jede Verarbeitung entsprechend dem Zweck besteht, kann bei einem gemeinsamen Hinweis der Hinweis auf die Betroffenenrechte in einem Text gegeben werden.

- wenn die Verarbeitung auf einer Einwilligung beruht (Art. 6 Abs. 1 Satz 1 lit. a oder Art. 9 Abs. 2 lit. a DS-GVO), das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
Hinweis: Das überschneidet sich mit Art. 7 Abs. 3 DS-GVO.

- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.
Hinweis: Jedenfalls für die Gestaltung der Informationspflicht muss entschieden werden, ob ein Verfahren im Sinne von Art. 22 DS-GVO vorliegt.

Das Zusammenstellen dieser Informationen ist leicht. Es kann jedoch eine Herausforderung darstellen, die Masse der Informationen „unterzubringen". Ein Teil der Pflichtinformationen hiernach überschneidet sich mit den Anforderungen nach Art. 4 Nr. 1 und Artt. 7, 8 DS-GVO. Es wäre eine Förmelei ohne Mehrwert für den

Einwilligenden, wenn die Informationen zwei Mal gegeben werden müssten, nur weil sie in zwei verschiedenen Regelungen genannt sind.

Die Information ist dem Einwilligenden „zum Zeitpunkt der Erhebung" der Daten zu geben. Das bedeutet zunächst, dass die Daten nicht zwingend vor der Einwilligung gegeben werden müssen. Sie müssen allerdings in einem Zusammenhang zur Erhebung geben werden. Die Anforderungen ist damit jedenfalls erfüllt, wenn sie im Rahmen der Eingabemaske oder des Anmeldebuttons gegeben werden.

Kurzum: Die Informationspflicht muss im Zusammenhang mit der Erhebung, aber nicht zwingend davor erfolgen.

Hieraus ergibt sich aber auch, dass die Informationspflicht nicht für Bestandsdaten – also Daten, die vor dem 25.05.2018 erhoben worden sind - nachgeholt werden müssen. Für Bestandsdaten kommt die Regelung zum Zug, wenn neue Daten erhoben werden.

Kurzum: Es gibt keine pauschale Pflicht zur Information derjenigen, die vor dem 25.05.2018 eingewilligt haben.

Wird ein Double-Opt-In-Verfahren eingesetzt und die Bestätigungsanfrage sofort mit Eingabe der Daten versendet, dürfte der Informationspflicht auch genügt sein, wenn die Informationen in der Bestätigungsanfrage enthalten sind. Das gilt jedenfalls für die Informationen nach Art. 13 Abs. 2 DS- GVO (siehe direkt nachfolgend). Wer ganz sicher gehen möchte, sollte diese Informationen auch im Double-Opt-In-Verfahren nochmals geben, selbst wenn sie schon bei der Anmeldung gegeben werden; das ist aber rechtlich nicht zwingend.

Wenn die Einwilligung offline oder am Telefonat eingeholt wird, war zunächst umstritten, ob ein Medienbruch für das zur Verfügung stellen der Informationen nach Abs. 2 zulässig ist (bspw. Information nach Abs. 1 auf der Postkarte mit der Einwilligung und die Informationen nach Abs. 2 durch Verweis auf eine Internetseite

oder sonstige Abrufbarkeit). Dem Gesetz sind keine Anhaltspunkte zu entnehmen, warum es nicht zu einem Medienbruch kommen dürfen sollte.

Dementsprechend haben auch die deutschen Datenschutzaufsichtsbehörden anerkannt, dass die Informationspflicht gestuft erfüllt werden kann (DSK, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), November 2018, Seite 7): „Grundsätzlich ist vom Verantwortlichen zum Zeitpunkt der Datenerhebung über alle Themen nach Art. 13 Abs. 1 und 2 DS-GVO zu informieren. Allerdings besteht schon rein praktisch nicht immer die Möglichkeit, der betroffenen Person alle Informationen aus Art. 13 Abs. 1 und 2 DS-GVO sofort voll-ständig geben zu können, z. B. bei Bestell-Postkarten als Zeitschriften-Beilage, bei Bestellungen am Telefon oder bei Kaufverträgen an Automaten. Die Aufsichtsbehörden unterstützen daher den Vorschlag der Artikel 29-Gruppe (WP 260, S. 17) für ein zweistufiges Informationsmodell."

Kurzum: Die Informationen nach Abs. 1 und Abs. 2 des Art. 13 DS-GVO können auf unterschiedliche Weise gegeben werden.

Da nach Abs. 2 nur die Informationen zu geben sind, „die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten", kann im Einzelfall auch geprüft werden, ob auf einzelne Informationsbestandteile verzichtet werden kann.

8. ABMELDUNG UND WIDERRUF DER EINWILLIGUNG

Wird die Einwilligung widerrufen oder einer gesetzlich zulässigen Verarbeitung widersprochen, wird diese Verarbeitung unzulässig.
Das bedeutet aber nicht, dass die Daten automatisch gelöscht werden müssen. Die personenbezogenen Daten, die zum Nachweis der Rechtmäßigkeit der Verarbeitung bis zum Widerruf bzw. Widerspruch erforderlich sind, dürfen (und sollten) weiterhin gespeichert bleiben (Art. 17 Abs. 1 lit. b, Abs. 3 lit. e DS-GVO). Die Daten müssen erst dann gelöscht werden, wenn die möglichen Ansprüche der betroffenen Person verjährt sind. Eine Verwendung für Direkt-Werbung ist aber nicht mehr zulässig.

Das leuchtet auch ein: Wird bspw. die Einwilligung widerrufen und müssten die personenbezogenen Daten dann sofort vollständig gelöscht werden, hätte der Versender keine Möglichkeit mehr, sich gegen eine Abmahnung der betroffenen Person zu wehren und die Rechtmäßigkeit nachzuweisen.

Kurzum: Der Widerruf der Einwilligung macht die Zusendung von E-Mail-Werbung unzulässig. Allerdings müssen die Daten, welche zum Nachweis der Zulässigkeit der Zusendung erforderlich sind, nicht sofort gelöscht werden.

9. ZULÄSSIGE DAUER DER VERARBEITUNG PERSONENBEZOGENER DATEN

Wie lange dürfen E-Mail-Adressen zur Zusendung von E-Mail-Werbung genutzt werden? Die Frage taucht immer wieder auf. Dabei ist zu unterscheiden, ob eine Einwilligung oder § 7 Abs. 3 UWG zugrunde liegt.

Die deutschen Datenschutzaufsichtsbehörden stellen für die Einwilligung auf Folgendes ab (DSK, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung

der Datenschutz-Grundverordnung (DS-GVO), November 2018, Seite 10): „Die Zivilgerichte sehen bei erteilten Einwilligungen zur werblichen Kontaktaufnahme teilweise keine unbegrenzte Gültigkeit. So hat das LG München I mit Urteil vom 8. April 2010, Az. 17 HK O 138/10, entschieden, dass eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert" und deshalb insoweit keine rechtliche Grundlage mehr ist."

Dem ist zu entnehmen, dass für „genutzte" E-Mail-Adressen kein „Verfallsdatum" besteht. Entscheidend ist vielmehr, dass der BGH bereits klargestellt hat, dass eine Einwilligung keiner Wirksamkeitsbeschränkung unter zeitlichen Aspekten unterliegt (BGH, 01.02.2018, III ZR 196/17, K&R 2018, 310 ff. m. Anm. Eckhardt). Eine Einwilligung ist also wirksam bis zu ihrem Widerruf durch den Einwilligenden oder – sofern dies in der Einwilligung geschieht – bis die auflösende Befristung oder Bedingung eingreift (ausführlicher: Eckhardt, DSK-Orientierungshilfe Direktwerbung: Alles geklärt?, K&R 2019, 289,291).

Denselben Maßstab wollen die deutschen Datenschutzaufsichtsbehörden im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO anlegen (siehe: DSK, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), November 2018, Seite 12): „Wenn nach der Rechtsprechung eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert" und deshalb insoweit keine rechtliche Grundlage mehr ist (siehe hierzu unter 3.5), kann dieser zeitliche Maßstab auch bei der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu den vernünftigen Erwartungen der betroffenen Person eine Orientierung bieten, wenn nach einer langen „Werbepause" die Kontaktdaten der Person plötzlich wieder für eine Werbezusendung verarbeitet werden."

Abgesehen von den bereits hiergegen genannten Gründen spricht auch dagegen, dass die Bestandskundenwerbung nach § 7 Abs. 3 UWG auf „eigene ähnliche" Produkte abzielt und daher insbesondere eine erstmalige Werbung möglich sein muss, wenn das zunächst erworbene Produkt ersetzt werden muss.

10. RECHTE DER BETROFFENEN PERSON: AUSKUNFT, LÖSCHUNG UND DATENPORTABILITÄT

Die betroffenen Personen haben nach Artt. 15 bis 20 DS-GVO umfassende Rechte und Ansprüche. Neu ist vor allem, dass nach Art. 12 DS-GVO vorbereitende Maßnahmen zu ergreifen sind, um die Rechte und Ansprüche zu erfüllen. Das Recht auf Löschung wurde bereits gesondert angesprochen. Neu ist das Recht auf Vergessenwerden, das im Rahmen des E-Mail-Marketings keinen speziellen Anwendungsfall findet, weil es für personenbezogene Daten gilt, die „öffentlich gemacht" wurden.

Das Recht auf Datenportabilität in Art. 20 DS-GVO ist weniger eine datenschutzrechtliche als eher kartellrechtliche Regelung, weil sie den Wechsel von einem Anbieter zu einem anderen erleichtern soll. Das Recht gilt für die personenbezogenen Daten, die die betroffene Person dem Verpflichteten „bereitgestellt" hat. Wann Daten „bereitgestellt" wurden, ist noch nicht eindeutig geklärt. Aufgrund des Wortlauts gilt die Regelung jedenfalls nicht für alle Daten, welche das werbetreibende Unternehmen erhebt. Es wird eine gewisse Form des Hingebens durch die betroffene Person erforderlich sein, um von bereitgestellten Daten ausgehen zu können.

11. SPEZIELLE EPRIVACY-REGELUNGEN

Der Entwurf zu einer ePrivacy-Verordnung aus dem Januar 2017 hatte sich zwischenzeitlich erledigt. Die EU-Kommission hatte in Aussicht gestellt, einen „neuen Anlauf" mit einem neuen Entwurf zu machen. Die kroatische Ratspräsidentschaft hat dennoch am 21.2.2020 einen neuen Entwurf für eine ePrivacy-Verordnung veröffentlicht. Wie es seit Januar 2017 fast jede Ratspräsidentschaft getan hat, die in der Zwischenzeit mehrfach standardmäßig gewechselt hat. Die Erfolgsaussichten dieses Entwurfs sind zum Zeitpunkt der Drucklegung offen.

Die ePrivacy-Verordnung soll inhaltlich die Datenschutzrichtlinie 2002/58/EG ablösen. Sie soll daher auch eine Regelung zur Zusendung von E-Mail-Werbung enthalten und würde damit die Regelungen § 7 Abs. 2 Nr. 3, Abs. 3 UWG ablösen und gegenüber der DS-GVO vorrangige Spezialregelungen enthalten.

Spezialregelungen zum „Messen" des Empfängerverhaltens und zum Profiling/Analysieren des Empfängers/Kunden müssen nicht enthalten sein und waren in dem Entwurf zu einer ePrivacy-Verordnung aus dem Januar 2017 auch nicht enthalten.

DATENSCHUTZ BEAUFTRAGTER

eco bietet mehr
Leistungen und Vorteile für eco-Mitglieder

DATENSCHUTZAUDITS

DATENSCHUTZWORKSHOPS

EXTERNER DATENSCHUTZBEAUFTRAGTER

- Hohe Fachkunde und Praxiserfahrung im Bereich Internet und Telekommunikation durch über 20 Jahre Branchenerfahrung des größten Verbands der Internetwirtschaft in Europa
- Servicepakete "à la carte" (zugeschnitten auf Ihre Bedürfnisse)
- Faire Preise – ab 400,- EUR
- Keine zusätzlichen Kosten für Ausbildungen oder Weiterbildungen von Mitarbeitern
- Keine internen Interessenskonflikte aufgrund anderer Rollen im Unternehmen

eco Service
Externer Datenschutzbeauftragter

Beschäftigen sich in Ihrem Unternehmen zehn oder mehr Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten? Sind Sie fit im Umgang mit Mitarbeiterdaten? Wie transferieren Sie Daten grenzüberschreitend? Erfüllen Sie die Vorgaben der EU-Datenschutzgrundverordnung?

eco bietet Ihnen konkrete Hilfe bei allen datenschutzrelevanten Fragen.

Die meisten Unternehmen der Telekommunikations- und Internetwirtschaft sind gesetzlich verpflichtet einen Datenschutzbeauftragten zu bestellen. eco stellt seinen Mitgliedern diesen auf Wunsch und bietet damit eine professionelle Lösung im Bereich Telekommunikation und Internet, um den Herausforderungen des Datenschutzes zu begegnen, Ihre gesetzlichen Pflichten zu erfüllen, Bußgelder zu vermeiden und Wettbewerbsvorteile zu sichern.

PAKET 1: ECO DATENSCHUTZAUDITS

- Überprüfung und Bewertung Ihrer Datenschutzkonzepte sowie technischer Einrichtungen
- Erstellung eines ausführlichen Ergebnisberichts mit Maßnahmenkatalog
- Vor-Ort-Besichtigungen in Ihrem Unternehmen

PAKET 2: ECO DATENSCHUTZWORKSHOPS

- Praxisnahe Vorträge
- Individuell zugeschnitten auf unterschiedlicheUnternehmensabteilungen
- Sensibilisierung Ihrer Mitarbeiter im Umgang mit personenbezogenen Daten

PAKET 3: EXTERNER DATENSCHUTZBEAUFTRAGTER „RUND UM SORGLOS" (INKL. PAKET 1 & 2)

Das Paket umfasst unter anderem folgende Leistungen:

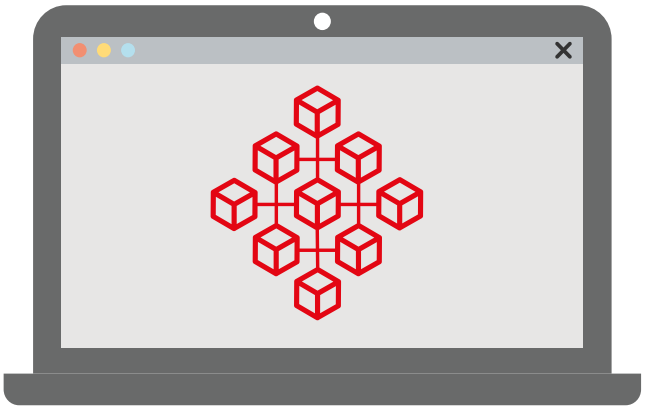
- Stellung des externen betrieblichen Datenschutzbeauftragten für Ihr Unternehmen
- Unterstützung und Beratung der Unternehmensleitung zu Fragen des Datenschutzes und der Datensicherheit sowie der Einhaltung der DS-GVO und anderer datenschutzrechtlicher Vorschriften
- Überprüfung Ihrer datenschutzrelevanten Verfahren
- Erarbeitung von Datenschutzkonzepten
- Durchführung interner Datenschutzaudits
- Datenschutzworkshops

Besuchen Sie uns auf unserer Webseite **datenschutz.eco.de** oder schreiben Sie uns eine E-Mail an **datenschutzbeauftragter@eco.de** und wir nehmen Kontakt zu Ihnen auf.

GDPR Playbook

Blockchain und die Verantwortlichkeit nach der DS-GVO

Klaus Brisch
Nico Winter



A EINFÜHRUNG

Der Begriff „Blockchain" dürfte zu den prominentesten Begriffen der Tech-Szene aus den vergangenen Jahren avanciert sein. Der Blockchain-Technologie werden bisweilen Eigenschaften zugeschrieben, die die Welt verändern können und sollen. Sie verspricht Datensouveränität und die direkte Interaktion zwischen den Beteiligten, ohne Hinzuziehung eines Intermediäres. Die Interaktion beschränkt sich dabei nicht auf Transaktionen, sondern schließt Anwendungen und Prozessabläufe – etwa durch die Nutzung von Smart Contracts — ein, die durch die Architektur der Blockchain-Technologie manipulationssicher, nachvollziehbar und effizient durchführbar werden. Nun ist die auch als Distributed Ledger Technologie bezeichnete Blockchain-Technologie sicherlich revolutionär. Einfügen in die geltenden Rechtsrahmen muss sie sich dennoch.

Ebenfalls von großer Prominenz ist aktuell das Datenschutzrecht. Auch hier gibt es Revolutionen (oder doch nur Evolutionen?), wie etwa die Datenschutz-Grundverordnung (DSGVO). Die DSGVO hat keinen geringeren Auftrag, als die Grundrechte natürlicher Personen zu schützen, indem sie eine unzulässige oder ungewollte Verarbeitung personenbezogener Daten verhindert und für eine zulässige oder erlaubte Datenverarbeitung Sicherheitsregeln aufstellt. Diese Vorgaben haben bereits bei vielen Unternehmen zu tiefgreifenden Veränderungen des Tagesgeschäftes gesorgt, um den datenschutzrechtlichen Anforderungen zu genügen.

Werden personenbezogene Daten im Sinne der DSGVO im Kontext einer Blockchain verarbeitet, unterliegt diese Verarbeitung den Vorgaben des Datenschutzrechtes. Die vielerorts geforderte Ausnahme für die Blockchain gibt es – konsequenter Weise – nicht. Konsequent deswegen, da es auch bei einer Datenverarbeitung unter Einsatz einer Blockchain zu einer Grundrechtsbeeinträchtigung durch eine unzulässige Datenverarbeitung kommen kann. Nun ist die Blockchain-Technologie zu bestimmten Vorgaben und Prinzipien des Datenschutzrechtes ganz besonders auf Kollisionskurs. Hervorzuheben ist dabei die hoch umstrittene Frage, wer

für die Datenverarbeitung im Kontext einer Blockchain als Verantwortlicher im datenschutzrechtlichen Sinne zu sehen ist. Wo es zwischen der Technologie und dem Recht knarzt und wie der aktuelle juristische Meinungsstand zur Frage der Verantwortlichkeit liegt, soll in diesem Beitrag dargestellt werden.

