

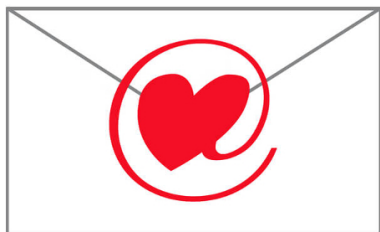
## Datenschutz *aktuell* Ausgabe April 2019

### Der Datenschutz Newsletter aus Nürnberg

Liebe Leser des Datenschutz Newsletter,

ab April 2019 erscheint der Datenschutz Newsletter in einem neuen, professionellen Format. In unregelmäßigen Abständen informieren wir Sie nunmehr intensiver und auch mit mehreren Beiträgen pro Ausgabe. Ich hoffe Ihnen hiermit, bei Ihren Datenschutz Aufgaben, praktische Unterstützung geben zu können.

Ihr Peter Brandmann



### **Ausgeschiedene Mitarbeiter als Adressaten von E-Mails – was tun mit den Mails?**

**Ein Mitarbeiter scheidet aus dem Unternehmen aus. Kann der Arbeitgeber den Mail-Account des Mitarbeiters einfach schließen? Wie ist mit E-Mails umzugehen, die ausdrücklich an ihn gerichtet sind? Das Bayerische Landesamt für**

**Datenschutzaufsicht bietet in seinem Tätigkeitsbericht für 2015/2016 einige Orientierungshilfen für diese Fragen.**

#### **Existieren schon Regelungen?**

Vorab sei auf Folgendes hingewiesen: Falls zu diesem Thema eine Betriebsvereinbarung existiert, ist alles klar. Es gelten ihre Regelungen. Manchmal treffen das Unternehmen und der ausscheidende Mitarbeiter auch eine ausdrückliche Vereinbarung, etwa in einem Aufhebungsvertrag. Schön für alle Beteiligten! Denn das schafft Klarheit.

#### **Und wenn nicht?**

Aber was ist, wenn es an Beidem fehlt? Vielleicht lässt sich noch über eine einvernehmliche Regelung reden. Aber manchmal erscheint das kaum vorstellbar, etwa nach einer fristlosen Kündigung. In solchen Fällen hilft die Meinung der Datenschutzaufsicht weiter.

#### **Schließung des Mail-Accounts**

Zunächst zu der Frage, wie lange ein Mail-Account noch bestehen darf. Etwa drei Monate nach dem Ausscheiden sollte er nach Auffassung des Landesamts geschlossen

werden. Der Grund: Danach ist nicht mehr damit zu rechnen, dass noch Mails an den ausgeschiedenen Mitarbeiter eingehen. Eine ausdrückliche gesetzliche Regelung dazu gibt es aber nicht.

### **Private Nutzung erlaubt oder nicht?**

Schwieriger ist eine Antwort auf die Frage, ob Mails, die noch eingehen, an einen anderen Mitarbeiter weitergeleitet werden dürfen. Hier unterscheidet das Landesamt danach, ob der Arbeitgeber die private E-Mail-Nutzung erlaubt hat oder nicht.

### **Falls private Nutzung verboten ist ...**

Relativ freie Hand hat der Arbeitgeber, wenn er die private E-Mail-Nutzung verboten hat. In diesem Fall kann er einfach festlegen, dass eine Weiterleitung erfolgt. Denn private Mails können dann ja eigentlich keine eingehen.

Im Einzelfall kann dies aber trotzdem vorkommen. Denn immer wieder gibt es Absender, die nicht wissen, dass die private Nutzung verboten ist, oder denen das egal ist.

### **Umgang mit einzelnen privaten Mails**

Sofern eine private Mail im Unternehmen weitergeleitet wird, darf der Empfänger ihren Inhalt nicht lesen. Das gilt naturgemäß nur dann, wenn er schon am Absender und/oder am Betreff erkennen kann, dass die Mail privaten Charakter hat. Eine solche Mail ist entweder zu löschen oder an den ausgeschiedenen Mitarbeiter weiterzusenden.

### **Falls private Nutzung erlaubt ist ...**

Falls der Arbeitgeber private Mails erlaubt hat, handelt es sich um eine freiwillige Leistung des Arbeitgebers. Das führt jedoch nicht dazu, dass er einfach die Weiterleitung aller eingehenden Mails anordnen kann. Vielmehr muss er dann das Fernmeldegeheimnis beachten.

