Newsletter Datenschutz

Ausgabe April | 2018

# Newsletter der Sanovis GmbH

Liebe Leserin, lieber Leser,

die Datenschutz-Grundverordnung steht vor der Tür. Mit ihr sind zahlreiche Änderungen im Datenschutz verbunden, auf die Sie sich vorbereiten müssen. Ihre neue Ausgabe hilft Ihnen dabei. Eine wichtige Rolle kommt der Frage zu, wo sich die zu schützenden Daten befinden. Ist es zum Beispiel erlaubt, betriebliche E-Mails nach Hause weiterzuleiten oder müssen diese auf betrieblichen Geräten verbleiben? Wie findet man seine eigenen Daten im Internet, wenn man sie löschen lassen will?
Für den Datenschutz ist Transparenz in der Datenhaltung entscheidend. Gleichzeitig kommt der Vertraulichkeit personenbezogener Daten eine große Bedeutung zu. Deshalb erfahren Sie auch, wie es um die Verpflichtung auf das Datengeheimnis in Zeiten der Datenschutz-Grundverordnung steht.
Wir wünschen Ihnen wieder viele wertvolle Einsichten in den Datenschutz!

*Ihr Dr. Uwe Günther, Geschäftsführer, Sanovis GmbH, Geschäftsfeldeiter Datenschutz, Curacon GmbH*

## Die Verpflichtung auf das Datengeheimnis

**Wer in einem Unternehmen mit personenbezogenen Daten umgeht, muss auf das Datengeheimnis verpflichtet sein. So war man es bisher gewohnt. Die Datenschutz-Grundverordnung (DSGVO) sieht keine förmliche Verpflichtung mehr vor. Trotzdem werden Unternehmen auch in Zukunft eine Verpflichtung unterzeichnen lassen.**

### Ende eines gewohnten Rituals?

Es gehört zum gewohnten Ritual: Wer neu in ein Unternehmen eintritt, muss eine „Verpflichtung auf das Datengeheimnis" unterschreiben. Dazu erhält er ein Infoblatt. Hintergrund ist eine entsprechende Regelung im bisherigen Bundesdatenschutzgesetz (BDSG-alt). Am 25. Mai 2018 löst die DSGVO das BDSG-alt ab. Die DSGVO enthält keine Regelung mehr, wonach Beschäftigte auf das Datengeheimnis zu verpflichten sind. Das hört sich zunächst nach einem willkommenen Abbau von Bürokratie an. Doch so einfach ist es nicht.

### Herausforderung „Rechenschaftspflicht"

Die DSGVO verpflichtet alle Unternehmen dazu, die Datenschutzvorschriften zu beachten. Zusätzlich sieht sie eine „Rechenschaftspflicht" vor. Das heißt: Unternehmen müssen nachweisen können, dass sie die DSGVO tatsächlich beachten. Zur Einhaltung der DSGVO gehört es, den Mitarbeitern zu verdeutlichen, welche Pflichten sie im Datenschutz haben. Dazu braucht es eine Art Belehrung. Sie muss schriftlich dokumentiert sein. Anders lässt sich nicht nachweisen, dass den Mitarbeitern ihre Pflichten klar waren.

### Muster der Datenschutzaufsicht

Auf der Webseite des Bayerischen Landesamts für Datenschutzaufsicht findet sich das Muster „Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)". Es führt die wesentlichen Grundsätze auf, die im Datenschutz zu beachten sind. Damit erinnert es nur an das, was sich ohnehin schon aus dem Gesetz ergibt. Der Text schafft keine Pflichten, die dort nicht enthalten sind. Von daher gibt es keinen Grund für einen Beschäftigten, die Unterschrift zu verweigern.

### Kreis der zu Verpflichtenden

Zu verpflichten sind alle Personen, die mit personenbezogenen Daten umgehen. Das sind außer der „Stammbelegschaft" auch Auszubildende, Praktikanten und Leiharbeiter. Wichtig ist, dass die Verpflichtung bei Aufnahme der Tätigkeit erfolgt. Also spätestens am ersten Arbeitstag. Selbstverständlich kann sie jedoch auch schon vorher geschehen.