Zunächst werden in diesem Beitrag die technischen Grundlagen der Blockchain-Technologie in gebotener Kürze dargelegt. Anschließend folgt eine Darstellung der Verarbeitung personenbezogener Daten im Blockchain-Kontext. Zuletzt wird eine Einordnung der Netzwerkteilnehmer in das Verantwortlichkeitsgefüge der DSGVO unternommen.

B DIE BLOCKCHAIN

I. Die Technologie

So viel vorab: Es gibt sie nicht, „die eine Blockchain". Überhaupt ist die Blockchain-Technologie eine Technologie, die in verschiedenen Ausprägungen funktionieren kann. Während die grundlegende Technologie unverändert bleibt, kann zwischen verschiedenen Arten der Blockchain unterschieden werden. So gibt es öffentliche, private und konsortiale Blockchains: An öffentlichen Blockchains können grundsätzlich unendlich viele Netzwerkteilnehmer partizipieren, die alle dieselben Berechtigungen haben und Transaktionen validieren können. Eine private Blockchain hingegen steht unter der Kontrolle einer einzelnen Organisation, welche bestimmt wird Zugang zu dieser Blockchain hat. Diesen bekommt in der Regel nur ein ausgewählter und berechtigter Kreis von Netzwerkteilnehmern. Zudem haben nicht alle Teilnehmer die gleichen Berechtigungen innerhalb der Blockchain. Die konsortiale Blockchain wird als geschlossenes System von einem Konsortium kontrolliert, das über den Zugang zu dieser Blockchain bestimmt.

Eine Blockchain lässt sich (vereinfacht) zusammengefasst als verteilte Datenbank beschreiben (Distributed Ledger), die von ihren Nutzern selbst verwaltet wird. Sinn

und Zweck dieser Datenbanken ist es, Informationen, insbesondere Transaktionen, dezentral und unveränderlich abzuspeichern und darzustellen. Dies erfolgt unter Einsatz eines Peer to Peer Netzwerkes. Wird eine Information bzw. Transaktion an das Blockchain Netzwerk übermittelt, wird sie – dezentral – auf allen in diesem Peer to Peer Netzwerk vernetzten Rechnern gespeichert. Dies geschieht in der Weise, dass mehrere Transaktionen in Blöcken ("Blocks") zusammengefasst werden. Diese Blöcke von Informationen werden sodann von den Teilnehmern des Netzwerks selbst nach bestimmten Vorgaben verifiziert. Verifiziert die Mehrheit des Netzwerks die Informationen, wird der gesamte Block verschlüsselt und unveränderlich an einen anderen (zuvor erstellten) Block angehängt. Da jeder neu erstellte Block in der ihm eigenen Identifikationsnummer auch eine Prüfsumme (Header) des vorherigen Blocks enthält, werden die aneinandergehängten Blocks „untrennbar" miteinander verbunden. Durch die Verbindung vieler Blöcke entsteht die Blockchain. Durch die Übernahmen der Prüfsummer des jeweils vorherigen Blocks kann der Inhalt eines Blocks nicht mehr verändert werden, ohne dass dies Auswirkungen auf alle anderen nachfolgenden Blöcke hätte. Dies führt dazu, dass die in der Blockchain gespeicherten Daten faktisch fälschungssicher sind. Um Einträge in der Blockchain (unbemerkt) zu verändern, müsste quasi die gesamte Blockchain verändert werden, damit die Prüfsummen aller nachfolgenden Blöcke wieder korrekt sind.

Es werden stets nur neue Blöcke angehängt, alte jedoch nicht gelöscht. Durch diesen Prozess werden die in der Blockchain gespeicherten Daten immer „nur" ergänzt, aber nicht verändert oder überschrieben. Auf diese Weise bleibt die gesamte Transaktionshistorie für jeden Teilnehmer der Blockchain nachvollziehbar.

II. Protagonisten in der Blockchain-Welt

In der Blockchain-Welt spielen verschiedene Teilnehmer mit. So gibt es die Stelle, die die Blockchain-Struktur in technischer Hinsicht programmiert hat. Da eine Blockchain (wie oben erläutert) ein Peer to Peer Netzwerk ist, bedarf es zur Funktion der Blockchain verschiedener Netzwerkknotenpunkte (sog. Nodes), die ihre Rechenkapazität zur Speicherung der Blockchain zur Verfügung stellen. Die

Blöcke mit den gehashten Werten, aus denen die Chain besteht, werden von den Minern berechnet. Zuletzt gibt es noch die Nutzer, die die Blockchain nutzen, um eine Transaktion ausführen.

Zu beachten ist, dass die Bestimmung der Teilnehmer maßgeblich von dem konkreten Blockchain-Setup abhängt und insofern durchaus variieren kann. So ist es z. B. im Falle einer Private Blockchain üblich, dass es keine Miner gibt, sondern die neuen Blöcke durch einen sog. Validator berechnet werden. Das Basis-Teilnehmer-Setup einer Public-Blockchain dürfte allerdings im Wesentlichen aus den vorgenannten Protagonisten bestehen.

III. Exkurs: Smart Contracts

Eine Blockchain ermöglicht – je nach Programmierung – nicht nur die Abwicklung von Transaktionen, sondern auch das Implementieren von sogenannten Smart Contracts. Hierbei handelt es sich nicht (zwingend) um Verträge im juristischen Sinne, sondern um automatisch ausführbare Programmcodes, die vorgegebene Transaktionsregeln abbilden. Der Smart Contract überprüft, ob alle zuvor festgelegten Bedingungen erfüllt sind. Ist dies der Fall, wird die Transaktion automatisch über die Blockchain abgewickelt. So könnte beispielsweise bei einem mittels Smart Contract geleasten Fahrzeug der Motor nur dann gestartet werden, wenn vorher die Leasingrate gezahlt wurde – eine Bedingung, die der Smart Contract selbstständig überprüft. Durch die Anwendung von Smart Contracts können Prozesse automatisiert werden, wodurch sich die Einschaltung eines Intermediäres erübrigt, was letztlich zu Kosteneinsparungen führt.

C PERSONENBEZOGENE DATEN IN DER BLOCKCHAIN

I. Die Personenbeziehbarkeit von Daten

Die Anwendbarkeit der DSGVO setzt voraus, dass personenbezogene Daten verarbeitet werden. Wann es sich bei einem Datum um ein personenbezogenes Datum handelt, ist in der DSGVO definiert: Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person wir dann als identifizierbar angesehen, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann. Nach der vorstehenden Defintion genügt es also bereits, dass eine Person durch ein bestimmtes Datum identifizierbar ist (z.B. die Religionszugehörigkeit). Die Wahrscheinlichkeit der Identifizierbarkeit steigt bei der Möglichkeit der Verknüpfung und Zusammenführung mit anderen (personenbezogenen) Daten an. Nicht zwingend erforderlich ist, dass ein Datum aus sich heraus direkt eine Person identifiziert (wie. z.B. ein Name).

Nach der Auffassung des Europäischen Gerichtshofes (EuGH)[1] ist eine Identifizierbarkeit bereits dann gegeben, wenn die Identifizierung nur durch Hinzuziehung und Verbindung des in Rede stehenden Datums mit anderen Daten möglich ist. Dabei ist es nicht einmal erforderlich, dass der die Identifizierung Vornehmende direkten Zugriff auf zusätzliche Daten hat. Vielmehr genügt es, wenn dieser gegenüber einem anderen einen Anspruch auf Herausgabe dieser Daten hat.

Danach ist es durchaus möglich, dass ein bestimmtes Datum für den einen Datenverarbeiter als personenbezogenes Datum zu qualifizieren ist, während das exakt gleiche Datum für einen anderen Datenverarbeiter keinen Personenbezug aufweist. Insofern ist das Zusatzwissen bzw. etwaige rechtliche Ansprüche auf Erlangung eines Zusatzwissens der datenverarbeitenden Stelle sowie die Mittel und Möglichkeiten der Erlangung des Zusatzwissens bei der Qualifikation eines Datums als personenbezogen oder nicht personenbezogen miteinzubeziehen.

[1] EuGH, Urt. v. 19.10.2016 - Rs C-582/14 – Breyer./.Bundesrepublik Deutschland

Aus dem Urteil des EuGHs sowie der Definition durch die DSGVO ist der Begriff der Personenbeziehbarkeit weit auszulegen, sodass im Zweifel regelmäßig von einer Personenbeziehbarkeit auszugehen ist.

II. Verarbeitung personenbezogener Daten im Kontext der Blockchain

Die DSGVO findet nur dann Anwendung, wenn im Kontext einer Blockchain personenbezogene Daten verarbeitet werden. In Frage kommen hierbei verschiedene Datenarten bzw. Daten aus verschiedenen Quellen.

1. Verarbeitung von Identifiern

Zunächst kommen all jene Daten in Frage, die zur Bestimmung eines Transaktionsteilnehmers erforderlich sind. Denn trotz aller gewünschter Anonymität und trotz der Ausschaltung eines Intermediäres muss zumindest klar sein, an wen etwas transferiert wird. In der Regel dient der Public-Key dazu, die andere an der Transaktion beteiligte Person zu bestimmen.

> Zum Hintergrund: Jeder Blockchain-Nutzer benötigt zur Durchführung von Transaktionen ein Schlüsselpaar bestehend aus Public- und Private-Key. Dieses Schlüsselpaar besteht jeweils aus einem Hashwert, ist einmalig und wird für den Nutzer vor der ersten Transaktion generiert. Während der Private-Key von dem Nutzer geheim zu halten ist, muss er den Public-Key bekanntgeben, um an Transaktionen teilnehmen zu können. Um eine Transaktion z. B. von A zu B durchzuführen ist es erforderlich, dass A den Public-Key von B kennt. Mit Hilfe dieses Public-Key's können die Transaktionsdaten dergestalt verschlüsselt werden, dass nur B diese wieder entschlüsseln kann, nämlich mit seinem Private-Key. Das Key-Set dient zur Bestimmung des Empfängers und zur Sicherstellung, dass nur der Empfänger die an ihn adressierte Botschaft entschlüsseln kann. Um etwa eine Kryptowährung an einen bestimmten Nutzer zu transferieren, ist es erforderlich, dass dem Sender der Public-Key des Empfängers bekannt ist.

Der Public-Key ist grundsätzlich einem bestimmten Nutzer zugeordnet. Sofern es sich bei dem Nutzer um eine natürliche Person handelt, kann dieser Key als personenbezogen qualifiziert werden, denn dann gehört der eine Key zu einer bestimmten natürlichen Person. Vor dem Hintergrund der oben dargestellten Relativität des Personenbezugs ist die Qualifikation eines Datums als personenbezogen allerdings aus Sicht des Datenverarbeiters zu bestimmen, nicht hingegen aus Sicht der betroffenen natürlichen Person. Nun wäre also die Frage, ob ein Datenverarbeiter, der den Public-Key einer natürlichen Person kennt, die hinter dem Key stehenden Person identifizieren kann.

Betrachtet man einen Public-Key isoliert, kommt man schnell zu dem Ergebnis, dass sich unmittelbar aus dem Key keine Rückschlüsse auf eine natürliche Person ergeben. Ob der Public-Key aus Sicht eine Datenverarbeiters dennoch als personenbezogen qualifiziert werden kann, hängt also maßgeblich davon ab, ob dieser Datenverarbeiter Zugriff auf weitere, mit dem Public-Key in Verbindung stehende Daten hat, die eine Identifizierung des Public-Key-Nutzers erlauben. Auf diese Frage kann keine pauschale Antwort gegeben werden. Vielmehr hängt dies davon ab, ob es sich um eine Private- oder Public-Blockchain handelt und/oder in welchem Kontext die mit dem Public-Key in Verbindung stehende Transaktion erfolgt:

- Bei dem Betrieb einer Private-Blockchain ist eine Nutzeridentifizierung vor Beginn der Nutzung der digitalen Infrastruktur regelmäßig erforderlich. Der Betreiber der Blockchain hat in diesem Fall auch regelmäßig Kenntnis darüber, welche Person welchen Public-Key verwendet. In diesem Fall kann über den Public-Key eine Person identifiziert werden, sodass der Public-Key als personenbezogenes Datum zu qualifizieren ist.

- Bei einer Public-Blockchain ist es maßgeblich, welche Verbindungen eine Transaktion zu einer Leistung oder Handlung außerhalb der Blockchain hat: Wird der Kaufpreis für eine Leistung oder Ware im Rahmen eines Online-Kaufs, etwa durch eine Bitcoin-Transaktion gezahlt, erhält der Empfänger

der Bitcoins neben dem Public-Key des Käufers auch z.B. dessen Rechnungs- oder Lieferanschrift. In diesem Fall ist der Public-Key für den Verkäufer als personenbezogenes Datum zu qualifizieren.

• Für den Betreiber einer Node in einer Public-Blockchain hingegen gibt es weder Anhaltspunkte dahingehend, welche Person hinter einem Public-Key steht, noch hat dieser Node-Betreiber in der Regel eine Möglichkeit zusätzliche Informationen zu erlangen, die in Verbindung mit dem Public-Key eine Person identifizierbar machen.

2. Verarbeitung von Transaktionsdaten

Abgesehen von dem Public-Key kann auch die Transaktion selbst personenbezogene Daten enthalten. Die französische Aufsichtsbehörde CNIL führt hier als Beispiele Eigentumsurkunden oder Zeugnisse an.

Auch bezüglich dieser Daten ist natürlich der relative Ansatz des Personenbezugs maßgeblich. Gerade bei Daten, die in Transaktionen aufgenommen werden, muss sich eine Identifikation der dahinterstehenden natürlichen Person in der Regel aus den Daten selbst ergeben. Dies dürfte bei den vorstehenden Beispielen (Urkunden und Zeugnissen) jedoch unproblematisch sein.[2]

Sofern solche Daten in einer Transaktion enthalten sind, kann dies wiederum Folgen für die Betrachtung des Public-Keys als personenbezogenes Datum haben: Hat ein Node keine Möglichkeit, den Public-Key einer Transaktion einer natürlichen Person zuzuordnen, ergibt sich aber aus weiteren Transaktionsdaten die Identität einer natürlichen Person und ist des weiteren davon auszugehen, dass diese Person identisch ist mit dem Inhaber des Public-Keys, so ist auch der Public-Key als personenbezogenes Datum zu qualifizieren.

[2] CNIL, Blockchain, Solutions for a responsible use of the blockchain in the context of personal data, 06.11.2018, overview on website: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

3. Fazit

Die Frage, ob im Kontext einer Blockchain personenbezogene Daten verarbeitet werden, kann nach dem Vorstehenden nicht allgemein, sondern muss jeweils konkret mit Blick auf den Einzelfall beantwortet werden. Fest steht aber auch, dass die im Rahmen einer Blockchain-Transaktion verarbeiteten Daten personenbezogen sein können, was dazu führt, dass das Datenschutzrecht im Kontext der Blockchain Relevanz hat.

D VERANTWORTLICHKEIT

I. Verantwortlichkeitsgefüge der DSGVO

Nach der DSGVO ist derjenige für eine Datenverarbeitung verantwortlich, der die Zwecke und Mittel der Datenverarbeitung bestimmt. Möglich ist auch eine gemeinsame Verantwortlichkeit. Diese liegt dann vor, wenn mehrere als Verantwortliche zu qualifizierende Datenverarbeiter die Zwecke und Mittel der Datenverarbeitung gemeinsam festlegen.

Zwar befasst mit der Datenverarbeitung aber nicht verantwortlich im Sinne der DSGVO ist der Auftragsverarbeiter. Auftragsverarbeiter ist, wer personenbezogene Daten im Auftrag eines Dritten und auch nur in dem diesbezüglich vorgegebenen Umfang verarbeitet.

Die Qualifizierung als Verantwortlicher oder Auftragsverarbeiter folgt den tatsächlichen Umständen und nicht etwa irgendwelchen vertraglichen Konstrukten. Vielmehr besteht für die an einer Datenverarbeitung beteiligten Instanzen die Pflicht, die tatsächlichen Gegebenheiten vertraglich zutreffend abzubilden.

II. Blockchain und die datenschutzrechtliche Verantwortlichkeit

Die Bestimmung der Rollen der Beteiligten in einer Blockchain-Struktur aus

datenschutzrechtlicher Sicht zählt zu den größten Herausforderungen. Die Zuordnung im Verantwortlichkeitssystem der DSGVO ist stark umstritten. Dieser Umstand liegt maßgeblich darin begründet, dass die Blockchain strukturell so aufgebaut ist bzw. sein soll, dass der alles kontrollierende (verantwortliche) Intermediär nicht erforderlich ist. Aus datenschutzrechtlicher Sicht ist die Bestimmung des Verantwortlichen jedoch zwingend.

Bei der Bestimmung der Verantwortlichkeit sind alle Player im Kosmos der Blockchain zu betrachten. Diejenige Stelle, die die Blockchain programmiert hat, Teilnehmer/ Nutzer des Blockchain-Netzwerkes, die Nodes oder die Miner der Blockchain. Auch bei der Suche nach dem Verantwortlichen ist zwischen Public- und Private-Blockchain Strukturen zu unterscheiden. Während eine Public-Blockchain nicht nur dezentral strukturiert, sondern auch nicht dezentral gesteuert wird, gibt es bei einer Private-Blockchain in der Regel eine zentrale Verwaltungs- oder Zulassungsstelle. Diese beiden Varianten sind aus rechtlicher Sicht daher differenziert zu betrachten.

III. Verantwortlichkeit in einer Public-Blockchain

Bei einer Public-Blockchain fehlt es denklogisch an einer kontrollierenden Instanz, die den Betrieb der Blockchain verantwortet. Aus diesem Grund sind die einzelnen Protagonisten des Netzwerks zu betrachten, wenn es um die Frage der Verantwortlichkeit geht.

1. Programmierer der Datenbank

Auch bei einer Public-Blockchain gibt es eine die Blockchain initiierende Stelle, welche die erste Version der Blockchain programmiert. Die Stelle, die die Datenbank entwickelt, verarbeitet jedoch keine personenbezogenen Daten im Rahmen der Anwendung dieser Datenbank. Insofern kommt eine Verantwortlichkeit nicht in Betracht.

2. Miner

Die Miner sind als Rechenmaschine der Blockchain hauptsächlich damit befasst, neue Blöcke der Kette zu errechnen. Zwar sind davon mitunter personenbezogene Daten tangiert, jedoch ohne dass diese in irgendeiner Form direkt verarbeitet werden. Mitunter werden die Miner mit Telekommunikationsdienstleistern verglichen. Auch bei dem Signaltransport kommt es zu einer Weiterleitung personenbezogener Daten von A nach B, ohne dass dieser Transport der Daten durch Telekommunikationsdienstleister als Datenverarbeitung qualifiziert wird.