### **Einwilligung nötig**

Ohne eine Einwilligung des ausgeschiedenen Mitarbeiters wäre eine Weiterleitung privater Mails daher nicht zulässig. Andererseits dürfte dann auch niemand in den Account schauen, um dienstliche und private Mails zu trennen.

Das Ergebnis: Der Account wäre letztlich insgesamt blockiert. Für viele Unternehmen ist das nicht akzeptabel.

### **Übliche Bedingungen für private Nutzung**

In der Praxis ist deshalb üblich, dass der Arbeitgeber private Mails nur unter Bedingungen erlaubt:

**Bedingung 1:** Der Arbeitnehmer erklärt sich damit einverstanden, dass Mails, die nach seinem Ausscheiden eingehen, an einen anderen Mitarbeiter weitergeleitet werden.

**Bedingung 2:** Er ist außerdem damit einverstanden, dass dieser andere Mitarbeiter den Betreff und den Absender aller eingehenden Mails prüft. Hat eine Mail danach erkennbar privaten Charakter, öffnet er sie nicht. Je nach Vereinbarung löscht er sie oder leitet sie an den ausgeschiedenen Mitarbeiter weiter.

### Eigenes Smartphone als Lösung?

Falls private Mails erlaubt sind, geht es also nicht ohne relativ komplizierte Vereinbarungen. Das ist ein wichtiger Grund dafür, warum viele Unternehmen auf dienstlichen Geräten nur dienstliche Mails erlauben.

Viele Mitarbeiter haben ohnehin ständig ihr privates Smartphone dabei. Private Mails schreiben sie von dort aus. Mit den Inhalten solcher Mails hat der Arbeitgeber nichts zu tun. Datenschutzprobleme gibt es keine.

### Folgeprobleme anderer Art

Allerdings: Mailen ist hier eine private Tätigkeit während der Arbeitszeit. Ob und in welchem Umfang sie erlaubt ist, sollte man klären, bevor es Ärger gibt. Selbstverständlich ist eine solche Erlaubnis auf keinen Fall.

Außerdem: Probleme kann auch der umgekehrte Fall bereiten. Ein Arbeitnehmer benutzt sein privates Smartphone, um dienstliche Mails zu verschicken. Auch das ist nicht einfach so erlaubt.

\* \* \* \*



### Auskunftsrecht nach der DSGVO

Die DSGVO gibt Personen, deren Daten irgendwo gespeichert sind, viele Rechte. Am wichtigsten ist dabei das „Auskunftsrecht der betroffenen Person“. Wer es ausüben will, muss einige Spielregeln kennen. Der interne Aufwand für Unternehmen kann auch bei korrekten Anfragen enorm sein. Die DSGVO nimmt darauf letztlich keinerlei Rücksicht. Ob ein Antragsteller mit der Antwort inhaltlich etwas anfangen kann, ist wiederum sein Problem.

### Auskunftsrecht als „Recht der Rechte“

Das Auskunftsrecht gilt als das wichtigste Recht, das die DSGVO gewährt. Ein wesentlicher Grund dafür: Nur wer weiß, wo Daten über ihn gespeichert sind, kann weitere Rechte geltend machen, etwa das Recht auf die Berichtigung von falschen Daten.

### Zwei Stufen des Rechts

Genau genommen unterscheidet die DSGVO in ihrem Artikel 15 zwei Stufen des Auskunftsrechts:

- **Stufe 1:** Die betroffene Person kann Auskunft darüber verlangen, ob ein Unternehmen oder eine Behörde überhaupt über Daten verfügt, die sie betreffen. Die Antwort auf diese Frage ist im Ergebnis einfach: Ist das der Fall, lautet die Antwort „ja“ (Fall der Positivauskunft). Ist das nicht der Fall, lautet die Antwort „nein“ (Fall der Negativauskunft).
- **Stufe 2:** Falls Daten vorhanden sind, besteht ein Anspruch der betroffenen Person, diese Daten zu erhalten. Außerdem muss sie eine ganze Reihe von Informationen zu den Daten bekommen. Dazu gehört etwa die Angabe des Zwecks, zu dem die Daten verarbeitet werden.