### Inhalt statt Formalie!

Die Inhalte der Verpflichtung sind das eigentlich Wichtige. Aus diesem Grund wäre es auch nicht gut, die Verpflichtung als eine lästige Formalie anzusehen nach dem Motto: „Das haken wir am ersten Arbeitstag schnell ab, und dann liegt das Formular eben jahrelang in der Personalakte." Die Datenschutzaufsicht empfiehlt, alle Beschäftigten immer wieder einmal daran zu erinnern, dass die Verpflichtung weiterhin gilt und was sie bedeutet. Dies kann durch Aushänge, aber auch zum Beispiel durch eine E-Mail an alle oder in Schulungen geschehen. Hier können die Unternehmen wählen.

## Weiterleitung von E-Mails „nach Hause"

**Viele Arbeitnehmer tun es gelegentlich: Sie leiten eine dienstliche E-Mail nach Hause auf den privaten E-Mail-Account um. Alles kein Problem? Es kommt darauf an! Nicht alles, was einem Arbeitnehmer vernünftig erscheint, ist es auch aus der Sicht der Gerichte.**

### Vernünftige Gründe

Die Gründe für das Weiterleiten einer E-Mail sind unterschiedlich. Ein Beispiel: Tagsüber hat die Zeit nicht gereicht, um eine wichtige, aber ziemlich umfangreiche E-Mail zu lesen. Also möchte man das abends zuhause nachholen. Ein weiteres Beispiel: Eigentlich möchte man am nächsten Tag im Homeoffice das dienstliche mobile Gerät nutzen. Gerade jetzt „spinnt" es aber. Also weicht man mit den wichtigsten E-Mail-Nachrichten sozusagen auf den privaten PC aus.

### Ein problematischer Fall

Diese Argumente hören sich vernünftig an. Doch, dass man auch rasch in ein problematisches Licht geraten kann, musste ein Arbeitnehmer in einem Fall erfahren, den das Landesarbeitsgericht Berlin-Brandenburg am 16. Mai 2017 entschieden hat. Ein Mitarbeiter hatte an einem einzigen Tag in einem Zeitraum von 90 Minuten nicht weniger als 96 E-Mails an seine private E-Mail-Adresse geschickt. Fast jede dieser E-Mails hatte umfangreiche Anhänge. Der Gesamtumfang der E-Mail-Nachrichten einschließlich der Anhänge betrug fast 1.300 Seiten.

### Berechtigte Fragen des Arbeitgebers

Als der Arbeitgeber dies bemerkte, begann er, Fragen zu stellen. Die Antworten des Arbeitnehmers darauf waren eher „windelweich". Besonderen Verdacht schöpfte der Arbeitgeber, als er erfuhr, dass der Arbeitnehmer zu diesem Zeitpunkt bereits ein gutes Angebot für eine Arbeitsstelle bei einem Konkurrenzunternehmen erhalten hatte. Die Befürchtung lag nahe, dass der Arbeitnehmer nützliche Informationen zum neuen Arbeitgeber mitnehmen wollte. Sie verstärkte sich, als der bisherige Arbeitgeber erfuhr, dass der Arbeitnehmer tatsächlich einen Arbeitsvertrag mit dem Konkurrenzunternehmen abgeschlossen hatte.

### Fristlose Kündigung rechtens

Die Reaktion des Arbeitgebers kann nicht überraschen: Er kündigte dem Mitarbeiter fristlos. Damit hatte der Arbeitgeber Erfolg. Denn das Landesarbeitsgericht bestätigte die Wirksamkeit der Kündigung. Folgende Aspekte waren dabei aus Sicht des Gerichts besonders wichtig:

- Wer ohne nachvollziehbaren Grund zahlreiche E-Mails an seine private E-Mail-Anschrift weiterleitet, verletzt in schwerwiegender Weise die Pflicht, auf die Interessen seines Arbeitgebers Rücksicht zu nehmen.
- Das gilt insbesondere, wenn er in Verhandlungen mit einem neuen Arbeitgeber steht und der neue Arbeitgeber ein Konkurrenzunternehmen betreibt.
- Es ist Sache des Arbeitnehmers, eine dienstliche Notwendigkeit für die Weiterleitung darzulegen.

### Vorsicht mit dem Argument „Homeoffice"!

Wenig wissen wollte das Gericht von dem Argument, dass dem Arbeitnehmer Arbeit im Homeoffice erlaubt gewesen sei. Allein daraus ergibt sich keine Genehmigung, E-Mails auf den privaten E-Mail-Account weiterzuleiten. Dies gilt vor allem dann, wenn der Arbeitgeber für die Arbeit zuhause ein dienstliches Notebook zur Verfügung stellt. Und genau das war vorliegend der Fall. Eine Speicherung auf einem privaten Computer ist dann für die Arbeit nicht erforderlich.