Die französische Datenschutzaufsichtsbehörde „CNIL" vertritt die Auffassung, dass Miner gegebenenfalls als Auftragsverarbeiter zu qualifizieren sind, da diese eine Datenverarbeitung „auf Weisung" durchführen. Dies hätte zur Folge, dass der Abschluss eines Auftragsverarbeitungsvertrages verpflichtend wäre, was in der anonymen Realität der Blockchain jedoch zu erheblichen Schwierigkeiten führen dürfte.

3. Nodes/Blockchain Teilnehmer

Anders als der Entwickler der Datenbank hat eine Node bzw. ein Teilnehmer des Netzwerkes Schreib- und Leserechte und ist in die Durchführung einer Transaktion dergestalt eingebunden, dass sie bzw. er der Kette neue Blocks hinzufügt. Zudem übermittelt eine Node die Transaktionsdaten an andere Nodes. Da eine Transaktion personenbezogene Daten enthalten kann, wird vermehrt der Standpunkt vertreten, dass Nodes als Datenverarbeiter verantwortlich für eben diese Datenverarbeitung sind, sofern sie diese Daten in das Netzwerk einbringen.

Diese weit verbreitete Auffassung deckt sich mit der Auffassung der CNIL, wonach derjenige als Verantwortlicher für eine Datenverarbeitung gilt, der personenbezogene Daten zu Zwecken einer Transaktion in die Datenbank einpflegt. Dabei, so die CNIL zutreffend, ist eine Ausnahme zu machen, wenn diese Datenverarbeitung nicht im Zusammenhang mit einer beruflichen oder kommerziellen Tätigkeit erfolgt. Die Durchführung einer Transaktion durch eine Privatperson würde demnach nicht zu

einer datenschutzrechtlichen Verantwortlichkeit dieser Person führen.

Verschiedentlich wird zudem die Auffassung vertreten, dass alle Nodes gemeinsam verantwortlich für die Datenverarbeitung sind. Dies setzt allerdings voraus, dass die Nodes die Zwecke und Mittel der Datenverarbeitung gemeinsam festlegen, woran es regelmäßig fehlen dürfte. Zwar arbeiten Nodes in einer Vielzahl mit anderen Netzwerkknotenpunkten zwingend zusammen, da dies eine Mindestanforderung für die Funktion eines Peer to Peer Netzwerkes ist. Jedoch erfolgt diese Zusammenarbeit weder nach Absprache, noch haben die Nodes gegenseitig die Möglichkeit, Einfluss auf die Datenverarbeitung anderer Nodes auszuüben. Eine gemeinsame Verantwortlichkeit aller Nodes ist daher abzulehnen.

4. Fazit

Unter Beachtung der Auffassung der französischen Datenschutzaufsichtsbehörde und der aktuellen herrschenden Meinung in der juristischen Literatur sind die Nodes bzw. Teilnehmer eines Blockchain-Netzwerkes dann als Verantwortliche zu qualifizieren, wenn diese zu selbst festgelegten Zwecken und mit eigenen Mitteln Daten in die Blockchain einbringen und diese Datenverarbeitung nicht nur privaten Zwecken dient.

Die für die Erstellung neuer Blöcke zuständigen Miner sind hingegen nicht verantwortlich im Sinne der DSGVO, können aber unter Umständen Auftragsverarbeiter sein.

IV. Verantwortlichkeit in einer Private-Blockchain

Anders als in einer für jeden Nutzer offen zugänglichen Blockchain hat eine Private Blockchain die Eigenschaft, dass sie entweder zulassungsbeschränkt ist oder bzw. und zentral gesteuert und verwaltet wird.

Setzt etwa ein Unternehmen eine Blockchain-Lösung für die interne Logistik ein, ist die Frage der Verantwortlichkeit schnell geklärt. Gleiches gilt für eine Konsortial-Blockchain, bei der der Zutritt zur Blockchain von einer vorherigen Autorisierung durch eine zentrale Stelle abhängt. Eine solche Blockchain-Lösung kommt etwa im Bereich der Energiewirtschaft in Frage.

In beiden Varianten werden die Zwecke und Mittel der Datenverarbeitung im Kontext der Blockchain zentral dann durch das Unternehmen bzw. durch ein Gremium des Konsortiums bestimmt. In diesem Fall gibt es eine zentralisierte Stelle, die für die Datenverarbeitung im Sinne der DSGVO verantwortlich ist. Ein Abstellen auf Nodes oder Miner ist in diesem Fall verfehlt.

E FAZIT

Die Frage nach der Verantwortlichkeit im Kontext einer Blockchain ist sicherlich noch nicht final beantwortet. Dies gilt insbesondere für die Public-Blockchain. Zwar werden bestimmte Auffassungen, etwa die Zuteilung der Verantwortlichkeit an eine Nodes bzw. den einzelnen Teilnehmer, mittlerweile vermehrt vertreten. Dennoch fehlt hier bislang eine belastbare Stellungnahme etwa von dem Europäischen Datenschutzausschuss. Im Rahmen einer Private Blockchain ist die Frage der Verantwortlichkeit stets eine Frage der konkreten Ausgestaltung bzw. der Struktur eines Blockchain-Netzwerkes. Dennoch gibt es in einem solchen Setup sehr häufig eine zentrale Stelle, die über die Datenverarbeitung bestimmt und daher als Verantwortlicher im datenschutzrechtlichen Sinne fungiert.

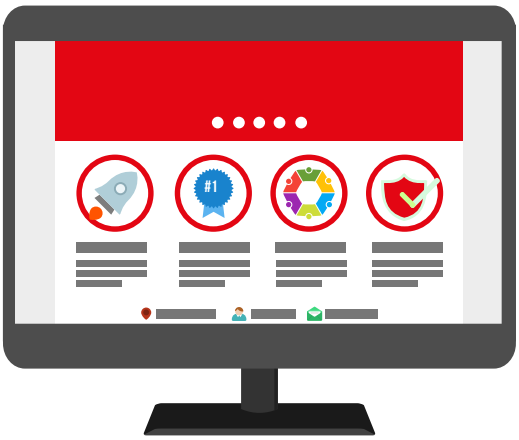
Ein Auszug aus dem Buch
„DSGVO für Website-Betreiber“,
von Christian Solmecke und Sibel Kocatepe

GDPR Playbook

DSGVO FÜR WEBSITE-BETREIBER

Ihr Leitfaden für die sichere Umsetzung der EU-Datenschutz-Grundverordnung

Christian Solmecke
Sibel Kocatepe



2.5 DATENSCHUTZ-FOLGENABSCHÄTZUNG

Gänzlich neu trifft Sie unter Umständen die in Art. 35 DSGVO geregelte Datenschutz-Folgenabschätzung. Datenschutz-Folgenabschätzung bedeutet konkret, dass Sie in manchen Fällen im Voraus eine Abschätzung vornehmen müssen, welche Folgen die vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten haben könnte. Wann dies der Fall ist und wie eine solche Schätzung abzulaufen hat, erläutern wir Ihnen im Folgenden.

2.5.1 IN WELCHEN FÄLLEN IST EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCHZUFÜHREN?

Eine Datenschutz-Folgenabschätzung ist nach Art. 35 Abs. 1 DSGVO immer dann durchzuführen, wenn ein Datenverarbeitungsverfahren aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt. Dies ist insbesondere bei der Verwendung neuer Technologien der Fall. Daher soll gemäß Art. 35 Abs. 3 DSGVO eine Datenschutz-Folgenabschätzung insbesondere dann erfolgen, wenn

- es sich um Technologien handelt, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten,

- eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten erfolgt oder

- systematisch eine umfangreiche Überwachung öffentlich zugänglicher Bereiche stattfinden soll.

Da die zuvor erläuterten Fälle einer notwendigen Folgenabschätzung nur Regelbeispiele sind, damit keinesfalls abschließend, soll die Aufsichtsbehörde den Verantwortlichen darin unterstützen, abschätzungsbedürftige Datenverarbeitungsvorgänge zu ermitteln. Der europäische Gesetzgeber erlegt den Aufsichtsbehörden in Art. 35 Abs. 4 und 5 DSGVO daher die Pflicht auf, eigene Listen der Verarbeitungsvorgänge zu erstellen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (sogenannte Blacklist) bzw. für die gerade keine Datenschutz-Folgenabschätzung erforderlich ist (sogenannte Whitelist).

Dieser Pflicht zur Erstellung von Black- und Whitelists ist die Artikel-29-Datenschutzgruppe, ein Zusammenschluss der europäischen Aufsichtsbehörden, nachgekommen. Sie hat am 4. April 2017 die »Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ›likely to result in a high risk‹ for the purposes of Regulation 2016/679« (WP 248 17/EN) veröffentlicht, an denen Sie sich orientieren können.

Hinweis

Die Artikel-29-Datenschutzgruppe, (engl. Article 29 Data Protection Working Party) ist das unabhängige Beratungsgremium der EU-Kommission in datenschutzrechlichen Fragestellungen. Die rechtliche Grundlage dieser Gruppe geht auf die europäische Datenschutzrichtlinie zurück (95/46/EG), die inzwischen durch die Datenschutz-Grundverordnung ersetzt wurde. Diese neue Gesetzeslage hat zudem zur Folge, dass seit dem 25. Mai 2018 die Art. 29-Datenschutzgruppe durch ihren Rechtsnachfolger, den Europäischen Datenschutzausschuss, abgelöst wurde. Dieser besteht jedoch derzeit noch nur auf dem Papier. Hier sollten Sie weitere Entwicklungen mitverfolgen – auch im Hinblick auf die Frage, ob der Europäische Datenschutzausschuss der bisherigen Rechtsauffassung der Artikel 29-Datenschutzgruppe folgen wird.

Die Empfehlungen beinhalten dabei sowohl Beispiele für Verfahren, bei denen eine Datenschutz-Folgenabschätzung erforderlich sein soll, als auch Vorschläge zur Dokumentation der erforderlichen Prüfung.

Die Arbeitsgruppe sieht beispielsweise eine Datenschutz-Folgenabschätzung für die automatische Analyse von Nutzerverhalten auf Social-Media-Kanälen als grundsätzlich erforderlich an. Weiterhin soll eine Folgenabschätzung auch dann vorgenommen werden, wenn Mitarbeiter im Hinblick auf ihr Nutzungsverhalten von IT-Systemen überwacht werden sollen. Nicht abschätzungsbedürftig seien dagegen beispielsweise Datenverarbeitungen beim bloßen Versand von Newslettern.

Hinweis

Inzwischen haben auch die einzelnen nationalen Aufsichtsbehörden die ersten Whitelists für die Datenschutz-Folgenabschätzung auf ihren Internetplattformen veröffentlicht. Als Orientierung sind die Listen geeignet, lassen aber noch viel Raum für Unsicherheiten, da sie weder einheitlich noch vollständig sind. Nach Angaben der Aufsichtsbehörden solle vielmehr der Verantwortliche – also Sie – im Wege einer Vorabprüfung bewerten, ob eine Verarbeitungstätigkeit einer Datenschutz-Folgenabschätzung bedarf oder nicht. Für diese Prüfung wird in den Dokumenten eine weitere Liste bereitgestellt, welche Kriterien bei der Prüfung heranzuziehen sind.
Ein Beispiel einer solchen Whitelist können Sie der Liste nach Art. 35 Abs. 4 DSGVO aus Baden-Württemberg[1] entnehmen:

1. Bewerten oder Einstufen (Scoring)
(»Evaluation or scoring«)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
(»Automated decision making with legal or similar significant effect«)
3. Systematische Überwachung
(»Systematic monitoring«)
4. Vertrauliche oder höchst persönliche Daten
(»Sensitive data or data of a highly personal nature«)
5. Datenverarbeitung in großem Umfang
(»Data processed on a large scale«)
6. Abgleichen oder Zusammenführen von Datensätzen

(»Matching or combining datasets«)
7. Daten zu schutzbedürftigen Betroffenen
(»Data concerning vulnerable data subjects«)
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
(»Innovative use or applying new technological or organisational solutions«)
9. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert
(»When the processing in itself prevents data subjects from exercising a right or using a service or a contract«)

Sie sollten sich an der Whitelist der für Sie zuständigen Behörde orientieren. Bisher wurden folgende Listen veröffentlicht:

- Baden-Württemberg, abrufbar unter *https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorgängen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf*
- Thüringen, abrufbar unter *https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf*
- Schleswig-Holstein, abrufbar unter *: https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf*
- Rheinland-Pfalz, abrufbar unter *https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_OE.pdf*
- Saarland, abrufbar unter *https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/Download/dsfa_muss_liste_dsk_de.pdf*
- Hamburg, abrufbar unter *https://datenschutz-hamburg.de/dsgvo-information/art-35-mussliste-nicht-oeffentlich/*
- Niedersachsen, abrufbar unter *https://lfd.niedersachsen.de/download/131098*
- Berlin, abrufbar unter *https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/datenschutzfolgeabschaetzung/BlnBDI-2018-DSFA-nicht-oeffentlich.pdf*

• Brandenburg, abrufbar unter *https://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.596771.de*

• Bundesdatenschutzbeauftragte, abrufbar unter https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html?cms_templateQueryString=Datenschutz+folgenabschätzung&cms_sortOrder=score+desc

Beachten Sie dabei jedoch, dass es sich keinesfalls um abschließende Listen handeltund diese ständig aktualisiert werden. Dies bedeutet für Sie, dass Sie auch an dieser Stelle ständig die neusten Entwicklungen mitverfolgen müssen.

Sofern die für Sie zuständige Behörde noch keine Liste veröffentlicht hat, sollten Sie auch dies im Blick behalten. Denn es ist zu erwarten, dass sich das kurzfristig noch ändern wird.

2.5.2 WIE IST DAS VERFAHREN DURCHZUFÜHREN UND WAS BEINHALTET ES?

In der Praxis erfolgt die Folgenabschätzung in einem dreistufigen Verfahren, in das Sie gemäß Art. 35 Abs. 2 DSGVO – sofern vorhanden – den Datenschutzbeauftragten einbeziehen müssen. Dieses Verfahren, das sich maßgeblich an Art. 35 Abs. 7 DSGVO orientiert, möchten wir Ihnen im Folgenden erläutern.

Auf der ersten Stufe ist zunächst eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Verarbeitungszwecke vorzunehmen. Sofern Sie sich bei der Datenverarbeitung auf ein berechtigtes Interesse zur Datenverarbeitung ohne Einwilligung stützen, dann muss auch dies berücksichtigt werden. Weiterhin müssen Sie eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der

Verarbeitungsvorgänge in Bezug auf den genannten Zweck durchführen, um im Ergebnis zu entscheiden, ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht.

Wenn ein solches Risiko besteht, müssen Sie auf der zweiten Stufe eine Bewertung dahingehend vornehmen, ob die von Ihnen im konkreten Fall geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren ausreichen, um den Schutz der Daten zu gewährleisten. Sie müssen auch nachweisen, dass durch Ihre Maßnahmen und Vorkehrungen die Regelungen der europäischen Datenschutz-Grundverordnung eingehalten werden und dass Sie den Interessen der Betroffenen Rechnung tragen.

Kommen Sie dabei zu dem Ergebnis, dass die Datenverarbeitung ein hohes Risiko zur Folge hätte, müssen Sie gemäß Art. 36 DSGVO auf der dritten Stufe die Aufsichtsbehörde konsultieren, wenn Sie keine Maßnahmen zur Eindämmung des Risikos treffen.

Die Aufsichtsbehörde kann dann grundsätzlich innerhalb von 8 Wochen eine schriftliche Empfehlung an Sie aussprechen, wenn sie der Ansicht ist, dass die geplanten Verfahren nicht in Einklang mit den Datenschutzgesetzen stehen.

Hinweis
Das Konsultationsverfahren schützt Sie nicht vor anderen aufsichtsrechtlichen Befugnissen der Behörde. Diese kann weiterhin Datenschutzüberprüfungen in Ihrem Unternehmen durchführen, auf vermeintliche Datenschutzverstöße hinweisen und ein Verbot des Verarbeitungsvorgangs erlassen!

Die einzelnen Schritte der Datenschutz-Folgenabschätzung, ihren Inhalt und ihr Ergebnis sollten Sie schriftlich dokumentieren, um im Streitfall oder im Rahmen aufsichtsbehördlicher Untersuchungen nachweisen zu können, dass Sie das Verfahren dem Gesetz entsprechend durchgeführt und gegebenenfalls erforderliche Konsequenzen daraus gezogen haben.

Hinweis
Es kann unter Umständen zweckmäßig sein, die Dokumentation der Datenschutz-Folgenabschätzung mit dem Verzeichnis über die Verarbeitungstätigkeiten zu verknüpfen.

2.6 AUFTRAGSVERARBEITUNG

Dass Daten von Unternehmen nicht nur intern verarbeitet werden, ist weder praktisch noch rechtlich neu. Vielmehr steigt die immense wirtschaftliche Bedeutung des Outsourcings: Einerseits werden Datenverarbeitungen gemeinsam mit ganzen Arbeitsprozessen insgesamt ausgelagert. Andererseits werden die Datenmengen, mit denen Unternehmen in ihren täglichen Prozessen umgehen müssen, auf externen Speichern verwaltet.

Neu ist bei dem Ganzen nun die rechtliche Lage: Die Datenschutz-Grundverordnung hat ebenso wie das neue Bundesdatenschutzgesetz eine Vielzahl der Regelungen zur Auftragsverarbeitung (vormals »Auftragsdatenverarbeitung«) reformiert. Was genau das nun für Sie bedeutet, möchten wir Ihnen in diesem Abschnitt näher erläutern.

2.6.1 WAS IST AUFTRAGSVERARBEITUNG?

Unter einem Auftragsverarbeiter versteht der europäische Gesetzgeber laut Art. 4 Nr. 8 DSGVO »eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet«. Die Auftragsverarbeitung zeichnet sich demnach nach der europäischen Definition lediglich durch das Auftragsverhältnis aus, ohne auf weitere Merkmale aus dem Innenverhältnis wie Weisungsgebundenheit oder Verantwortlichkeiten abzustellen. Demnach sind eigenverantwortliches Handeln und eigene Entscheidungsspielräume

des Auftragsverarbeiters durchaus zulässig.