### Berechtigte Sorge der Unternehmen vor dem Aufwand

Das umfassende Auskunftsrecht ist sicher eine große Errungenschaft des Datenschutzrechts. Dennoch sind viele Unternehmen davon nicht nur begeistert. Sie haben keineswegs etwas zu verbergen, wie manche Kritiker glauben. Vielmehr fürchten sie den Aufwand, den solche Anfragen verursachen. Er ergibt sich aus mehreren Aspekten:

- Zunächst einmal muss überall im Unternehmen gesucht werden, ob Daten über die anfragende Person vorhanden sind. Hinweise darauf, wo wahrscheinlich etwas zu finden ist, erleichtern die Suche. Beispiel: Die anfragende Person gibt an, dass sie mehrfach als Zeitarbeiter im Unternehmen gearbeitet hat. Ausdrücklich verpflichtet ist sie zu solchen Angaben allerdings nicht. Sinnvoll sind sie trotzdem. Sie können eine Antwort wesentlich beschleunigen.
- Der Auskunftsanspruch betrifft auch Daten auf Papier. Dies kann den Aufwand bei der Suche vervielfachen. Die DSGVO nimmt auf die Besonderheiten von Daten auf Papier letztlich keine Rücksicht mehr.
- Der Auskunftsanspruch ist zeitlich nicht begrenzt. Er erstreckt sich auf alle Daten, die vorhanden sind – auch auf solche, die schon viele Jahre unangetastet im Firmenkeller liegen.
- Der Auskunftsanspruch besteht auch dann, wenn es um sehr große Datenmengen geht, etwa um mehrere tausend Seiten.

### Recht auf eine kostenlose Kopie

Sind die Daten gefunden, hat die anfragende Person Anspruch auf eine kostenlose Kopie. Besonders bei umfangreichen Papierunterlagen kann dies für das Unternehmen ins Geld gehen. „Eine“ Kopie ist dabei wörtlich zu nehmen. Wer eine zweite Kopie will, etwa weil er die erste Kopie verloren hat, muss dafür zahlen.

### Notwendige Vernichtungsaktionen

Viele Firmen haben die DSGVO zum Anlass genommen, entbehrliche Unterlagen zu

vernichten. Solche Aktionen sind bei Mitarbeitern nicht immer beliebt, aber wichtig. Wenn die gesetzlichen Aufbewahrungsfristen (beispielsweise aus dem Steuerrecht) abgelaufen sind, steht einer Vernichtung von Unterlagen nichts entgegen.

### Grenzen bei Geschäftsgeheimnissen

Der Auskunftsanspruch geht zwar weit. Grenzen hat er aber trotzdem. So ist ausdrücklich festgelegt, dass „das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen“ darf. Dies wirkt abstrakt, hat aber sehr konkrete Auswirkungen. In den Erwägungsgründen der DSGVO ist als Beispiel genannt, dass der Auskunftsanspruch Geschäftsgeheimnisse nicht beeinträchtigen darf. Der Auskunftsanspruch darf sie also nicht aushebeln.

### Kein Anspruch auf eine verständliche Auskunft

Wer Auskunft verlangt, erhält die Daten übrigens so, wie sie vorliegen. Ob er inhaltlich mit ihnen etwas anfangen kann, ist sein Problem. Denn einen Anspruch auf Erläuterung des Inhalts von Daten sieht die DSGVO nicht vor. Dies wird vor allem im Bereich der Medizin wichtig. In der DSGVO heißt es ausdrücklich, dass sich der Auskunftsanspruch auch auf Daten in Patientenakten bezieht. Die Verständlichkeit der dort verwendeten Fachbegriffe und Kürzel ist damit in keiner Weise garantiert. Es ist Sache des Antragstellers, wie er damit klarkommt.

\* \* \* \*



### Das Verzeichnis von Verarbeitungstätigkeiten

**„Verzeichnis“ – das hört sich nach Bürokratie und Arbeit an. Und was bitte bedeutet der seltsame Begriff „Verarbeitungstätigkeiten“? In jedem Fall sollten Sie wissen: Unternehmen droht Ärger, wenn sie kein solches Verzeichnis haben. Also helfen Sie mit, es zu erstellen, wenn man Sie darum bittet.**

#### Neue Regeln seit 25. Mai 2018

Unternehmen müssen seit 25. Mai 2018 die Europäische Datenschutz-Grundverordnung (DSGVO) beachten. Sie ist ein EU-Gesetz. Das hat sich herumgesprochen. Weniger bekannt ist den meisten, dass die DSGVO neue Formalien mit sich bringt. Kernstück ist dabei das „Verzeichnis von

Verarbeitungstätigkeiten“.

**Das Ziel: Überblick**

Dieses Verzeichnis muss in jedem Unternehmen vorhanden sein. Es soll einen Überblick schaffen, mit welchen personenbezogenen Daten das Unternehmen umgeht und was es mit den Daten tut. Dabei wird es oft um Daten von Kunden gehen. Aber auch Daten von Arbeitnehmern sind erfasst. Ebenso Daten von Lieferanten, wenn dabei Namen von Personen auftauchen.