### Faustregeln und Empfehlungen

Daraus ergeben sich folgende Ratschläge für die Praxis:

- Bedenken Sie, dass dienstliche E-Mails oft Geschäftsgeheimnisse enthalten. Aufwändige Schutzmechanismen Ihres Unternehmens helfen nichts, wenn Sie diese Vorkehrungen durch eine Weiterleitung von E-Mails an Ihren privaten Account unterlaufen.
- Deshalb gilt: Wenn Sie dienstliche E-Mails an Ihren privaten E-Mail-Account weiterleiten wollen, sollten Sie vorher

  mit Ihrem Arbeitgeber klären, ob das in Ordnung geht. Das vermeidet spätere Streitigkeiten.

- Seien Sie vorsichtig mit der Überlegung, eine solche Weiterleitung erleichtere doch nur die Arbeit. Dies gilt auch, wenn Sie von zuhause aus arbeiten dürfen (Homeoffice). Ihr Arbeitgeber sieht die Dinge möglicherweise ganz anders.
- Besonders kritisch wird es, wenn Ihnen für die Arbeit zuhause ein dienstliches Gerät zur Verfügung steht. Dann gibt es im Normalfall keinen nachvollziehbaren Grund, stattdessen ein privates Gerät einzusetzen.
- Sollte dies ausnahmsweise doch einmal erforderlich sein, weil zum Beispiel technische Defekte beim dienstlichen Gerät vorliegen, melden Sie diese Defekte umgehend dem Arbeitgeber! Dann kann man absprechen, wie verfahren wird.

Wer die Entscheidung des Gerichts im Original nachlesen möchte, sollte bei Google einfach das Aktenzeichen „7 Sa 38/17" eingeben. Angst vor Juristendeutsch sollte man dabei freilich nicht haben.

## DSGVO: Transparenz bei den Daten ist Trumpf

**Die in Kürze anzuwendende Datenschutz-Grundverordnung (DSGVO) enthält viele Vorgaben für den Datenschutz. Gemeinsam ist ihnen: Man muss zunächst einen Überblick darüber haben, welche zu schützenden personenbezogenen Daten vorhanden sind. Wie aber gewinnt man die notwendige Übersicht?**

### Unternehmen müssen wissen: Wo sind die Daten?

Die Datenschutz-Grundverordnung enthält eine Reihe von Rechten für die Betroffenen, deren personenbezogenen Daten verarbeitet werden. Es bestehen Informationspflichten bei der Datenerhebung, Auskunftsrechte, Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit, Widerspruchsrechte, und es gibt das Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu sein. Bevor ein Unternehmen aber diese Pflichten und Rechte umsetzen kann, muss es wissen, wo es welche Daten von welchen Betroffenen zu welchem Zweck verarbeitet.

Genau hier haben viele Unternehmen Probleme: Als größte Herausforderung sehen die deutschen Unternehmen dabei die Anforderungen des Artikels 17 (Recht auf Löschung/Vergessenwerden; 63 Prozent). Der Grund hierfür sind nicht nur die Schwierigkeiten, Daten sicher und vollständig zu löschen. Vielen Unternehmen fehlt die Übersicht, wo denn die Daten überhaupt sind.

### Sie können dabei helfen, Transparenz herzustellen

Die notwendige Übersicht über die Datenhaltung ist heute aus mehreren Gründen schwieriger. Früher waren die Computer, mit denen die Daten verarbeitet wurden, im Büro und nicht mobil, wie dies die Notebooks, Tablets und Smartphones sind. Die Bürobeleuchtung und die Heizung waren noch nicht vernetzt, es gab kein Internet der Dinge. Ebenso gab es keine Cloud-Dienste in dem Umfang, wie sie heute verfügbar sind. Private IT-Geräte waren noch privat und nicht so leistungsfähig, dass man in Versuchung geraten konnte, diese beruflich zu nutzen. Diese Zeiten aber sind vorbei. Umso wichtiger ist es, dass Sie als Mitarbeiterin oder Mitarbeiter dabei helfen, eine bessere Übersicht über die Daten zu bekommen.

Die Transparenz bei den Daten erfordert, dass Sie selbst Transparenz bieten. Es geht dabei nicht darum, dass man jede Ihrer Aktivitäten haarklein nachvollziehen kann. Sondern darum, dass die IT-Abteilung wissen muss, welche Geräte im Einsatz sind, welche Cloud-Dienste die Mitarbeiter verwenden und ob sie genehmigte Privatgeräte nutzen. Tatsächlich ist die sogenannte Schatten-IT, also die IT, die sich unabhängig von der an sich zuständigen IT-Abteilung bildet, eine große Gefahr für die Transparenz und den Datenschutz.