Hinweis: Vergleich zur alten Rechtslage
Damit unterscheidet sich die neue europäische Definition deutlich von dem früheren deutschen Verständnis einer Auftragsdatenverarbeitung i.S.d. § 11 BDSG a.F., wonach der für die jeweilige Dienstleistung bzw. Datenverarbeitung eingeschaltete Auftragnehmer tatsächlich nur unterstützend tätig werden durfte. Er durfte also gegenüber dem Auftraggeber lediglich Hilfstätigkeiten ohne eigenen Entscheidungsspielraum hinsichtlich der verarbeiteten Daten erbringen. Aufgrund dieses Verständnisses erfolgte nach der alten Rechtslage eine Abgrenzung zur sogenannten Funktionsübertragung auf den Auftragnehmer mit der Folge, das dieser selbst als datenschutzrechtlich verantwortliche Stelle anzusehen war. Eine solche Differenzierung ist nun jedoch obsolet, wodurch zum Beispiel auch der besonders relevante Bereich des Cloud Computings durchaus unter die Definition der Auftragsverarbeitung gefasst werden kann.

2.6.2 WO SPIELT AUFTRAGSVERARBEITUNG EINE ROLLE?

Das Outsourcing von Arbeitsprozessen und damit auch von Datenverarbeitungen prägt heute in weiten Teilen das Alltagsgeschehen in fast allen Unternehmen. Aus Kostenoder Know-how-Gründen werden immer mehr einzelne Prozesse und teilweise auch ganze Aufgabenbereiche an externe Dienstleister ausgelagert, zum Beispiel an Callcenter zur Kundenbetreuung, an externe Agenturen zur Durchführung von Marketingaktionen oder an externe Lohnbuchhaltungen.

Insbesondere im IT-Bereich nimmt die Auftragsverarbeitung beispielsweise durch Einschaltung externer Wartungsdienstleister und Rechenzentren sowie durch die wachsende Nutzung von Cloud-Services rasant zu. Denn für Unternehmen bedeutet die Auslagerung von Daten eine deutliche Einsparung von Kapazitäten auf mehreren

Ebenen. Große unternehmensinterne Rechen- und IT-Zentren müssen nicht mehr bereitgehalten werden. Große Investitionen entfallen damit ebenso vollständig wie die Wartung der Hardware und die Sicherung sowie das regelmäßige Updaten der Software. Diese Aufgaben werden zusammen mit den betreffenden Daten an den Cloud-Anbieter ausgelagert. Die Bereitstellung ebenso wie die anschließende Abrechnung erfolgt dann bedarfsabhängig, ohne ständig laufende Kosten zu erzeugen. Das bedeutet gleichzeitig bessere Organisationsmöglichkeiten und mehr Flexibilität.

2.6.3 WORIN BESTEHT DIE RECHTLICHE PROBLEMATIK?

Diese besondere Konstellation der Datenverarbeitung durch einen externen Auftragnehmer ist im Hinblick auf die Verantwortlichkeit für die Einhaltung datenschutzrechtlicher Regelungen nicht unproblematisch. Da mit der Aufgabenübertragung regelmäßig auch eine Übermittlung von personenbezogenen Daten etwa der Kunden oder Mitarbeiter des auslagernden Unternehmens verbunden ist, entsteht in datenschutzrechtlicher Hinsicht ein dringlicher Regelungsbedarf hinsichtlich der Fragen, welches Unternehmen für den Schutz der verarbeiteten Daten verantwortlich ist und welche Maßnahmen hierfür erforderlich sind. In der Konsequenz betrifft dies auch die Frage, wer gegenüber Aufsichtsbehörden und Betroffenen haftet, wenn es zu Datenschutzverstößen kommt. Dieses Problem verschärft sich zudem dann, wenn die Daten zur Auftragsverarbeitung ins Ausland transferiert werden. Auf diese Fragen gibt nun der europäische Gesetzgeber in der Datenschutz-Grundverordnung ebenso eine Antwort wie der deutsche Gesetzgeber im neuen Bundesdatenschutzgesetz.

2.6.4 WELCHE REGELUNGEN GELTEN BEI DER AUFTRAGSVERARBEITUNG?

Die Auftragsverarbeitung ist in der europäischen Datenschutz-Grundverordnung in Art. 28 und Art. 29 DSGVO geregelt. Die Datenschutz-Grundverordnung normiert damit den Rahmen der Zulässigkeit einer Datenverarbeitung durch beauftragte Dritte. Möchten Sie demnach einen Auftragsverarbeiter einsetzen, dann ist es gemäß Art. 28 Abs. 1 DSGVO Ihre Pflicht, nur mit solchen Auftragsverarbeitern zu kooperieren, »die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet«.

Hinweis
Diese Pflicht hat der deutsche Gesetzgeber mit einer ähnlichen Formulierung auch noch einmal in § 62 Abs. 2 BDSG kodifiziert und damit deren Wichtigkeit unterstrichen.

Als Beleg für eine solche Qualität des von Ihnen beauftragten Unternehmens können Sie zum Beispiel Zertifizierungen anführen, die im Rahmen eines Datenschutzaudits erteilt werden.

Darüber hinaus ist auch nach dem neuen europäischen Datenschutzrecht eine Auftragsverarbeitung nur dann zulässig, wenn die Zusammenarbeit auf einem schriftlich oder – neuerdings auch in elektronischer Form – abgefassten Vertrag zur Auftragsverarbeitung basiert. Wie ein solcher Vertrag aussieht, können Sie zudem in unserem Muster in Abschnitt 5.4 sehen.

Insgesamt ähneln die neuen Regelungen der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes den Vorgaben des § 11 BDSG a.F. Auch wenn viele Aspekte dabei bereits bekannt sind und beibehalten wurden, wird der

Auftragsverarbeiter nun durch die Vorgaben des Art. 28 Abs. 3 DSGVO stärker in die Pflicht genommen, für die Einhaltung der Datenschutzregelungen zu sorgen. Denn anders als nach den Regelungen des früher geltenden Bundesdatenschutzgesetzes ist der Auftragsverarbeiter seit der Reform für die Datenschutzkonformität der Verarbeitungsprozesse mitverantwortlich.

Daraus ergibt sich für ihn zum Beispiel die Pflicht,

- einen Vertreter zu bestimmen (Art. 27 Abs. 1 DSGVO),
- ein Verzeichnis aller von ihm getätigten Verarbeitungen zu erstellen (Art. 30 Abs. 2 DSGVO),
- mit der Datenschutzaufsicht zusammenzuarbeiten (Art. 31 DSGVO),
- die technischen und organisatorischen Maßnahmen der Datensicherheit einzuhalten (Art. 32 Abs. 1 DSGVO) oder
- die allgemeinen Grundsätze der Datenübermittlung in Drittländer oder an internationale Organisationen zu beachten (Art. 44 DSGVO).

2.6.5 WELCHE KONSEQUENZEN HAT EIN VERSTOSS DES AUFTRAGSVERARBEITERS?

In den Fällen, in denen sich der Auftragsverarbeiter nicht an Ihre Weisungen hält (indem er zum Beispiel die Daten abredewidrig verarbeitet oder erforderliche Sicherheitsmaßnahmen nicht beachtet), wird er selbst gemäß Art. 28 Abs. 10 DSGVO als Verantwortlicher behandelt und haftet damit voll und eigenständig für die Konsequenzen aus den Datenschutzverstößen. Er wird demnach so behandelt, als hätte das Auftragsverhältnis zwischen Ihnen und ihm nicht bestanden, was zur Folge hat, dass der eigentliche Auftragsverarbeiter mit Geldbußen von bis zu 20 Millionen Euro oder 4 % des Umsatzes des vergangenen Geschäftsjahres rechnen muss – je nachdem, welcher Betrag höher ist.

Hinweis

Dieser Haftung können Auftragsverarbeiter auch nicht durch einen vollständigen Haftungsausschluss in ihren Allgemeinen Geschäftsbedingungen entgehen, da ein solcher unwirksam ist.

Ganz grundsätzlich haftet der Auftragsverarbeiter gemäß Art. 82 Abs. 2 S. 2 DSGVO für den durch die Datenverarbeitung entstandenen Schaden nämlich nur dann, wenn er einer ihm speziell auferlegten Pflicht nicht nachgekommen ist oder Ihre rechtmäßig erteilten Anweisungen für die Datenverarbeitung nicht beachtet oder diesen zuwiderhandelt. Von dieser Haftung kann sich der Auftragsverarbeiter nur dann befreien, wenn er beweisen kann, dass »er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist«, so Art. 82 Abs. 3 DSGVO.

2.7 DATENTRANSFER IN DRITTSTAATEN

Der Datentransfer ins außereuropäische Ausland betrifft insbesondere die Inanspruchnahme ausländischer Cloud-Dienste (siehe Abbildung 2.4) und stellt dessen Nutzer vor die Frage, wie es in diesen Fällen eigentlich mit dem Datenschutz aussieht: Welches Datenschutzrecht findet Anwendung und wie kann Datenschutz für betroffene EU-Bürger garantiert werden?

Zu diesen und anderen Fragen in Bezug auf den Datentransfer ins außereuropäische Ausland, sogenannte Drittstaaten, hat sich auch der europäische Gesetzgeber im Zuge der Reformen Gedanken gemacht.

Da die europäische Datenschutz-Grundverordnung einen einheitlichen Datenschutz-Standard gewährleisten soll, kann dieser am besten garantiert werden, wenn die Datenverarbeitung in einem der Mitgliedstaaten der Europäischen Union erfolgt. Doch in einer globalisierten und digitalisierten Welt ist diese Vorstellung wohl uto-

pisch. Dies weiß auch der europäische Gesetzgeber. Er hat daher den Datentransfer in Drittstaaten zum Schutz der EU-Bürger bestimmten Einschränkungen unterworfen, die in Art. 44 ff. DSGVO normiert sind.

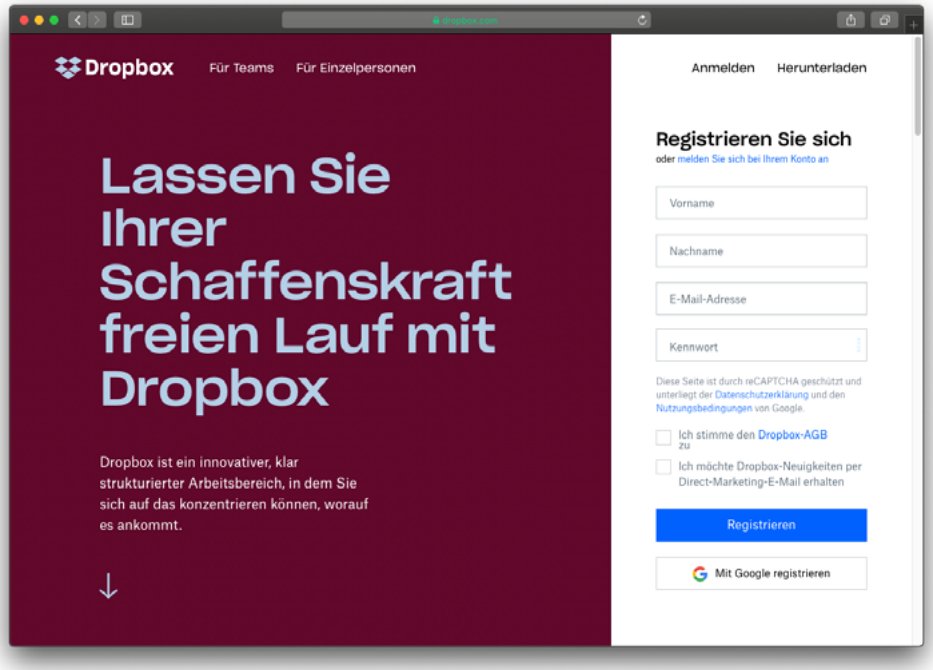


Abbildung 2.4 Dropbox ist eine beliebte Cloud mit Sitz in den USA – einem Drittstaat.

Hinweis

Wir empfehlen Ihnen ganz grundsätzlich, für die Übermittlungen von personenbezogenen Daten in Drittstaaten möglichst umfassend Verschlüsselungen einzusetzen und die Schlüsselverwaltung möglichst in der Europäischen Union durchzuführen.

2.7.1 UNTER WELCHEN BEDINGUNGEN IST EIN DATENTRANSFER IN DRITTSTAATEN ZULÄSSIG?

Ob personenbezogene Daten in einem konkreten Einzelfall in Drittstaaten überführt werden dürfen, wird auf Basis eines zweistufigen Verfahrens beurteilt (sogenannter Zwei-Stufen-Test). Danach ist Grundvoraussetzung, dass die allgemeinen Anforderungen an eine rechtskonforme Datenübermittlung erfüllt werden. Folglich muss entweder eine Einwilligung des Betroffenen oder ein anderer gesetzlicher Erlaubnistatbestand für die Übermittlung personenbezogener Daten vorliegen (siehe Abschnitt 2.3).

Erst wenn die erste Stufe ergibt, dass dies sichergestellt werden kann, wird auf der zweiten Stufe geprüft, ob die spezifischen Voraussetzungen für einen Datentransfer in Drittstaaten entsprechend den Art. 44 ff. DSGVO vorliegen. Entscheidend ist dabei, dass das Datenschutzniveau am Zielort dem europäischen Schutzniveau entspricht. Denn ein Großteil der Software in Drittstaaten ist nicht mit dem europäischen Recht kompatibel und weist große Defizite auf. Aus diesem Grund sieht Art. 45 Abs. 1 DSGVO vor, dass personenbezogene Daten grundsätzlich nur dann an ein Drittland übertragen werden dürfen, wenn die Europäische Kommission beschlossen hat, dass dieses Land ein angemessenes Schutzniveau bietet. Man spricht dabei auch von einem sogenannten »Angemessenheitsbeschluss «. Zudem muss der Betroffene über den Transfer seiner Daten ins Ausland mindestens informiert werden.

Praxistipp
Zur Information des Betroffenen bietet sich die Datenschutzerklärung an, der die Betroffenen zustimmen sollten, bevor Sie mit der Datenverarbeitung und dem Datentransfer beginnen.

2.7.2 IN WELCHE DRITTSTAATEN IST EIN DATENTRANSFER ZULÄSSIG?

Welche Länder einen Standard gewährleisten, der dem europäischen Schutzniveau entspricht, entscheidet die Europäische Kommission per Beschluss. Sie veröffentlicht diesen Beschluss im Amtsblatt der Europäischen Union und auf ihrer Website.

Hinweis

Die Website der Europäischen Kommission mit Informationen zum Datenschutz erreichen Sie über *https://ec.europa.eu/info/law/law-topic/data-protection_en (siehe Abbildung 2.5).*

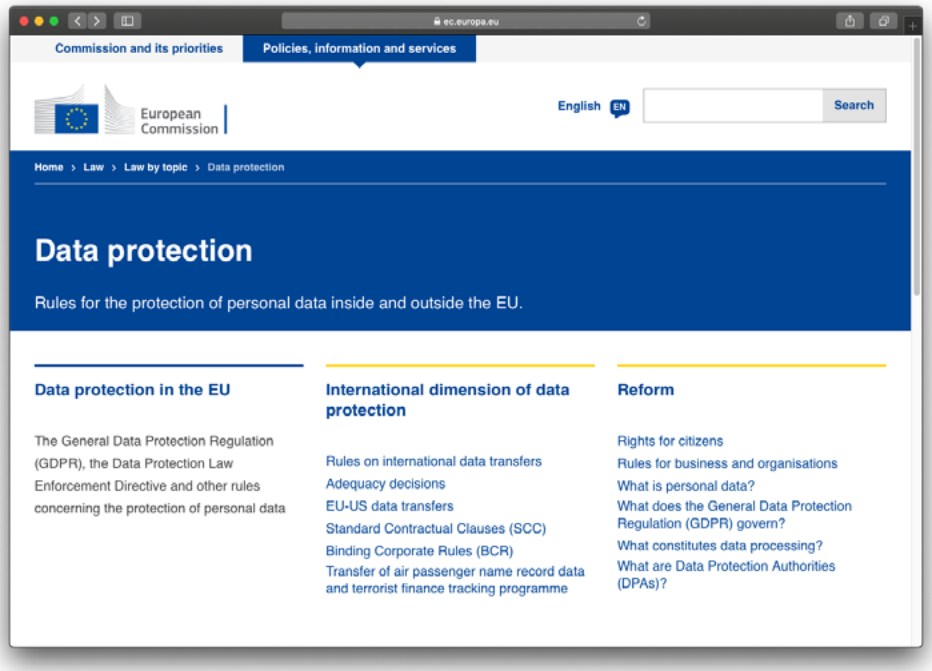


Abbildung 2.5 Die Website der Europäischen Kommission

Bei dieser Beurteilung untersucht die Kommission, ob das jeweilige Land im Hinblick auf ein bestimmtes Gebiet bzw. einen bestimmten Sektor oder in einer

speziellen Datenkategorie ein dem europäischen Standard entsprechendes Schutzniveau gewährleistet. Diese Einschätzung erfolgt dann einerseits auf Grundlage eigener nationaler Datenschutzregelungen und einer effektiven Durchsetzung der Regelungen durch Aufsichtsbehörden sowie andererseits durch eingegangene internationale Verpflichtungen. Diese Voraussetzungen erfüllen derzeit beispielsweise die Schweiz, Kanada, Argentinien, Israel, Australien oder Neuseeland, nicht jedoch beispielsweise Japan, Indien und China.

Hinweis: USA

Auch die USA gehörten zwischenzeitlich zu den unsicheren Drittstaaten. Denn der Europäische Gerichtshof (Urteil vom 06.10.2015, Az. C-362/14) hatte entschieden, dass das sogenannte Safe-Harbor-Abkommen ungültig sei, weil es nicht den geltenden gesetzlichen Voraussetzungen entspreche. Insbesondere seien die Daten durch das Abkommen nicht genügend vor den US-amerikanischen Geheimdiensten geschützt gewesen.

Zu einem neuen Datenschutzabkommen zwischen Europa und den USA kam es dann mit dem Privacy-Shield-Abkommen, dessen endgültige Fassung die Kommission am 12.07.2016 offiziell als Angemessenheitsentscheidung verabschiedete. Bei dem Privacy-Shield-Abkommen handelt es sich ebenso wie bei seinem Vorgänger nicht um ein rechtsverbindliches Abkommen, sondern eher um einen rechtlichen Rahmen, zu dessen Einhaltung sich Unternehmen in den USA seit dem 01.08.2016 verpflichten können, indem sie sich in die sogenannte Privacy-Shield-Liste eintragen.

Achtung: Brexit!