### **Pflicht zur Vorlage des Verzeichnisses**

Die Datenschutzaufsicht kann jederzeit verlangen, dass ihr ein Unternehmen das Verzeichnis vorlegt. Ansonsten droht ein Bußgeld. Und wenn ein Betroffener Auskunft über seine Daten verlangt, hilft das Verzeichnis dabei, diese Daten zu finden. Es ist also sinnvoll, dieses Verzeichnis sorgfältig zu erstellen. Ab und zu muss es auch aktualisiert werden.

### **Formular mit oft banalen Antworten**

Nehmen Sie es deshalb ernst, wenn Sie mithelfen sollen, für eine gute Qualität des Verzeichnisses zu sorgen! Normalerweise bedeutet das, dass Sie ein Formular ausfüllen müssen, sei es elektronisch oder auf Papier. Dort wird zum Beispiel gefragt,

- welche personenbezogenen Daten Sie am Arbeitsplatz verarbeiten,
- zu welchem Zweck Sie das tun und
- wie lange die Daten aufbewahrt werden.

Die Antworten darauf wirken manchmal recht banal. Beispielsweise ist jedem klar, dass eine Versandabteilung Kundendaten verwendet, um Bestellungen zu bearbeiten. Aber das muss eben festgehalten werden. Im Übrigen zeigt das Beispiel, dass das Formular oft schnell ausgefüllt ist. Der Aufwand hält sich also meistens in Grenzen.

### **Zögern Sie nicht lange!**

Lassen Sie entsprechende Anfragen nicht lange liegen! Denn alle Meldungen aus dem Unternehmen zu einem Verzeichnis zusammenzuführen – das braucht durchaus etwas Zeit. Und ab 25. Mai 2018 muss das Verzeichnis fix und fertig vorliegen. Sonst kann es für das Unternehmen Ärger geben.

### **„Verarbeitungen auf Papier“**

Eines wundert viele: In das Verzeichnis müssen auch „Verarbeitungen“ aufgenommen werden, bei denen keine EDV zum Einsatz kommt. Klar: Diese Fälle werden seltener. Aber da und dort gibt es immer noch Hängeregistaturen, die alphabetisch nach den Namen geordnet sind, um nur ein typisches Beispiel zu nennen. Auch das ist dann eine „Verarbeitung“, die in das Verzeichnis muss. Dasselbe würde natürlich für Karteikarten gelten, die nach Namen geordnet sind.

### **Überflüssige Datenträger entsorgen!**

Eine solche Kartei steht zwar noch herum, wird aber gar nicht mehr benutzt? Das hilft nichts, sie muss trotzdem in das Verzeichnis. Vielleicht ein guter Anlass, die Kartei

endlich einmal zu entsorgen. Doch fragen Sie bitte vorher genau nach, ob sie wirklich weg kann oder aus irgendwelchen Gründen doch noch aufgehoben werden muss. Das kann durchaus vorkommen, etwa weil die Steuergesetze das vorschreiben.

### **Kein Einsichtsrecht für Betroffene**

Dürfen eigentlich Betroffene Einsicht in das Verzeichnis nehmen? Dürfte also beispielsweise ein Kunde verlangen, dass er hineinschauen darf? Nein. So etwas gab es früher einmal. Jetzt ist das nicht mehr vorgesehen. Das Verzeichnis ist eine rein interne Angelegenheit.

### **Aufbewahrung des Verzeichnisses**

Wo das Verzeichnis geführt wird, kann das Unternehmen selbst festlegen. Oft liegt es beim Datenschutzbeauftragten. Eine Aufbewahrung durch eine andere Stelle ist aber auch möglich. Für den Datenschutzbeauftragten ist das Verzeichnis wichtig, weil er einen Überblick haben muss, wo personenbezogene Daten liegen.

### **Zulässige Sprachen: Deutsch und Englisch**

Normalerweise ist das Verzeichnis in deutscher Sprache zu führen. Die Aufsichtsbehörden für den Datenschutz akzeptieren es aber auch, wenn Englisch verwendet wird. Hier hat das Unternehmen also die Wahl.

Manche Unternehmen legen dabei einen Katalog der englischen Begriffe fest, die verwendet werden dürfen. Das hat dann gute Gründe. Denn wenn eine Aufsichtsbehörde den Inhalt des Verzeichnisses sprachlich nicht versteht, kann sie eine Übersetzung fordern. Sprachliche Originalität ist deshalb hier fehl am Platz.