### Mehr Transparenz, keine Schatten-IT

Wer glaubt, das Problem „Schatten-IT" sei schon lange genug bekannt und deshalb gelöst, irrt leider. Wie eine aktuelle Studie von VMware und Forbes zur Digitalisierung der Arbeitswelt ergab, hat das Thema nichts an Aktualität eingebüßt. Wer die nötigen technologischen Helfer nicht von seinem Unternehmen zur Verfügung gestellt bekommt, besorgt sie sich weiterhin selbst ohne offizielle Absprache mit der Unternehmens-IT. Mittlerweile wurde bereits jede fünfte Anwendung in Unternehmen in ganz Europa von Mitarbeitern selbst eingeführt, so ein weiteres Ergebnis der Studie. Damit stellt Schatten-IT europaweit immer noch eine große Herausforderung für Unternehmen dar.

### Ganz konkrete Praxistipps

Wenn Sie dazu beitragen, die Schatten-IT zu verhindern, helfen Sie mit, die Transparenz über die Datenhaltung zu erhöhen. Damit legen Sie eine Grundlage dafür, dass die Datenschutz-Grundverordnung und die damit verbundenen Betroffenenrechte besser eingehalten und umgesetzt werden können. Notwendig sind dafür folgende Schritte:

1. Nutzen Sie nur die betrieblichen Endgeräte und Speichermedien. Private Geräte dürfen Sie nur betrieblich nutzen, wenn der Arbeitgeber dies ausdrücklich erlaubt hat. Private Speichermedien sollten generell tabu sein. Fragen Sie stattdessen nach einem USB-Stick bei der zuständigen Stelle im Unternehmen, wenn Sie ein Speichermedium brauchen.
2. Wenn Sie neue oder andere Anwendungen oder Apps benötigen, fragen Sie die zuständige Stelle im Unternehmen. Mobile Apps lassen sich zwar meist selbst auf dem Smartphone installieren und viele Cloud-Apps stehen kostenlos über den Browser zur Verfügung. Doch mit diesen Apps können Risiken für das Unternehmen und die Daten verbunden sein. In jedem Fall führen nicht zugelassene Apps dazu, dass die Transparenz über die Datenhaltung und Datenverarbeitung sinkt – und das ist ein Problem bei der Einhaltung der DSGVO. Das darf nicht mehr sein!

**Impressum**

**Redaktion:**
Dr. Uwe Günther
Sanovis GmbH

**Anschrift:**
Richard-Strauss-Str. 69
81679 München
Telefon: +49 89 99 27 579 22
E-Mail: Uwe.Guenther@Sanovis.com

## Eigene Daten finden und löschen lassen

**Umfragen zeigen, dass viele Verbraucher von dem Recht auf Vergessenwerden Gebrauch machen wollen. Trifft das auch auf Sie zu? Dann sollten Sie zuerst wissen, wie Sie Ihre Daten im Internet überhaupt finden können. Hier sind einige Tipps.**

### Betroffenenrechte selbst nutzen

82 Prozent der Verbraucher in Europa wollen ihre neuen Rechte aus der Datenschutz Grundverordnung (DSGVO) ausüben und die Daten, die Unternehmen zu ihnen erfassen, einsehen, begrenzen oder löschen, so eine Umfrage von Pegasystems. Sogar ganze 90 Prozent wollen sich darüber informieren, wie ihre Daten verwendet werden. Für mehr als die Hälfte (57 Prozent) ist es sehr wichtig, die Nutzung persönlicher Daten direkt zu kontrollieren. Für 31 Prozent ist dies zumindest noch wichtig.

Die deutliche Mehrheit (93 Prozent) würde das Recht zur Datenlöschung nutzen, wenn Unternehmen ihre Daten auf eine Weise nutzen, mit der sie nicht einverstanden sind. 89 Prozent würden das Geschäftsverhältnis daraufhin ganz kappen. Über Dreiviertel der Befragten (78 Prozent) bevorzugen Unternehmen, die mit den Daten offen und transparent umgehen. Knapp die Hälfte der Befragten (47 Prozent) würde ihre Daten gelöscht haben wollen, wenn Unternehmen die Informationen mit anderen Unternehmen austauschen oder gar verkaufen würden.

