WHITEPAPER

PRAXISORIENTIERTE UMSETZUNG VON INFORMATIONSPFLICHTEN

Herausgeber:
eco – Verband der Internetwirtschaft e.V.

Autor:
Christian Schmoll
Rechtsanwalt, Fachanwalt IT-Recht, CIPP/E, CIPM

VERBAND DER INTERNETWIRTSCHAFT

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[1] 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.

[1] http://web.br.de/interaktiv/datenschutzerklaerungen/

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[2] („Leitlinien für Transparenz")[3] 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.

[2] 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.
[3] 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[4] 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" 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.

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

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 verweisen 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 Prozessdoku-

mentation 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[5] 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.*

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

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.

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 Datenschutzaufsichtsbehörde 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

ÜBER DEN AUTOR

Christian Schmoll
Rechtsanwalt, Fachanwalt IT-Recht,
CIPP/E, CIPM

Christian Schmoll ist Rechtsanwalt und Fachanwalt IT-Recht in München. Er berät seit 15 Jahren zahlreiche internationale Unternehmen im Bereich des IT- und Datenschutzrechts. Nach einer langjährigen Tätigkeit als Inhouse-Jurist und Leiter der Rechtsabteilung internationaler IT-Unternehmen ist er als selbständiger Rechtsanwalt (www.g3s.legal) und als externer Datenschutzbeauftragter (www.dp.institute) tätig. Er ist Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Manager (CIPM) und zertifizierter Datenschutzbeauftragter (TÜV).

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

September 2019