\* \* \* \*



### **Die DSGVO und Daten auf Papier**

**Der Datenschutz soll uns vor „Gefahren der EDV“ bewahren – so hört man es häufig. Dabei gehen von Daten auf Papier oft viel größere Risiken für den Schutz personenbezogener Daten aus. Deshalb gilt die Datenschutz-Grundverordnung (DSGVO) auch für Daten auf Papier.**

**EDV = böse, Papier = harmlos?**

Sie wollen nicht glauben, dass Daten auf Papier für den Datenschutz gar nicht so harmlos sind? Dann

stellen Sie sich einfach zwei Fragen:

- Sehen Sie es Daten auf Papier an, ob jemand diese Daten gelesen hat?
- Sehen Sie es Daten auf Papier an, ob jemand das Papier kopiert hat?

Beide Fragen sind natürlich mit Nein zu beantworten. Wären die Daten statt auf Papier in elektronischer Form gespeichert, sähe das Ganze etwas anders aus. Lesezugriffe lassen sich genauso einfach protokollieren wie ein Download von Daten. Ob jemand erlaubt gehandelt hat oder nicht, kommt im Ernstfall daher schnell ans Licht.

### **Papier ist nicht „besser“!**

Klar, lückenlos funktioniert auch das nicht. So könnte jemand, der dazu berechtigt ist, Daten am Bildschirm aufrufen. Dann könnte er mit seinem Smartphone ein Foto des Bildschirms machen. Und schon hätte er das Verbot, die Daten zu kopieren, umgangen. Dennoch ändern solche Ausnahmefälle nichts am Prinzip: Personenbezogene Daten auf Papier sind mindestens genauso gefährdet wie elektronische Daten, wenn nicht sogar noch viel stärker!

### **Schreiben als Speicherung von Daten**

Die DSGVO hat daraus die nötigen Folgerungen gezogen. Sie gilt unabhängig davon, ob Daten auf Papier gespeichert sind oder in elektronischer Form. Sie haben richtig gelesen: Auch das Festhalten von Daten auf Papier, ob mit Bleistift oder Drucker, bezeichnet die DSGVO als Speicherung von Daten! Das wirkt auf den ersten Blick ungewohnt. Aber wenn man kurz überlegt, ist das nur konsequent.

### **Schreiben als Verarbeitung von Daten**

Haben Sie diese gedankliche Hürde genommen, fallen Ihnen einige andere Aspekte der DSGVO nicht mehr schwer. Die DSGVO gilt ausdrücklich auch für die „nicht automatisierte Verarbeitung personenbezogener Daten“. So sagt es Art. 2 Abs. 1 DSGVO. Eine Form der Verarbeitung ist die Speicherung. Das definiert Art. 4 Nr. 2 DSGVO. Aus beidem zusammen folgt: Wer Daten auf Papier festhält, verarbeitet diese Daten, und zwar nicht automatisiert.

### **Notizzettel = „Dateisystem“?**

Heißt das, man muss nun für jeden Notizzettel die DSGVO beachten? So weit geht die DSGVO nicht. Falls Daten nicht automatisiert verarbeitet werden, findet die DSGVO nämlich nur Anwendung, wenn die Daten „in einem Dateisystem gespeichert sind.“ So sagt es Art. 2 Abs. 1 DSGVO.

Sie verzweifeln allmählich etwas, weil das schon wieder ein neuer Begriff ist? Keine Sorge! Dieser Begriff ist klar definiert: Ein „Dateisystem“ ist jede strukturierte Sammlung personenbezogener Daten (Art. 4 Nr. 6 DSGVO). Beispiele für solche strukturierten Sammlungen sind Karteien und Hängeregistaturen, aber auch alphabetisch sortierte Unterlagen in Ordnern. Ein ungeordneter Haufen mit Notizzetteln fällt also nicht unter die DSGVO. Datenschutzgerecht entsorgen sollten sie ihn bitte trotzdem!





---

## Impressum

### Redaktion:

Peter Brandmann (V.i.S.d.P.)  
Externer Datenschutzbeauftragter nach § 40 Abs. 6 BDSG-neu  
Zertifizierte Fachkraft DSGVO nach Art. 37 Abs. 5 DSGVO

### Anschrift:

pb beratung & training  
Inhaber: Peter Brandmann  
Schneppenreuther Weg 51  
90425 Nürnberg

Telefon: 0911 3506118

E-Mail: [peter.brandmann@pb-beratung-training.de](mailto:peter.brandmann@pb-beratung-training.de)