Ein Gedanke, an den viele sich noch gewöhnen müssen, ist der, dass Großbritannien bald nicht mehr zur Europäischen Union gehört – dies hat auch Konsequenzen für den Datenschutz. Gemäß einer Mitteilung der Europäischen Kommission vom 9.1.2018 ist das Vereinigte Königreich ab dem 30.3.2019 als Drittland im Sinne der Datenschutz-Grundverordnung zu behandeln, für das dann erst einmal noch kein Angemessenheitsbeschluss

besteht. Bis ein solcher Beschluss ergeht, steht Großbritannien auf einer Stufe mit Ländern wie China oder auch Russland. Von einem Datentransfer nach Großbritannien sollten Sie daher in der Zwischenzeit besser Abstand nehmen, wenn Sie nicht die andernfalls erforderlichen Garantien vorweisen können, die wir Ihnen im Folgenden erläutern werden.

2.7.3 IST EIN DATENTRANSFER IN UNSICHERE DRITTSTAATEN AUCH OHNE KOMMISSIONSBESCHLUSS ZULÄSSIG?

Wenn Sie Daten in Drittländer übertragen möchten, für die kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, können Sie dies gemäß Art. 46 Abs. 1 DSGVO tun, wenn Sie mit geeigneten Garantien die Einhaltung des europäischen Datenschutzniveaus vorsehen und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Welche Garantien dies sein können, hat der Gesetzgeber in Art. 46 Abs. 2 DSGVO geregelt. Danach sind beispielsweise sogenannte Binding Corporate Rules oder Verträge zwischen Auftraggeber und Auftragsverarbeiter unter Verwendung der bestehenden Standarddatenschutzklauseln der Europäischen Kommission ebenso effektive Garantien wie nun auch europäische Zertifizierungen.

2.7.4 KANN EIN DATENTRANSFER IN DRITTSTAATEN AUCH OHNE ANGEMESSENHEITSBESCHLUSS UND OHNE GARANTIEN ERFOLGEN?

Ausnahmen von dem Erfordernis eines Kommissionsbeschlusses oder geeigneter Garantien hat der europäische Gesetzgeber ebenfalls vorgesehen und diese in Art. 49 DSGVO normiert. Danach ist ein solcher Datentransfer zum Beispiel dann zulässig,

wenn die von der Datenverarbeitung betroffene Person in die Datenübermittlung ausdrücklich eingewilligt hat, nachdem sie umfassend und transparent über die damit verbundenen Risiken – insbesondere im Hinblick auf die Durchsetzung von Betroffenenrechten – und ihr jederzeitiges Widerrufsrecht belehrt wurde. Dies ist in der Praxis wohl der bedeutendste Ausnahmefall innerhalb des eng auszulegenden Ausnahmekatalogs. Darüber hinaus ist eine Datenübermittlung unter anderem auch dann unter bestimmten Voraussetzungen zulässig, wenn die Datenübermittlung zur Vertragserfüllung im Interesse der betroffenen Person erforderlich ist oder wichtigen öffentlichen Interessen, lebenswichtigen Interessen des Betroffenen oder berechtigten Interessen des Verantwortlichen dient.

Das Buch „**DSGVO für Website-Betreiber**“ ist erschienen im Rheinwerk Verlag und hier erhältlich
https://www.rheinwerk-verlag.de/dsgvo-fur-website-betreiber_4801/

Ein Auszug aus dem Buch
„**DSGVO für Website-Betreiber**“,
von Christian Solmecke und Sibel Kocatepe

GDPR Playbook

Leitfaden zur Erstellung eines Datensicherheitskonzepts

Christian Solmecke
Sibel Kocatepe

5.6 LEITFADEN ZUR ERSTELLUNG EINES DATENSICHERHEITS-KONZEPTS

Hinweis

Die Formulierung eines Datensicherheitskonzepts erfordert ein hohes Maß an technischem, wirtschaftlichem und juristischem Wissen. Eine große Zahl von Details muss beachtet werden, um ein Maximum an Sicherheit zu gewährleisten. Die Erstellung eines solchen Konzepts ist folglich sehr komplex und bedarf einer ordentlichen Strukturierung und Detailgenauigkeit, um seinen Zweck als Sicherheitsleitlinie erfüllen zu können. Im Folgenden möchten wir Ihnen einen Leitfaden zur Erstellung eines Sicherheitskonzepts an die Hand geben. Dieser Leitfaden beschränkt sich ebenso wie das Muster zum Datenschutzkonzept lediglich auf den Aufbau eines solchen Konzepts und enthält keine Formulierungsvorschläge, da Konzepte grundsätzlich sehr individuell auf die jeweiligen Datenverarbeitungsprozesse in jedem einzelnen Unternehmen abgestimmt werden müssen und daher inhaltlich nicht verallgemeinert werden können.

1. DEFINITIONEN

Damit beim Lesen und Umsetzen des Sicherheitskonzepts alle Beteiligten von derselben Basis ausgehen, bietet es sich an, das Konzept mit einem Katalog von Definitionen der fachlichen Begriffe zu beginnen, die in dem Konzept eine besondere Bedeutung haben und einheitlich verwendet werden müssen. Beispiele für wichtige Begriffe, die Sie – auch unter Hinzuziehung gesetzlicher Definitionen – näher bestimmen sollten, sind:

- Daten
- Personenbezogene Daten
- Anwendungsdaten
- Systemdaten

- Protokolldaten
- Software
- Verarbeitung
- Datenschutz
- Datensicherheit
- Datensicherung
- Katastrophenschutz
- Vollsicherung
- inkrementelle Sicherung
- differenzielle Sicherung
- Verlässlichkeit
- (sowie bei Bedarf weitere Begriffe)

2. ZWECK DES SICHERHEITSKONZEPTS

Das eigentliche Konzept sollte dann mit einer Beschreibung des Zwecks bzw. des Ziels und der Motivationslage des Leitfadens beginnen, da dies die Basis der folgenden Sicherungsmaßnahmen ist. Allgemein beschrieben ist der Zweck eines solchen Konzepts die Dokumentation der Sicherheitsleitlinien in einem Unternehmen und der in Bezug darauf ergriffenen technischen und organisatorischen Maßnahmen. Weiterhin kann das Konzept im Rahmen einer aufsichtsbehördlichen Prüfung als Anhaltspunkt für den Datensicherheitsstandard in einem Unternehmen herangezogen werden. Dieser Punkt sollte eher allgemein und nicht zu detailliert formuliert werden. Er bleibt in der Regel auch dann bestehen, wenn sich Änderungen bei den Regelungen zu den einzelnen Verfahren ergeben. Typische Motivationslagen sind zum Beispiel die Abhängigkeit der unternehmerischen Tätigkeit vom Datenbestand sowie der Schutz vor Risiken wie Anwenderfehlern, Hackerangriffen, Hardwarefehlern oder Schadensfällen im eigenen Haus, die zur Beschädigung oder gar zum Verlust der Daten führen können.

3. DARSTELLUNG DER EINFLUSSFAKTOREN

An dieser Stelle Ihres Konzepts sollten Sie darstellen, von welchen Faktoren die Sicherheit in Ihrem IT-System beeinflusst wird. Dabei kommen verschiedene Parameter in Betracht, die im Folgenden beispielartig aufgelistet werden:

- Datenspezifikation
- Rekonstruktionsaufwand ohne Datensicherung
- Vertraulichkeitsbedarf
- Integritätsbedarf
- Datenvolumen
- Änderungsvolumen und Änderungszeitpunkte
- Kenntnisse und Fähigkeiten der IT-Anwender
- (sowie bei Bedarf weitere Faktoren)

4. BESCHREIBUNG DER RISIKOLAGE

Ein Sicherheitskonzept sollte auch immer einen Passus enthalten, der allgemeine Sicherheitsrisiken ebenso beschreibt wie konkrete Gefährdungslagen in dem jeweiligen Unternehmen.

Allgemeine Sicherheitsrisiken sind dabei zum Beispiel Gefahren durch:

- unbewusstes menschliches Fehlverhalten wie falsche Bedienungen aufgrund fehlender IT-Anwenderkenntnisse oder Versehen
- bewusstes menschliches Fehlverhalten wie Cyberangriffe oder Sabotage
- technische Komplikationen wie Hardwareprobleme
- höhere Gewalt wie Feuer, Überschwemmungen oder Erdbeben
- (sowie eventuell weitere Risiken)

5. DATENSICHERUNGSPLAN

Dieser Punkt des Konzepts sollte eine Erläuterung der Verfahren enthalten, die die Geschäftsführung des Unternehmens zur Datensicherheit plant. Dabei wird allgemein zwischen drei Varianten unterschieden:

- der Volldatensicherung, bei der alle Daten zu einem bestimmten Zeitpunkt auf einem Datenträger gespeichert werden und bei der auch bei erneuten Datensicherungen eine vollständige Sicherung der Daten erfolgt

- der inkrementellen Datensicherung, die im Anschluss an die vorhergehende Volldatensicherung erfolgt und bei der nur die Daten gesichert werden, die sich seit der letzten Sicherung verändert haben

- der differenziellen Datensicherung, bei der zwar ebenfalls als Erstes eine Volldatensicherung erfolgt, jedoch die veränderten Daten immer nur in Bezug zur Vollsicherung gespeichert werden

Dabei müssen Sie zunächst die Datenart festlegen und danach einen Plan aufstellen, der verschiedene Aspekte berücksichtigt, wie die Art der Datensicherung, die Häufigkeit und den Zeitpunkt der Datensicherung, das Datensicherungsmedium oder den Aufbewahrungsort für das Speichermedium. Weiterhin sollte der Datensicherungsplan auch Informationen zur Vorgehensweise bei Datenrestaurierungen und zu Restaurierungsübungen sowie zu den Randbedingungen für die Archivierung der Daten enthalten. Weiterhin sollten Sie auch einplanen, dass Ihr Unternehmen ein arbeitsfähiges Lesegerät für die gespeicherten Daten bereithält und Mitarbeiter zur Datensicherung verpflichtet sowie erforderliche Schulungen vornimmt.

6. TECHNISCHE, ORGANISATORISCHE UND PERSONELLE SICHERHEITSREGELUNGEN

Der letzte Punkt des Sicherheitskonzepts stellt letztlich die geplante Reaktion auf die zuvor im Konzept dargestellten Aspekte in Form von technischen, organisatorischen und personellen Maßnahmen dar. Er ist damit eine Spiegelung des theoretischen Konzepts in die Praxis. Dieser Teil des Sicherheitskonzepts enthält einerseits eine allgemeine Beschreibung der Regelungen zur Datensicherung und andererseits eine Darstellung der technischen Umsetzung dieser allgemeinen Regelungen. Der Aufwand, den Sie für technische, organisatorische und personelle Maßnahmen betreiben, muss in einem angemessenen Verhältnis zum Schutzzweck stehen.
Zu den zahlreichen möglichen technischen Maßnahmen gehören zum Beispiel neben der Erstellung eines Datenbestandsverzeichnisses und der Regelung der Vorgehensweise zur Wiederherstellung der Daten auch die folgenden technischen Kontrollmechanismen:

- Zutrittskontrollen (z. B. Sicherung des Gebäudes bzw. der Räume)
- Zugangskontrollen (z. B. Authentifizierungsverfahren)
- Zugriffskontrollen (z. B. Benutzerkennung mit Passwort)
- Weitergabekontrollen (z. B. Verschlüsselungen)
- Eingabekontrollen (z. B. Benutzeridentifikation)
- Auftragskontrollen (z. B. Stichprobenprüfungen)
- Verfügbarkeitskontrollen (z. B. Brandschutzmaßnahmen)
- Trennung der Verarbeitungsprozesse (z. B. getrennte Datenbanken)

Organisatorisch erforderlich ist zum Beispiel die Benennung von Verantwortlichen für jeden Aufgabenbereich und die Ermittlung des Bedarfs an Vertraulichkeit, Integrität und Verfügbarkeit. Personell sinnvolle Sicherheitsmaßnahmen sind beispielsweise Schulungen der Mitarbeiter zur Durchführung einer zuverlässigen und kompetenten Datensicherung sowie datenschutzbezogene Geheimhaltungs-

und Verpflichtungserklärungen. Dieser Teil des Konzepts bezieht sich letztlich auf die einzelnen Verfahren innerhalb eines Unternehmens, weshalb es nötig sein kann, diesen gegebenenfalls von Zeit zu Zeit anzupassen.

GDPR Playbook

Verantwortung im Datenschutz

Jan Philip Lutterbach
Matthias Bendixen
Kirstin Dauber

EINLEITUNG

Wie in allen rechtlichen Belangen stellt sich auch im Datenschutzrecht die Frage, wer sich um die Einhaltung der rechtlichen Verpflichtungen überhaupt kümmern muss. Diese Frage dürfte eng mit der Frage nach der Haftung im Falle eines Verstoßes gegen bestimmte Anforderungen verknüpft sein. Im Hinblick auf die rechtlichen Anforderungen, die die Datenschutzgrundverordnung (DS-GVO) an Unternehmen stellt, gilt es insoweit zunächst zu klären, welcher der an der Verarbeitung von Daten Beteiligten auch rechtlich verantwortlich im Sinne des Gesetzes ist und somit haftet, falls etwas fehlschlägt.

Auch wenn die DS-GVO bereits seit Mai 2018 in Kraft ist, bestehen in der Praxis weiterhin große Unsicherheiten wie die jeweiligen Datenverarbeitungsvorgänge umgesetzt werden müssen. Die DS-GVO stellt die Unternehmen dabei vor einige, neue wie alte, Herausforderungen, die von jedem Unternehmen bewältigt werden müssen. Diese Anforderungen treffen zwar größtenteils den sogenannten Verantwortlichen (Art. 4 Nr. 7 DS-GVO), aber auch der sogenannte Auftragsverarbeiter, der im Auftrag des Verantwortlichen tätig wird (Art. 4 Nr. 8 DS-GVO), soll durch die Regelungen der Verordnung stärker in die Verantwortung genommen werden als dies noch unter Geltung der ehemaligen Richtlinie 95/46/EG der Fall gewesen ist. Insoweit besteht für jedes Unternehmen - gerade auch im Hinblick auf die Haftung - das Bedürfnis die eigene Rolle in Bezug auf die stattfindenden Datenverarbeitungen zu identifizieren und mit der erforderlichen (vertraglichen) Grundlage zu versehen.

Dieser Beitrag soll dabei helfen, die Rollen der jeweils an der Verarbeitung beteiligten Parteien anhand von anschaulichen Beispielen aus der Praxis zu definieren. Dabei wird ein besonderes Augenmerk auf die Zusammenarbeit zwischen Unternehmen innerhalb einer Gruppe oder eines Konzerns gelegt.

A. UNTERSCHEIDUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER

Im Rahmen der Datenspeicherung und -verarbeitung spielt vor allem die Unterscheidung zwischen Verantwortlichen und Auftragsverarbeitern eine große Rolle, da an diese Stellungen unterschiedliche Anforderungen gestellt werden und sie durch unterschiedliche Pflichten und Haftungsrisiken gekennzeichnet sind.

Während die „für die Verarbeitung Verantwortlichen" die gesamte Verantwortung für die Verarbeitung personenbezogener Daten tragen, handeln die „Auftragsverarbeiter" lediglich im Auftrag und nach Weisung der Verantwortlichen und tragen dementsprechend eine geringere eigene Verantwortung. Eine richtige Einordnung der an der Verarbeitung personenbezogener Daten Beteiligten in diese Kategorien ist folglich sehr wichtig[1]. Die Bezeichnung der Beteiligten, zum Beispiel im Rahmen eines Vertrages, bestimmt jedoch nicht allein die rechtliche Stellung. Vielmehr ergibt sich diese aus den tatsächlichen Umständen[2]. Insoweit muss der Vertrag den tatsächlichen Umständen folgen. Um die jeweilige Stellung von den Beteiligten richtig einordnen zu können, müssen die Begriffe daher zunächst definiert werden.

I. Verantwortlicher

Verantwortlich sind diejenigen juristischen oder natürlichen Personen, Behörden, Einrichtungen oder andere Stellen, die eigenverantwortlich und unabhängig die Entscheidungen über den Zweck, also den Grund weshalb die personenbezogenen Daten überhaupt verarbeitet werden, sowie über die Art und Weise der Datenverarbeitung und schließlich auch über die Art der Daten selbst treffen[3].

[1] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 7.
[2] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 11.
[3] Paal/ Pauly: Datenschutz-Grundverordnung Bundesdatenschutzgesetz; 2. Aufl. 2018, Art. 4; Rdnr. 55.

1. Beispielsfälle

Beispiele für eine bestehende Verantwortlichkeit des datenverarbeitenden Beteiligten sind regelmäßig die Erhebung und Verarbeitung der Personaldaten der angestellten Mitarbeiter im Unternehmen in Form einer Personalakte. Hier bestimmt das Unternehmen, welches den Mitarbeiter angestellt hat, darüber, welche Daten es von seinen Mitarbeitern erhebt und verarbeitet, auch wenn dies teils durch rechtliche Vorgaben mitbestimmt ist. Jedenfalls verarbeitet das Unternehmen die Daten seiner Beschäftigten im eigenen Interesse im Rahmen der Personalführung, etwa um die Vergütung zu zahlen oder um den digitalen Arbeitsplatz des Mitarbeiters einrichten zu können.

Auch die Verarbeitung von Kundendaten im Rahmen von Kaufverträgen, wo das verkaufende Unternehmen ebenfalls ein eigenständiges Interesse an der Verarbeitung der Daten hat und über die Verarbeitung bestimmt, begründet eine Verantwortlichkeit in diesem Sinne.

Ein anderes Beispiel, welches eine Verantwortlichkeit begründet und nicht auf Vertragserfüllung fußt, ist die Verwendung von E-Mail-Adressen zum Versand eines Newsletters. Hier bestimmt das werbende Unternehmen über die Mittel und Zwecke der Verarbeitung der E-Mail-Adressen (Marketing) und ist somit verantwortlich für die Verarbeitung.

2. Was muss der Verantwortliche tun?

a) Information

Der Verantwortliche hat den Betroffenen umfassend über die Verarbeitung der personenbezogenen Daten zu informieren, sofern diese Daten bei dem Betroffenen selbst (Art. 13 DS-GVO) oder bei einer anderen Person erhoben wurden (Art. 14 DS-GVO). Diese Informationen haben in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu erfolgen. Zudem müssen diese Informationen dem Betroffenen unverzüglich, also ohne unbillige oder schuldhafte Verzögerung, mitgeteilt werden[4]. Unter gewissen Umständen

[4] Heckmann/Paschke in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 12, Rdnr. 32.

ist jedoch auch eine Fristverlängerung möglich. Dies soll sicherstellen, dass jeder Betroffene in die Lage versetzt wird, seine Rechte geltend machen zu können. Die Information muss bei Erhebung der Daten erfolgen; soweit die Daten, etwa im Online-Shop oder über ein Kontaktformular, über eine Webseite erhoben werden, eignet sich hierfür die Datenschutzerklärung der Webseite.