Es stellt sich die Frage: Wie ist es mit Ihnen? Wollen auch Sie zum Beispiel das Recht auf Vergessenwerden nutzen? Doch wie geht das eigentlich?

### Misstrauen ist weit verbreitet

In der Global-Trends-Studie von Ipsos gab jeder Zweite (54 Prozent) an, sich bei der Weitergabe seiner Daten unwohl zu fühlen. Nur jeder fünfte Internetnutzer (20 Prozent) in Deutschland hält seine Daten im Netz für sicher, wie eine weitere Befragung des Digitalverbands Bitkom ergab.

78 Prozent geben dagegen an, ihre Daten seien online eher (40 Prozent) oder völlig (38 Prozent) unsicher. Das höchste Vertrauen bei den Bürgern genießen beim Umgang mit ihren Daten der eigene Internet-Zugangsanbieter sowie der eigene E-Mail-Anbieter (je 49 Prozent). Das geringste Vertrauen wird den sozialen Netzwerken entgegengebracht (15 Prozent).

### Welche Daten sind bereits im Internet?

Wenn Sie selbst nun Ihre Daten zum Beispiel bei sozialen Netzwerken oder anderen Online-Diensten löschen lassen, also von Ihrem Recht auf Vergessenwerden Gebrauch machen wollen, stehen Sie vor einer Herausforderung: Wer hat Ihre Daten bekommen, und zwar von Ihnen selbst? Das ist weitaus schwieriger zu beantworten, als man im ersten Moment glauben mag. Bei der Vielzahl an Online-Diensten und Apps, die man nutzt, und mehr noch bei der enormen Zahl der Dienste, bei denen man sich einmal angemeldet hat und die man nicht oder nicht mehr nutzt: Wer hat da noch die Übersicht?

### Tipp: Suchmaschinen und spezielle Tools können helfen

Aus Sicht des Datenschutzes lautet die Empfehlung natürlich Datensparsamkeit, die Datenschutz-Grundverordnung spricht von Datenminimierung. So wichtig es auch ist, sich an dieses Prinzip zu halten: Sind die Daten bereits im Internet veröffentlicht, hilft Datenminimierung auch nicht mehr. Stattdessen müssen Sie auf Datensuche gehen, Sie müssen sich also selbst im Internet suchen. Hier erweisen sich Suchmaschinen wie ixquick.de oder duckduckgo.com als hilfreich. Über diese Tools können Sie nach Ihren eigenen Daten suchen, ohne die bei Suchmaschinen üblichen Nutzerspuren zu erzeugen.

Hat man möglichst viele seiner Daten gefunden, beginnt das Verfahren, entsprechende Löschanfragen zu erstellen. Hier bieten spezielle Tools und Dienste ihre Hilfe an. Sie suchen die Daten des Nutzers und helfen bei den Anfragen zur Löschung bei den jeweils verantwortlichen Stellen. Ein Beispiel für einen solchen Dienst ist Privacy Audit (http://privacyaudit.me/en/). Der Dienst listet die gefundenen Daten des Nutzers, bewertet die Risiken der Veröffentlichung und unterstützt bei den Löschanfragen.

**Haben Sie Ihre Daten im Griff? Testen Sie sich!**

**Frage:** ***Wenn Google Daten aus seinem Datenbestand löscht, sind sie aus dem Internet verschwunden. Stimmt das?***

a. **Nein, die Daten wären dann nur bei Google gelöscht.**
b. **Ja, was man bei Google nicht findet, ist nicht mehr im Internet.**

Lösung: Die Antwort a. ist richtig. Löschanfragen bei Google entfernen die Daten nicht dort, wo Google sie gefunden hat, also zum Beispiel nicht bei Webseiten oder sozialen Netzwerken, die Daten über einen Nutzer haben. Man muss jeweils die verantwortliche Stelle kontaktieren.

**Frage:** ***Das Recht auf Vergessenwerden garantiert die Umsetzung eines jeden Löschwunsches. Stimmt das?***

a. **Nein, die DSGVO enthält genaue Bedingungen dafür.**
b. **Ja, denn nur so kann man im Internet wirklich vergessen werden.**

Lösung: Die Antwort a. ist auch hier richtig. Nicht jeder Wunsch auf Datenlöschung muss umgesetzt werden. Der Artikel 17 der DSGVO enthält einen Kriterienkatalog. Das Recht auf Vergessenwerden gilt zum Beispiel dann nicht, wenn die Verarbeitung der Daten erforderlich ist zur Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.