Für die Information der Beschäftigten empfiehlt es sich entsprechend Datenschutzerklärungen vorzuhalten, die den Beschäftigten bei Vertragsschluss zur Verfügung gestellt werden.

b) Umsetzung geeigneter technischer und organisatorischer Maßnahmen

Die Folge einer Klassifizierung als Verantwortlicher ist weiter, dass er als vorwiegender Normenadressat in vollem Umfang unmittelbar verantwortlich und dazu angehalten ist, die Anforderungen der DS-GVO zu befolgen, zu interpretieren, die Konformität sicherzustellen, im Unternehmen praxisorientiert umzusetzen und seine Datenverarbeitungen aktuell zu halten. Er ist also für die Einhaltung der Datenschutzbestimmungen zuständig und wird zur Rechenschaft gezogen, wenn diese nicht eingehalten werden.

Das heißt, der Verantwortliche muss insgesamt für die Rechtmäßigkeit der Datenverarbeitung einstehen. Dies umfasst neben der Rechtmäßigkeit der Verarbeitung eines Datums zu einem bestimmten Zweck auch die Einrichtung und Aufrechterhaltung konkreter Maßnahmen, die die Einhaltung des Datenschutzes fördern, in technischer aber auch organisatorischer Sicht. Hierunter fällt zum Beispiel neben der Einrichtung und Prüfung von Berechtigungskonzepten für den Zugriff von Mitarbeitern auf Daten auch die Schulung der Mitarbeiter in datenschutzrechtlicher Sicht.

Bedient sich der Verantwortliche einer Stelle, welche die Daten im Auftrag des Verantwortlichen verarbeitet (Outsourcing), so hat er diesen sorgfältig auszuwählen und zu überwachen, da ihn dies nicht von der allgemeinen Verantwortung für die Rechtmäßigkeit der Verarbeitung entbindet.

c) Regelmäßige Überprüfung und Aktualisierung

Weiterhin hat der Verantwortliche seine eingesetzten technischen und organisatorischen Maßnahmen bei Bedarf zu überprüfen und zu aktualisieren. Anlässe für Überprüfungen stellen regelmäßig Gesetzesänderungen oder Änderungen in der Datenverarbeitung selbst dar[5].

d) Nachweispflicht (Rechenschaftspflicht)

Der Verantwortliche muss gemäß Art. 24 Abs. 1 S. 1 DS-GVO einen Nachweis über die Rechtmäßigkeit der Datenverarbeitung und die Wirksamkeit der dafür eingesetzten technischen und organisatorischen Maßnahmen, zum Beispiel durch ein Datenschutz-Management- System, erbringen. Hierzu ist es auch möglich die in Art. 40 DS-GVO näher bezeichneten Verhaltensregeln bzw. die in Art. 42 DS-GVO beschriebenen Zertifizierungsverfahren heranzuziehen[6].

II. Auftragsverarbeiter

Auf der anderen Seite gibt es die Stellung als Auftragsverarbeiter. Der Auftragsverarbeiter ist ein eigenständiger und vom Verantwortlichen abweichender Beteiligter, der auf Grundlage eines Vertrages personenbezogene Daten lediglich im Auftrag des Verantwortlichen und nicht selbst als Verantwortlicher verarbeitet. Dies kann sowohl ein Mitarbeiter des Verantwortlichen als auch ein eigenständiges externes

[5] Bertermann in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 24, Rdnr. 8.
[6] Bertermann in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 24, Rdnr. 11.

Unternehmen sein[7]. Der Auftragsverarbeiter zeichnet sich durch starke Weisungsgebundenheit gegenüber dem Verantwortlichen und mangelnder selbstständiger Entscheidungsbefugnis bezüglich der Zwecke und der Mittel der Verarbeitung aus, wobei der Verantwortliche dem Auftragsverarbeiter die Entscheidung über die Mittel auch übertragen kann. Hierbei darf es sich jedoch nicht, um Entscheidungen über wesentliche Aspekte der Mittel handeln, da diese Entscheidungen ausschließlich von dem Verantwortlichen zu treffen sind[8]. Der Auftragsverarbeiter kann jedoch alleine über die technischen und organisatorischen Mittel der Datenverarbeitung entscheiden, ohne dass er dadurch Verantwortlicher wird[9].

1. Beispielsfälle

Softwareunternehmen, die anderen ihre Software in der Cloud oder als Software-as-a-Service bereitstellen, sind regelmäßig nicht für die von ihrem Kunden verarbeiteten Daten zuständig, sondern fungieren als Auftragsverarbeiter, da sie die mit der Software verarbeiteten Daten nicht nach eigenem Ermessen verarbeiten können, sondern regelmäßig nur weisungsgebunden handeln, um die Software vertragsgemäß zur Verfügung zu stellen.

Ein weiteres Beispiel ist die Einschaltung eines Callcenters zum Abtelefonieren einer vom Auftraggeber zur Verfügung gestellten Kundenliste mit genauen Vorgaben zum Anruf oder als erste Anlaufstelle für Kundenanfragen. Das Callcenter hat dabei keinerlei eigene Entscheidungsbefugnis darüber welche Daten verarbeitet werden oder wie dies geschieht und darf die Kundendaten ausschließlich für den durch das auftraggebende Unternehmen vorgegebenen Zweck verarbeiten.

Beauftragt ein Unternehmen ein Drittunternehmen mit der technischen Wartung der eigenen IT-Infrastruktur erhält das Drittunternehmen auch Zugriff auf alle im System gespeicherten Daten und verarbeitet insoweit auch diese enthaltenen personenbezogenen Daten. Da die Verarbeitung durch das beauftragte Drittunternehmen ausschließlich dem angewiesenen Zweck - Wartung der Systeme - dient, handelt es sich um eine Auftragsverarbeitungssituation.

[7] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 30.
[8] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17.
[9] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17.

2. Was muss getan werden?

Der Auftragsverarbeiter schließt mit dem Verantwortlichen einen Vertrag in schriftlicher[10] oder elektronischer Form. Dieser Vertrag muss den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, sowie die Art der personenbezogenen Daten, die Kategorien Betroffener und die Pflichten und Rechte des Verantwortlichen festschreiben (Art. 28 Abs. 3 S. 1 DS-GVO).

Darf der Auftragsverarbeiter allein oder weit überwiegend allein über die eingesetzten Mittel der Datenverarbeitung entscheiden, so muss der Verantwortliche vom Auftragsverarbeiter zwar nicht im Detail, aber wenigstens über die wichtigsten Charakteristika informiert werden[11].

B. GEMEINSAM VERANTWORTLICHE (JOINT CONTROLLER)

Es gibt jedoch auch die Möglichkeit, dass mehrere Verantwortliche zusammen über die Datenverarbeitung entscheiden[12]. Art. 26 Abs. 1 DS-GVO zufolge ist von gemeinsam Verantwortlichen auszugehen, wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und die Mittel der Datenverarbeitung festlegen. Hierfür ist erforderlich, dass jeder der Beteiligten bestimmenden Einfluss auf die Datenverarbeitung hat, nicht aber, dass auch jeder Beteiligte Kontrolle über jeden Verarbeitungsschritt hat oder alle Beteiligten gleichrangigen Einfluss haben. Besonderes Augenmerk ist dabei auf die gemeinsame Festlegung des Zweckes der Verarbeitung zu legen. Auch hier sind die Rollenbezeichnungen im Vertrag regelmäßig nur ein Indiz und immer die tatsächlichen Beziehungen zueinander ausschlaggebend[13].

Hiervon strikt abzugrenzen ist der Fall, dass mehrere Verantwortliche selbstständig nebeneinander handeln. In einem solchen Fall ist jeder von ihnen nur für seine Datenverarbeitung verantwortlich und hat keinerlei Einflussmöglichkeiten auf bzw.

[10] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 32.
[11] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 34.
[12] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 22.
[13] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 23.

Kenntnis von der Datenverarbeitung des anderen. Es werden lediglich Daten untereinander ausgetauscht ohne dass gemeinsame Zwecke und Mittel vorliegen[14]. Ein Beispiel für eine solche Konstellation ist regelmäßig dann gegeben, wenn ein Unternehmen seine Forderungen an ein Inkassounternehmen abtritt, welches in der Folge personenbezogene Daten des Betroffenen zum Zwecke der Durchsetzung (dann) eigener Forderungen verarbeitet.

1. Beispielsfälle

a) Gruppenunternehmen

Häufig sind Unternehmen Teil einer Unternehmensgruppe innerhalb derer verschiedene Funktionen zentralisiert durch ein Gruppenunternehmen für die anderen Gruppenunternehmen übernommen werden. Hierzu finden Sie unter „D. Problemstellung bei der Datenverarbeitung im Konzernverbund" weitere Informationen.

b) Personalvermittler mit eigenem Pool an Bewerbern

Sind Personalvermittler laut Vertrag „im Auftrag" von Unternehmen auf der Suche nach geeigneten Bewerbern, sichten sie regelmäßig neben den Bewerbungen, die bei dem jeweiligen Unternehmen eingehen auch ihren eigenen Pool an Bewerbern, um die Wahrscheinlichkeit eines Vertragsabschlusses zu erhöhen.
Im Verhältnis zu dem jeweiligen Unternehmen sind sie zwar im Auftrag tätig. Im Verhältnis zu den einzelnen Bewerbern sind sie jedoch als Verantwortliche anzusehen, weil sie über die Zwecke und Mittel der Datenverarbeitung entscheiden. Es liegt somit eine gemeinsame Verantwortlichkeit vor[15].

c) Facebook Fanpage

Viele Unternehmen pflegen verschiedene Social-Media-Kanäle für ihre digitale Außendarstellung. Hierunter fallen häufig auch Facebook Fanpages. Hierzu hat der Europäische Gerichtshof mit Urteil vom 05. Juni 2018 entschieden, dass eine

[14] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 24.
[15] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 23.

gemeinsame Verantwortlichkeit zwischen dem Fanpagebetreiber und Facebook Inc. für das Erheben und Übermitteln von Daten an Facebook Inc. bestehe. In der Sache ging es darum, dass Facebook Cookies auf dem Rechner der Besucher einer Fanpage setzte, welche mit den Anmeldedaten solcher Nutzer, die bei Facebook Inc. registriert sind, verknüpft werden konnten.

Auszugsweise lautet das Urteil wie folgt:
"Es ist festzustellen, dass im vorliegenden Fall in erster Linie die Facebook Inc. [...] über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheiden, die die auf Facebook unterhaltenen Fanpages besucht haben, und somit unter den Begriff des „für die Verarbeitung Verantwortlichen" [...] fallen, [...].[16] "

Dennoch kommt das Gericht zu dem Ergebnis, dass eine gemeinsame Verantwortlichkeit gegeben sei, da der Fanpagebetreiber durch Einrichten der Fanpage einen Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung leiste. Dies auch, weil der Fanpagebetreiber die mittels der eingesetzten Cookies erhobenen Analysedaten im Wege der Parametrierung mitgestalten könne.

Weiter heißt es:
"Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien."

2. Was muss getan werden?

a) Joint Controller Agreement

Vertraglich geregelt werden muss dabei, wer welche Aufgabe wahrnimmt, die ihm nach der Verordnung obliegen, und wer insbesondere die für die Erfüllung der Rechte der betroffenen Personen erforderlichen Maßnahmen ergreift. Diese Regelungen müssen dabei für den Betroffenen transparent sein, wobei der Betroffene

[16] EuGH C-210/16, Rdnr. 30.

seine Rechte dennoch bei und gegenüber jedem einzelnen Verantwortlichen geltend machen kann (Art. 26 Abs. 3 DS-GVO). Die Beurteilung, ob eine gemeinsame Verantwortung vorliegt, erfolgt anhand der gleichen Maßstäbe wie bei einem alleinigen Verantwortlichen[17].

b) Prüfung Rechtmäßigkeit

Es erfolgt keine Privilegierung der gemeinsamen Verantwortlichen, d.h. auch der Transfer von Daten zu einem gemeinsamen Verantwortlichen muss mit einer Rechtsgrundlage nach Art. 6 DS-GVO gerechtfertigt werden und den generellen Anforderungen aus Art. 5 DS-GVO entsprechen[18].

Soweit ein gemeinsamer Verantwortlicher außerhalb der EU sitzt, bedarf es der weiteren Rechtfertigung dieses Transfers entsprechend Artt. 44 ff. DS-GVO.

c) Informationspflichten

Im Rahmen der Vereinbarung zwischen den gemeinsamen Verantwortlichen ist insbesondere zu regeln, welcher der Beteiligten die Informationspflichten aus Art. 13 DS-GVO zu erfüllen hat. Hierbei ist selbstverständlich auch über die gemeinsame Verantwortlichkeit und gemäß Art. 26 DS-GVO auch über die wesentlichen Inhalte der Vereinbarung zu informieren.

Häufig hat einer der gemeinsamen Verantwortlichen den direkten Kontakt zu den Betroffenen und sollte diese Verpflichtung übernehmen. Der andere Verantwortliche muss diese Pflicht dann nicht zusätzlich erfüllen.

Dies kann beispielsweise mittels der Datenschutzerklärung desjenigen Verantwortlichen erfolgen, der die personenbezogenen Daten über die eigene Website erhebt und sodann an den mit ihm gemeinsam Verantwortlichen zu übermitteln beabsichtigt.

[17] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 22.
[18] Kurzpapier Nr. 16 der Datenschutzkonferenz vom 19.03.2018.

C. HAFTUNG

In der DS-GVO gibt es mehrere Arten von Sanktionen, die im Falle eines Verstoßes gegen die Vorschriften der DS-GVO drohen. Vor allem von der Aufsichtsbehörde erhobene Bußgelder sowie zivilrechtliche Schadensersatzansprüche haben hierbei herausragende Bedeutung. Daneben kommen aber auch strafrechtliche Konsequenzen sowie Abmahnungen[19] durch Mitbewerber nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) in Betracht.

Die Aufsichtsbehörden sind bei Verstößen gegen Vorschriften der DS-GVO ermächtigt, Bußgelder zu verhängen, die in „jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sind (Art. 83 Abs. 1 DS-GVO). Hierzu steht den Aufsichtsbehörden ein Bußgeldrahmen von bis zu 20.000.000 Euro oder bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres zur Verfügung[20]. Welcher Stelle gegenüber die Bußgelder im Einzelnen angedroht werden, hängt von der verletzten Norm ab. Grundsätzlich können Geldbußen sowohl gegen Verantwortliche als auch gegen Auftragsverarbeiter verhangen werden. Zu prüfen ist insoweit zunächst, welche Stelle Adressat der verletzten Norm ist. Einzig der einzelne Mitarbeiter selbst kann kein Adressat einer Geldbuße durch die Aufsichtsbehörde sein[21].

Im Falle von Geldbußen gegen Unternehmen wird der Unternehmensbegriff im Sinne des EU-Kartellrechts (Art. 101 und 102 AEUV) als Grundlage genommen[22]. Dies hat zur Folge, dass auch ein Mutterkonzern gesamtschuldnerisch in Anspruch genommen werden kann, ohne dass er selbst an der Datenverarbeitung beteiligt gewesen ist. Voraussetzung ist, dass der Mutterkonzern in einem gewissen Maße auf die Tochterunternehmen einwirken kann[23] und Mutterkonzern und Tochterunternehmen als eine wirtschaftliche Einheit betrachtet werden kann[24]. Liegen diese Voraussetzungen vor, richtet sich die Höhe der umsatzabhängigen Geldbuße nach dem gesamten Jahreskonzernumsatz und nicht nur nach dem Umsatz des einzelnen Tochterunternehmens[25].

[19] EuGH- Urteil vom 29.07.2019, Az. C-40-17, Rdnr. 63.
[20] Gola/Jaspers/Müthlein/Schwartmann: DS-GVO/BDSG im Überblick, Datakontext, 3. Aufl., 2018, S. 96.
[21] Gola DS-GVO/Gola, 2. Aufl. 2018, DS-GVO, Art. 83 Rdnr. 16.
[22] Erwägungsgrund DS-GVO Nr. 150.
[23] Gola DS-GVO/Gola, 2. Aufl. 2018, DS-GVO, Art. 83 Rdnr. 19.
[24] Faust/Spittka/Wybitul, ZD 2016, 120, 121.
[25] Faust/Spittka/Wybitul, ZD 2016, 120, 121.

Auf der anderen Seite kann auch der jeweils Betroffene gemäß Art. 82 Abs. 1 DS-GVO selbst einen Anspruch sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter auf Schadensersatz haben. Voraussetzung hierzu ist das Vorliegen eines schuldhaften Verstoßes gegen die DS-GVO sowie ein durch die Verletzung entstandener Schaden beim Betroffenen[26].

Bedient sich ein Verantwortlicher eines Auftragsverarbeiters, haftet in erster Linie der Verantwortliche für dem Betroffenen entstandene Schäden. Der Auftragsverarbeiter haftet eingeschränkt nur soweit er gegen eine ihm auferlegte Pflicht aus der DS-GVO oder der nach Art. 28 DS-GVO zu vereinbarenden Auftragsverarbeitungsvereinbarung verstoßen hat. Ein klassischer Verstoß gegen Pflichten aus der Auftragsverarbeitungsvereinbarung wäre die eigenmächtige Verarbeitung der vom Verantwortlichen zur Erfüllung des Auftrags überlassenen personenbezogenen Daten zu eigenen Zwecken des Auftragsverarbeiters. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter oder mehrere Verantwortliche an derselben Verarbeitung beteiligt, können sie zunächst jeweils für den gesamten Schaden haftbar gemacht werden und haben im Anschluss entsprechende Regressansprüche untereinander[27]. Mit dieser Regelung bezweckt die DS-GVO, dass zugunsten der Betroffenen ein wirksamer Schadensersatz sichergestellt ist.

Ersetzt verlangen können Betroffene sowohl materielle als auch immaterielle Schäden. Der Begriff des immateriellen Schadens wird im Rahmen der DS-GVO weit ausgelegt[28]. Ein immaterieller Schaden ist grundsätzlich dann anzunehmen, wenn das Persönlichkeitsrecht des Betroffenen verletzt wurde. Dies ist unter anderem dann der Fall, wenn die Datenverarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einer Rufschädigung oder ähnlichen gesellschaftlichen Nachteilen geführt hat[29].

Die Bemessung des jeweiligen Schadensersatzes dürfte sich dabei nicht nur nach deutschen Vorgaben richten, sondern sich an europäischen Maßgaben orientieren, d.h. in der Regel etwas höher ausfallen als bei deutschen Gerichten[30].

[26] Nemitz in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 82, Rdnr. 11.
[27] Erwägungsgrund DS-GVO Nr. 146.
[28] Erwägungsgrund DS-GVO Nr. 146.
[29] Erwägungsgrund DS-GVO Nr. 75.
[30] Nemitz in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 82, Rdnr. 3.

1. Haftung des Verantwortlichen

Werden die Daten des Betroffenen unrechtmäßig, also insbesondere im Widerspruch zu Art. 6 DS-GVO, verarbeitet, haftet der Verantwortliche voll nach Art. 82 DS-GVO und ist dem Betroffenen zum Ersatz des daraus entstandenen Schadens verpflichtet. Diese Haftung tritt gemäß Art. 82 Abs. 4 DS-GVO auch dann ein, wenn mehr als ein Verantwortlicher oder neben dem Verantwortlichen auch ein Auftragsverarbeiter an der Datenverarbeitung beteiligt ist.

2. Haftung des Auftragsverarbeiters

Da der Auftragsverarbeiter grundsätzlich nur im Auftrag und auf Weisung des Verantwortlichen handelt, haftet er dem Betroffenen gegenüber in der Regel nicht auf einen durch die Datenverarbeitung entstandenen Schaden. Verstößt der Auftragsverarbeiter jedoch gegen seine Pflichten, die sich aus dem mit dem Verantwortlichen geschlossenen Vertrag oder aus der DS-GVO direkt ergeben, sieht die DS-GVO eine Haftung des Auftragsverarbeiters vor. Sofern der Auftragsverarbeiter wiederum selbst weitere andere Auftragsverarbeiter einsetzt, haftet er gemäß Art. 28 Abs. 4 S. 2 DS-GVO dem Verantwortlichen gegenüber, wenn der von ihm eingesetzte Auftragsverarbeiter seinerseits gegen Pflichten verstößt.

3. Haftung der Joint Controller

Gemäß Art. 26 Abs. 3 DS-GVO haften die gemeinsam Verantwortlichen dem Betroffenen gegenüber gesamtschuldnerisch für alle Ansprüche. Das bedeutet, dass der Betroffene alle Ansprüche aus einer unrechtmäßigen Datenverarbeitung zunächst gegenüber jedem Verantwortlichen einzeln ersetzt verlangen kann. Um die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten, muss jede einzelne Verarbeitung nach Art. 6 Abs. 1 DS-GVO rechtmäßig sein[31].

Sollte ein Verantwortlicher von dem Betroffenen wegen einer Datenschutzverletzung zur Verantwortung gezogen werden, so kann dieser bei dem anderen Verantwortlichen nach Art. 82 Abs. 5 DS-GVO Regress nehmen. Hierbei ist dann zu klären, in wessen Bereich die Verletzung des Betroffenen liegt[32], da jeder Verantwortliche nach Art.

[31] Bertermann in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 26, Rdnr. 14.
[32] Nemitz in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 82, Rdnr. 31..

82 Abs. 2 DS-GVO nur für den Schaden haftet „der durch eine nicht [der DS-GVO] entsprechende Verarbeitung verursacht wurde".

D. PROBLEMSTELLUNG BEI DER DATENVERARBEITUNG IM KONZERNVERBUND

Mehrere Verantwortliche, die als Unternehmen gelten, bilden gemäß Art. 4 Nr. 19 DS-GVO eine „Unternehmensgruppe", soweit diese Gruppe aus einem herrschenden und mehreren von diesem Unternehmen abhängigen anderen Unternehmen besteht. Auch und gerade in einem solchen Konzernverbund ist es gängige Praxis verschiedene Daten für Dienstleistungen, die zentral erbracht werden können, auch über die Grenzen der einzelnen Unternehmen hinweg zu verarbeiten und zu speichern, um einerseits Verantwortungen und Prozesse zu zentralisieren und andererseits Kosten zu sparen. Auf diese Weise können gewisse Prozesse, wie z.B. Human-Resources-Dienstleistungen, in weniger kostenintensive Auslandsniederlassungen verlegt werden, welche sodann den gesamten Konzern mit diesen Diensten versorgen. Die Muttergesellschaft gibt dabei meist die jeweiligen Rahmenbedingungen vor und diese werden in den einzelnen Tochtergesellschaften implementiert.

Im Bereich der konzerninternen Datenverarbeitung bzw. Datenübermittlung zwischen einzelnen Gesellschaften innerhalb eines Konzerns ist daher die richtige Qualifikation der datenschutzrechtlichen Zusammenarbeit entscheidend, um die Konformität mit der DS-GVO sicherzustellen und keinen Haftungsfall nach Art. 83 DS-GVO zu begründen.

Schon während der Geltung des BDSG-alt galten die allgemeinen Zulässigkeitsregeln für die Verarbeitung personenbezogener Daten. Wie bereits unter „C. Haftung" angedeutet, wird der Konzernverbund von der DS-GVO nicht als einheitliches Unternehmen angesehen. Vielmehr ist jede Konzerngesellschaft nach dem

nunmehr geltenden Recht der DS-GVO selbständiger „Verantwortlicher" oder „Auftragsverarbeiter". Denkbar ist aber auch, dass Konzerngesellschaften die Merkmale der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO erfüllen.

Jedenfalls sieht die DS-GVO im Konzernbereich einen Datenaustausch zwischen datenschutzrechtlich selbstständigen Rechtseinheiten vor. Jeder Datenaustausch ist damit ein Verarbeitungsvorgang, der einer Erlaubnisgrundlage nach Art. 6 DS-GVO bedarf. Im Bereich der DS-GVO gibt es also kein direktes „Konzernprivileg".

In Erwägungsgrund 48 zur DS-GVO findet sich allerdings doch ein „kleines Konzernprivileg". Dieser Erwägungsgrund sieht vor, dass „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln". Damit ist jedenfalls die Beurteilung der Rechtmäßigkeit von Datenverarbeitungen vereinfacht. Die Datenübermittlung von einer Gruppengesellschaft an eine andere Gruppengesellschaft muss im Ergebnis aber dennoch den gleichen Anforderungen genügen wie eine Übermittlung zwischen unabhängigen Kooperationspartnern.

Vertragliche Regelungsmöglichkeiten

Im Folgenden sollen mögliche Vereinbarungen, die zwischen den Gesellschaften einer Unternehmensgruppe getroffen werden können, damit ein Datenaustausch erfolgen darf, skizziert werden.

1. Auftrag oder gemeinsame Verantwortlichkeit

In der Praxis gehen viele Unternehmen davon aus, dass ein Transfer zwischen

Gruppenunternehmen unproblematisch möglich sein müsste und entsprechend weder eine vollständige Prüfung der Rechtmäßigkeit notwendig ist noch vertragliche Grundlagen zu schaffen sind. Wie oben bereits beschrieben ist dies nicht korrekt. Vielmehr bedarf es auch unter den Unternehmen einer Gruppe hinreichender vertraglicher Grundlagen für die Datenverarbeitung.

In der Praxis wird hier vielfach der Weg über (teils wechselseitige) Auftragsverarbeitungsvereinbarungen gewählt. Dies ist selten der richtige Weg, da die Auftragsverarbeitungsvereinbarung einzelne ausgelagerte Verarbeitungen im Auge hat, in der einer der Beteiligten streng nach Weisung tätig wird. Gerade zwischen Unternehmen einer Gruppe ist die Situation aber eher kooperativ und weniger subordinativ ausgestaltet.

Darüber hinaus dürfte die Einschätzung der Zusammenarbeit der verschiedenen Gruppenunternehmen regelmäßig eher in Richtung einer gemeinsamen Verantwortlichkeit gehen, da häufig beide Unternehmen gemeinsam entscheiden, wie der Prozess im Detail ausgestaltet werden soll. Dann wären Auftragsverarbeitungsvereinbarungen sogar das falsche Rechtsinstrument; vielmehr wäre dann ein Joint Controller Agreement angebracht.

2. Betriebsvereinbarungen

Gemäß der Öffnungsklausel in Art. 88 DS-GVO i. V. m. § 26 BDSG kann die Personaldatenübermittlung durch eine Betriebsvereinbarung zur Einführung und Nutzung von HR-Software zu rechtfertigen sein. Zu berücksichtigen ist hierbei, dass der Schutz der Interessen der Arbeitnehmer bei der konzerninternen Weitergabe ihrer personenbezogenen Daten sichergestellt ist.

3. Binding Corporate Rules bei Datenübermittlungen außerhalb der EU

Soweit eines der Gruppenunternehmen außerhalb der EU in einem Land sitzt, welches kein angemessenes Datenschutzniveau bietet, bedarf es neben der

allgemeinen Prüfung der Rechtmäßigkeit der Verarbeitung und der Weitergabe an einen Dritten, einer weiteren Rechtfertigung für den Transfer über die Grenzen der EU hinaus. Hier besteht die Möglichkeit der Rechtfertigung durch sogenannte „Binding Corporate Rules" (BCR). Hierbei handelt es sich um genehmigte verbindliche interne Unternehmensrichtlinien nach Art. 47 DS-GVO, die konzernweit gültige und verbindliche Vorgaben zur Regelung von Datenflüssen darstellen. Diese bewirken, dass ein einheitlicher Datenschutzstandard geschaffen wird. Damit die verbindlichen internen Datenschutzregelungen die entsprechende Wirkung entfalten können, müssen diese zuvor von der zuständigen Aufsichtsbehörde genehmigt werden.

E. ABSCHLIESSENDE WORTE

Da die korrekte Einordnung der Verantwortlichkeit im Datenschutz Auswirkungen auf allen Ebenen der datenschutzrechtlichen Rechtmäßigkeit hat, ist es zwingend erforderlich, diese bereits zu Beginn einer Prüfung eindeutig zu klären.

Dieser Artikel soll nicht als Anleitung zur Prüfung dienen, sondern lediglich ein besseres Verständnis für die verschiedenen Institutionen hervorrufen, die die DS-GVO für die Zusammenarbeit verschiedener Unternehmen bei einer Datenverarbeitung bietet. Die korrekte Einordnung von konkreten Prozessen in diese Institutionen hängt von verschiedenen individuellen Faktoren ab und sollte im Einzelfall jedenfalls aufmerksam und umfänglich geprüft werden. Am Ende hängt hiervon nicht nur die Haftung des Unternehmens sondern auch der Umfang der Prüfung des Prozesses auf seine Rechtmäßigkeit ab.

GDPR Playbook

Cloud Computing – Alles neu machte die DS-GVO?

Jens Eckhardt

Cloud Computing – Alles neu machte die DS-GVO?

Cloud Computing ist im Unternehmensalltag etabliert und wird häufig auch nicht mehr isoliert als solches wahrgenommen, sondern wirkt als eine Art „Basistechnologie" für verschiedene Erscheinungsformen der Digitalisierung. Ebenso selbstverständlich sind die damit verbundenen Datenschutzthemen. Der Anwendungsbeginn der DS-GVO hat gerade für die Cloud-Anwendungen Veränderungen gebracht.

Vorneweg lässt sich sagen, dass die DS-GVO nicht alles grundlegend geändert hat, da die Grundzüge des § 11 BDSG-alt fortgeführt sind. Gerade deshalb aber besteht das Risiko, die Besonderheiten zu übersehen. Diese Fortschreibung ist Segen und Fluch zugleich. Für die Übergangszeit vom alten zum neuen Datenschutzrecht war sie gut, weil Anpassungsbedarf bestenfalls nicht bestand. Allerdings erfolgte damit auch nicht der „große Wurf", der aus der Sicht des Cloud Providing wünschenswert gewesen wäre. Teilweise sind die Regelungen weiterhin von Ansätzen der beginnenden 1990iger Jahre geprägt. Der Blick ist daher nicht auf die Übergangszeit gerichtet, sondern auf verbliebene Herausforderungen.

Diese Herausforderungen zeigen sich aber zum Teil erst auf den zweiten Blick. In diesem Beitrag sollen sie nun schwerpunktmäßig beleuchtet werden.

1. Konstruktion der Auftragsverarbeitung

1.1 Warum Cloud-Computing nicht um das Thema Datenschutzrecht herum kommt?

Entscheidend ist, ob personenbezogene Daten des Auftraggebers in einer Cloud-Umgebung verarbeitet werden. Aus der Sicht des Datenschutzrechts ist zu beachten, dass für die Bewertung des Personenbezugs nicht primär auf den Cloud Anbieter abgestellt werden kann, sondern auf den Cloud Nutzer abgestellt werden muss. Sind die in die Cloud verlagerten Daten für den Cloud Nutzer personenbezogene

Daten, dann sollte das Datenschutzrecht mit ins Auge gefasst werden. Die bereits vor Jahren begonnene Diskussion, ob verschlüsselt in die Cloud verlagerte Daten nicht als personenbezogene Daten für den Cloud Anbieter zu behandeln sind und welche Anforderungen für eine solche Verschlüsselung zu gelten haben, ist noch nicht zu Ende geführt. Auch der für die DS-GVO relevante Begriff „Verarbeitung" ist durch die DS-GVO sehr weit gefasst, so dass typischerweise auch nicht anhand der Tätigkeit des Dienstleisters begründet werden kann, dass das Datenschutzrecht nicht zu beachten ist.

Die Chance der Klärung dieser Frage und die Definition der Anonymisierung wurde mit Einführung der DS-GVO verpasst. Sie war zwar im Gesetzgebungsverfahren ein Thema, fiel dann aber der politischen Beschleunigung des Gesetzgebungsverfahrens zum Opfer. Eine Definition ist in Art. 4 DS-GVO nicht erfolgt. Allein am Ende des Erwägungsgrundes 26 DS-GVO gibt es Anhaltspunkte, aber nicht für das Cloud Computing und die Digitalisierung erforderliche Klarheit.

Kurzum: There is no easy way out! Die Praxis zeigt, dass zuweilen mehr Zeit darauf verschwendet wird, die Nichtanwendbarkeit des Datenschutzes zu diskutieren, als es für eine datenschutzkonforme Realisierung erforderlich ist.

1.2 Die Auftragsverarbeitung als Mittel der Wahl

Das Instrument zur Einbindung von Externen in die Verarbeitung personenbezogener Daten ist die Auftragsverarbeitung. Für die Auftragsverarbeitung sind zwei Elemente prägend:

1. Der Auftragsverarbeiter handelt strikt weisungsgebunden (Artt. 28 Abs. 3 lit. a, 29 DS-GVO).

2. Der Auftraggeber schließt mit dem Auftragnehmer eine Vereinbarung nach Maßgabe des Art. 28 DS-GVO.

Diese enge Einbindung rechtfertigt – wie nach dem alten BDSG – datenschutzrechtlich die Verarbeitung durch einen Externen oder auch nur den Zugriff auf personenbezogene Daten, welche ein Externer für den Auftraggeber verarbeitet.

Auch wenn die vertragliche Gestaltung nicht immer so leicht ist, ist sie aus der Sicht des Cloud Providers – allein schon aus Haftungsgründen (siehe Ziffer 2) - die vorzugswürdige Gestaltung – zumindest dann, wenn mit einem Blick über den Tellerrand des Art. 28 DS-GVO weitere Aspekte vertraglich geregelt werden (hierzu nachfolgend).

2. Schadensersatz, Sanktionen und Co.

Die Haftung des Cloud Nutzers (Auftraggeber) hat sich durch die DS-GVO nicht grundsätzlich geändert. Er hat auch vor Geltung der DS-GVO für sein eigenes Verhalten und das seines Cloud Providers wie für eigenes Verhalten gehaftet (Stichwort: Haftung für Erfüllungsgehilfen, § 278 BGB).

Grundlegende Änderungen haben sich aber für die Haftung des Cloud Anbieters als Auftragsverarbeiter ergeben. Bis zum Anwendungsbeginn der DS-GVO war der Auftragsverarbeiter datenschutzrechtlich vor Bußgeldern durch die deutschen Datenschutzaufsichtsbehörden und Schadensersatzansprüchen durch diejenigen, deren Daten in der Cloud verarbeitet werden (sog. betroffene Person), geschützt.

Die DS-GVO hat hier zwei Stellschrauben gedreht:

- Die betroffene Person kann direkt den Cloud Provider auf Schadensersatz (auch gerichtlich) in Anspruch nehmen, wenn ihr aufgrund eines Verstoßes gegen das Datenschutzrechts ein Schaden entsteht (Art. 79 Abs. 2 DS-GVO). Damit ist die bisherige Privilegierung nach BDSG-alt entfallen.

Ein Schaden kann auch ein sog. immaterieller Schaden sein (Art. 82 Abs. 1 DS-GVO). Das Stichwort aus dem deutschen Recht ist hier „Schmerzensgeld". Das ist zwar in Deutschland eher zurückhaltend gesehen worden, nicht aber in den anderen Mitgliedstaaten der EU. Hierzu muss berücksichtigt werden, dass die Handhabung nach der DS-GVO EU-einheitlich erfolgen muss und daher die bisherige deutsche Zurückhaltung nicht zwingend auch zukünftig gilt.

• Die DS-GVO hat aber die Veränderung nicht bei der Abschaffung der Haftungsprivilegierung belassen, sondern sogar die Haftung erweitert.

Nach Art. 82 Abs. 4 DS-GVO haften der Auftraggeber (Cloud Nutzer) und der Auftragsverarbeiter (Cloud Provider) gesamtschuldnerisch. Das bedeutet, dass der Cloud Provider auch für Schäden im Sinne der DS-GVO haftet, die durch den Cloud Nutzer verursacht werden („Ist ... sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.").

Durch Art. 82 Abs. 2 Satz 2 DS-GVO ist die Haftung des Auftragsverarbeiter zwar begrenzt, da ein Auftragsverarbeiter für den durch eine Verarbeitung verursachten Schaden nur dann haftet, „wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat." Ob diese Begrenzung in der Praxis wirklich effektiven Schutz bietet, wird sich erst noch zeigen müssen.

Nur zur Gegenprobe: Wer auf die Idee kommt, wegen dieser Haftung lieber kein Auftragsverarbeiter sein zu wollen, stellt sich damit nicht besser. Denn dann haftet

er ohnehin als Verantwortlicher uneingeschränkt und kann sich nicht einmal auf die Haftungsbegrenzung nach Art. 82 Abs. 2 S. 2 DS-GVO berufen.
Auch mit Blick auf die Bußgelder hat sich die Konstellation für den Auftragsverarbeiter grundlegend geändert. Während er nach dem BDSG-alt nicht Adressat eines Bußgeldes werden konnte, sieht ihn die DS-GVO uneingeschränkt als Adressat von Bußgeldern vor.

Kurzum: Der Cloud Provider muss sich seiner (erweiterten) Haftung bewusst sein. Gerade für Cloud Provider ist das in vielen Konstellationen misslich, weil sie mit der eigentlichen Datenverarbeitung überhaupt nichts zu tun haben, sondern nur die Rahmenbedingungen für diese stellen. Das ändert aber nichts an der vorstehend beschriebenen Haftung. Durch entsprechende vertragliche Regelungen (Stichwort: Freistellungsregelungen) muss dieses Risiko „eingedämmt" werden.

3. Inhaltliche Anforderungen und Stolperfallen

Die inhaltlichen Anforderungen an die Vereinbarung über die Auftragsverarbeitung sind durch Art. 28 DS-GVO nicht vollkommen neu geregelt worden. Das liegt auch daran, dass die vorhergehenden deutschen Regelungen auf der Datenschutzrichtliniere 95/46/EG beruhten und die DS-GVO diese insoweit im Wesentlich fortgeschrieben hat.

Nicht alle inhaltlichen Aspekte der Ausgestaltung der Auftragsverarbeitung können nachfolgend behandelt werden, aber besondere Aspekte sollen angesprochen werden.

3.1 Elektronische Form des Abschlusses – Auch Erleichterungen durch die DS-GVO!

Die DS-GVO brachte nicht nur Verschärfungen. Mit dem Verzicht auf das sog.

Schriftformerfordernis und der Anerkennung der elektronischen Form brachte sie eine wesentliche Erleichterung zum online-Abschluss solcher Vereinbarungen (Art. 28 Abs. 9 DS-GVO). Dieses Verständnis hat sich zwischenzeitlich auch in Deutschland durchgesetzt, nachdem kurz nach dem Anwendungsbeginn der DS-GVO in der juristischen Fachliteratur Stimmen aufkamen, die auch in die Neuregelung das alte Schriftformerfordernis hineinlesen wollten.

Allerdings sollte dies nicht darüber hinwegtäuschen, dass der Auftraggeber (aber auch der Auftragnehmer) im Ernstfall den tatsächlichen Abschluss dieser Vereinbarung und ihren konkreten Inhalt beweisen können müssen.

3.2 Kontrollrecht vor Ort – Herausforderung im Cloud Computing?!

Die Vereinbarung über die Auftragsverarbeitung muss Folgendes vorsehen (so Art. 28 Abs. 3 S. 2 lit. h DS-GVO): „dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt **und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt".**

Mit anderen Worten: Die Cloud Nutzer muss ein Kontrollrecht vor Ort haben. Art. 28 DS-GVO zwingt ihn zwar nicht dazu, das Kontrollrecht vor Ort aktiv in jedem Fall auszuüben. Denn er muss nach Art. 28 Abs. 1 DS-GVO nur sicherstellen, dass der Cloud Provider geeignet ist. Er muss dieses Recht zu Kontrolle vor Ort aber dennoch haben - so scheint die derzeit herrschende Auslegung in Deutschland zu sein.

Die Cloud Provider stellt dies zwar vor Herausforderungen, aber nicht vor unlösbare. Denn selbst wenn dieser Ansicht gefolgt wird, wird nur der Ausschluss eines Kontrollrechts per se zum Problem. Eine angemessene inhaltliche Ausgestaltung ist hingegen nicht ausgeschlossen. Hierbei muss auch gesehen werden, dass ein unbeschränkter „Kontroll-Tourismus" ebenfalls mit den Vorgaben zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO kollidieren kann. Die zeitliche und räumliche

Ausgestaltung der Kontrollen vor Ort ist daher sogar geboten.

Zum Teil wird in Deutschland vertreten, dass der Cloud Provider die Kontrollen ohne zusätzliche Vergütung und Aufwandsentschädigung erbringen müsse und die Kosten hierfür insgesamt „einpreisen" könne. Jedenfalls eine Aufwandsentschädigung im Einzelfall sollte gestaltbar sein. Denn anderenfalls bestünde auch die Gefahr von Wettbewerbsnachteilen, weil nicht EU-weit einheitlich ein „Einpreisen" in die Grundvergütung vorgesehen ist.

3.3 Subunternehmer – Mehr Spielraum, aber dennoch Herausforderungen

3.3.1 Subunternehmer des Auftragsverarbeiters werden durch die DS-GVO als „weitere Auftragsverarbeiter" bezeichnet. Art. 28 Abs. 2 regelt die Einbindung so: *„Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben."*

Damit ist die sog. Widerspruchslösung neben dem sog. Zustimmungsvorbehalt im Gesetz anerkannt. Das ist für die Praxis eine erhebliche Vereinfachung.

Das Gesetz regelt die Ausgestaltung der Widerspruchslösung aber nur unvollständig. Was ist die Konsequenz eines Widerspruchs? Was ist der Vorlauf? Die Regelung wird so zu verstehen sein, dass die Möglichkeit des Widerspruchs so gestaltet ist, dass der Auftraggeber den Zugriff des Subunternehmers, dessen Einbindung er widerspricht, verhindern kann. In der Praxis sind verschiedene Gestaltungen zu finden, die diesem Umstand angemessen Rechnung tragen.

Aus Cloud Nutzer-Sicht sollte aber bei einer eventuellen Frist zur Sonderkündigung beachtet werden, dass diese so lang ist, dass eine Auswahl eines anderen Anbieters und eine Transition in dieser Frist möglich ist.
3.3.2 Die DS-GVO geht davon aus, dass ein Subunternehmer durch den Cloud Provider zu denselben vertraglichen Regelungen eingebunden werden muss, wie sie zwischen Cloud Nutzer und Cloud Provider gelten. Die DS-GVO formuliert dies so: *„... so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags ... dieselben Datenschutzpflichten auferlegt, die in dem Vertrag ... zwischen dem Verantwortlichen und dem Auftragsverarbeiter ... festgelegt sind"*. Mit anderen Worten: Es müssen die Vertragsbedingungen durchgereicht werden.

Eine Herausforderung stellt es dar, wenn die Regelung wörtlich genommen wird und „dieselben" (englisch: „the same") Bedingungen gefordert werden. Denn dann ist keine Abweichung möglich. Zur Herausforderung wird dies dann, wenn der Cloud Provider nicht selbst die Verträge mit seinen Auftraggebern und seinen Subunternehmern vorgibt, sondern selbst auf andere Cloud Services (PaaS, IaaS, ..) zurückgreift und diese ihre Vertragsbedingungen vorgeben. Dann befindet er sich unter Umständen in einer „Sandwich-Position" zwischen den Vorgaben seines Auftraggebers und den Vorgaben seines Subunternehmers. Dies muss frühzeitig bei der Gestaltung der Vertragsbedingungen berücksichtigt werden.

3.4 Sicherheit der Verarbeitung nach Art. 32 DS-GVO

Die Vereinbarung über Auftragsverarbeitung muss nach Art. 28 Abs. 3 S. 1 lit. c DS-GVO vorsehen, dass „der Auftragsverarbeiter alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift". Mit anderem Worten: In dem Vertrag müssen die technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung nach Maßgabe des Art. 32 DS-GVO geregelt sein.

Aus der Sicht des Cloud Providers wäre es zu kurz gesprungen, davon auszugehen, dass die Angemessenheit der Maßnahmen allein das Problem des Auftraggebers ist. Denn Art. 32 DS-GVO selbst nimmt explizit den Auftragsverarbeiter neben dem

Auftraggeber in die Pflicht, angemessene Schutzmaßnahmen zu treffen. Der Verstoß gegen Art. 32 DS-GVO kann für beide sowohl zu Schadensersatzansprüchen (Artt. 79, 82 DS-GVO) als auch zu Geldbußen (Art. 83 Abs. 4 lit. a DS-GVO) führen.
Das Dilemma ist, dass häufig der Cloud Nutzer nicht eigenständig über die Kompetenz zur Beurteilung der erforderlichen Maßnahmen verfügt und gerade deshalb auf den Cloud Service zurück greift und der Cloud Provider nicht weiß (und ggf. aus Datenschutzgründen auch nicht wissen will), welche Daten in seinem Cloud Service verarbeitet werden, und deshalb nicht die Angemessenheit der Maßnahmen bewerten kann.

Kurzum: Dieses Dilemma muss in den Vereinbarungen über die Auftragsverarbeitung klar angesprochen und geregelt sein. Beispielsweise kann (und muss) der Cloud Provider transparent machen, welche Schutzmaßnahmen nach Art. 32 DS-GVO ergriffen sind und der Cloud Nutzer dann bewerten, ob dies für seine Verarbeitung im Sinne des Art. 32 DS-GVO angemessen ist.

3.5 Risiko der unzureichenden Vereinbarung

Wer trägt das Risiko einer nicht den gesetzlichen Anforderungen entsprechenden Vereinbarung über die Auftragsverarbeitung? Natürlich der Auftraggeber. Aber auch der Auftragsverarbeiter.

Ist die Vereinbarung nicht ausreichend gestaltet, liegt keine Auftragsverarbeitung vor und der Datenempfänger – also der Cloud Provider - wird wie ein Dritter behandelt. Für den Cloud Provider bedeutet dies, dass er eine Rechtsgrundlage für die Erhebung der Daten benötigt und ihn selbst alle originären DS-GVO-Pflichten in Bezug auf diese Verarbeitung treffen. Das bedeutet zunächst, dass die Übertragung der Daten nach Maßgabe der Artt. 6 bis 10 DS-GVO zu prüfen ist. Jedenfalls bei Gesundheitsdaten nach Art. 9 DS-GVO wird dies typischerweise zur Unzulässigkeit führen.

Jedenfalls wenn eine Vertragspartei der anderen vorsätzlich eine unzureichende

Vereinbarung „unterschiebt", stehen sogar noch Schadensersatzansprüche im Raum. Auch die datenschutzrechtlich korrekte Ausgestaltung eines Cloud Services ist ein Qualitätsmerkmal.
Kurzum: Beide Seiten haben ein grundlegendes Interesse daran, dass eine den gesetzlichen Anforderungen genügende Vereinbarung geschlossen wird.

4. Meldung von Datenschutzpannen Art. 33 Abs. 2 DS-GVO

Die DS-GVO hat die Regelungen über die Pflicht zur Meldung von Datenschutzpannen grundlegend neu ausgestaltet. Der Cloud Nutzer ist als Verantwortlicher nach Art. 33 DS-GVO unverzüglich, jedenfalls binnen 72 Stunden, zur Meldung bei der Aufsichtsbehörde und nach Art. 34 DS-GVO zur Benachrichtigung der betroffenen Personen verpflichtet, wenn die Verletzung des Schutzes personenbezogener Daten (siehe Art. 4 Nr. 12 DS-GVO) ein Risiko bzw. ein hohes Risiko für Rechte und Freiheiten der betroffenen Personen darstellen kann.

Der Auftragsverarbeiter ist „nur" verpflichtet, eine Verletzung des Schutzes personenbezogener Daten unverzüglich zu melden (Art. 33 Abs. 2 DS-GVO). Das klingt einfacher, als es ist. Denn der Auftragsverarbeiter ist gut beraten, die Art und Weise der Meldung konkret auszugestalten.

Wie soll das geschehen, wenn bspw. samstags morgens um 5.53 Uhr eine solche Verletzung festgestellt wird. Wird dann versucht, die Ansprechpersonen zu kontaktieren? Wird einfach eine E-Mail gesendet? Was wenn das für hunderte oder tausende Kunden des Cloud Providers geschehen muss? Zu bedenken ist dabei, dass die Frist von 72 Stunden läuft – jedenfalls ab Kenntnis des Auftraggebers. Der Auftraggeber wird „unentspannt" sein, wenn er einer Datenschutzaufsichtsbehörde erklären muss, warum er den Vorfall nicht bereits 72 Stunden nach Kenntnis gemeldet hat, sondern im vorstehenden Beispiel erst am Montag morgens zu Beginn

der Geschäftszeiten mit der Bearbeitung begonnen hat.

Die Lösung: Klare, praktisch handhabbare Benachrichtigungswege und –arten sowie Klarstellung der Verantwortung des Auftraggebers. Auch diese sollten wie das Sicherheitskonzept in der Praxis erprobt werden, um Schwachpunkte nicht erst im Ernstfall zu entdecken.

Kurioserweise stellt sich in der Praxis mit dieser Benachrichtigung beim Cloud Provider häufig Entspannung ein; jedenfalls wenn das Problem dann auch schon behoben ist. Rechtlich geht es dann aber eigentlich erst richtig los. Warum? Wenn der Cloud Nutzer den Vorfall der Aufsichtsbehörde meldet, wird er sicherlich sich selbst „ins beste Licht" rücken und die Verantwortung dem Cloud Provider zuweisen und dann für sich die grundlegenden Weichen zur Abwehr von Geldbußen und Schadensersatzansprüchen stellen. Der Cloud Provider kommt hingegen erst wieder „ins Spiel", wenn sich die Aufsichtsbehörden mit Ermittlungen und die betroffenen Personen mit Ansprüchen an ihn wenden. Diese Ausgangsposition ist dann ungünstig.

Kurzum: Der Cloud Provider sollte auch diesen Aspekt bereits in der Vereinbarung mit dem Auftraggeber regeln, um nicht zu lange dem Spiel nur zuschauen zu müssen, sondern rechtzeitig „ins Spiel eingreifen" zu können und seine Rechte zu wahren.

5. Abgrenzung zur Joint Controllership (gemeinsame Verantwortlichkeit)

Nicht erstmals mit der DS-GVO, aber erstmals formalisiert durch die DS-GVO ist die sog. Joint Controllership. Auch hierbei geht es darum, dass zwei Unternehmer zusammenarbeiten. Die Formalisierung der sog. Joint Controllership in Art. 26 DS-GVO hat zu Diskussionen um die Abgrenzung zur Auftragsverarbeitung geführt.

Der entscheidende Unterschied ist: Bei der Auftragsverarbeitung entscheidet allein der Auftraggeber über Zwecke und Mittel der Verarbeitung. Bei der Joint Controllership entscheiden die Zusammenarbeitenden gemeinsam hierüber. Gerade bei Cloud Services als durch den Cloud Provider vorkonfigurierten Leistungen führte dies zu der Diskussion, ob der Cloud Provider über die Zwecke und Mittel mitentscheiden darf.

Typischerweise ist das zu verneinen, wenngleich die Abgrenzung nicht leicht ist. Allein ein Disclaimer hilft nicht, kann aber für die Auslegung hilfreich sein. Die Vereinbarung muss klar zum Ausdruck bringen, dass der Cloud Provider zwar eine vorkonfigurierte Leistung anbietet, aber der Cloud Nutzer allein darüber entscheidet, ob er damit personenbezogene Daten verarbeitet und dies für sich tut, während der Cloud Provider mit den Daten fremdnützig für den Auftraggeber umgeht.

6. Drittstaatentransfer

Die Nutzung von grenzüberschreitenden Cloud Services hat sich im Grundsatz durch die DS-GVO nicht geändert, wenngleich in den Artt. 44 ff. DS-GVO konkretere Ausgestaltungen erfolgt sind. Die Instrumente zum Datentransfer in Länder außerhalb der EU sind im Wesentlichen gleich geblieben.

Gleich geblieben ist auch die Diskussion, ob für den Drittstaatentransfer auf den Standort der Daten oder den Standort des Cloud Providers abzustellen ist. Die Tendenz geht dazu, auf den Standort der Daten abzustellen.

7. Art. 30 Abs. 2 DS-GVO – Verzeichnis von Verarbeitungstätigkeiten für den Cloud Service

Neu ist die Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten durch Auftragsverarbeiter nach Art. 30 Abs. 2 DS-GVO. Diese Pflicht ist von der generellen und allgemeinen Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten des Art. 30 Abs. 1 DS-GVO zu unterscheiden. Darin ist die Pflicht speziell für Auftragsverarbeiter vorgesehen, ein Verzeichnis zu allen Kategorien von im Auftrag durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten zu führen. Dieses Verzeichnis soll den Datenschutzaufsichtsbehörden die Kontrolltätigkeit erleichtern, da es diesen nach Art. 30 Abs. 3 DS-GVO auf Verlangen vorzulegen ist. Darüber hinaus soll es der Selbstkontrolle dienen. Ein Verstoß gegen die Pflicht ist bußgeldbewehrt.

Eine Pflicht zur Vorlage dieser beiden Verzeichnisse gegenüber einem Auftraggeber sieht die DS-GVO nicht vor. Es sollte auch gut überlegt werden, ob eine solche Pflicht in Verträge vorgesehen oder akzeptiert wird. Denn die Vorlage dieser Verzeichnisse gegenüber einem Auftraggeber kann zur Verletzung von Geheimhaltungspflichten in Bezug auf andere Vertragsverhältnisse führen.

8. Ein Fazit

Die DS-GVO stellt das Cloud Computing vor keine unlösbaren Herausforderungen. Sie brachte im Vergleich zum alten Datenschutzrecht sogar Erleichterungen und Vereinfachungen für das Angebot von Cloud Computing. Die Tücke der Vorgaben der DS-GVO kann jedoch darin bestehen, dass ihre Vorgaben zuweilen in ihren praktischen Auswirkungen unterschätzt werden. Geschieht dies nicht, lassen sich auch diese Aspekte vertraglich gestalten.

Kurzum: Die DS-GVO zwingt mehr denn je zu einer überlegten und transparenten Vertragsgestaltung. Eine solche stellt zugleich ein Qualitätskriterium des Cloud Computing dar, das auf die Qualität im Übrigen schließen lässt.

eco – Verband der Internetwirtschaft e. V.
Lichtstraße 43h
50825 Köln

fon: 0221 – 7000 48 – 0
fax: 0221 – 7000 48 – 111

E-Mail: info@eco.de
Web: https://www.eco.de

Vereinsregister Köln
Vereinsregisternummer: 14478

Umsatzsteueridentifikationsnummer:
VAT-ID: DE 182676944

Juni 2020