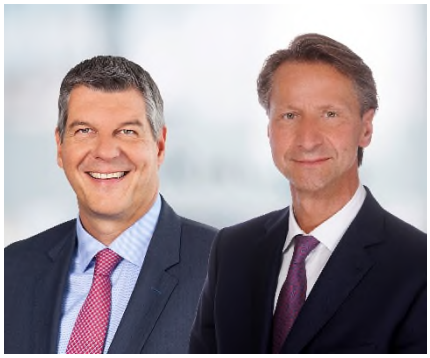
SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ



Liebe Leserin, lieber Leser,

wenn Sie sich über Cookie-Banner ärgern, dann sollten Sie wissen, wer diese Banner wirklich notwendig macht. Denn es ist an sich nicht der Datenschutz. Sie sollten aber auch die Tricks kennen, mit denen Cookie-Banner Ihre Einwilligung erschleichen wollen. Mehr dazu lesen Sie auf der ersten Seite Ihres neuen Newsletters.
Gut gemeint ist nicht immer gut gemacht, das gilt auch im Datenschutz. Erfahren Sie deshalb, worauf Sie bei Outlook-Einträgen zum Beispiel bei Bewerbungsgesprächen achten sollten. Lernen Sie aber auch den Unterschied zwischen Aufbewahrung und Archivierung sowie die Folgen für die Löschpflichten kennen.
Nicht zuletzt erfahren Sie diesmal, was es mit der sogenannten Verpflichtung auf das Datengeheimnis auf sich hat. Denn Sie sollten wissen, worauf Sie sich dabei genau verpflichten, damit das Datengeheimnis für Sie „kein Geheimnis“ mehr ist.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

April_2023

1 DAS SIND DIE TRICKS BEI COOKIE-BANNERN

Cookie-Banner sind unbeliebt und lästig. Und schuld daran ist der Datenschutz, so denken viele. Doch das stimmt nicht. Aber das ist nicht das Einzige, was bei Cookie-Bannern häufig nicht richtig ist. Viele Cookie-Banner missachten Vorgaben.

Nicht der Datenschutz will Cookie-Banner

Eine gut gemachte und faire Internetseite benötigt kein Cookie-Banner, weil sie nur technisch notwendige Cookies verwendet, so der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber.

Es sind die Website-Betreibenden, die personenbezogene Daten sammeln möchten und deshalb über Cookie-Banner die erforderliche Einwilligung der Nutzenden einholen müssen. Aber das ist nicht alles: Es sind nicht nur die Betreiber der betreffenden Websites, die Cookie-Banner notwendig machen. So manche arbeiten dabei auch mit unfairen oder rechtswidrigen Mitteln.

Datenschutzaufsichtsbehörden berichten von Tricks bei Cookie-Bannern

Der Ausschuss der Datenschutzaufsichtsbehörden in der EU (Europäischer Datenschutzausschuss) hatte dazu eine Task Force Cookie-Banner gebildet, die nun ihren Abschlussbericht veröffentlicht hat. Darin sind viele Abweichungen von den Vorgaben für eine rechtsgültige, freiwillige und informierte Einwilligung beschrieben, die bei Cookie-Bannern verschiedener Websites aufgedeckt wurden.

Öffnet man zum Beispiel eine Webseite und baut sich dort ein Cookie-Banner auf, das es leicht macht, alle Cookies zu akzeptieren, wo aber ein Ablehnen der optionalen Cookies augenscheinlich nicht möglich ist, dann entspricht dies nicht den rechtlichen Vorgaben. Die fehlende Schaltfläche zum Ablehnen der Cookies ist jedoch nur ein Beispiel von vielen.

Viele Cookie-Banner sind irreführend

Ber Der Bericht der Task Force Cookie-Banner zeigt, wie vielfältig die Tricks bei Cookie-Bannern sein können, mit denen Website-Betreiber die Einwilligung der betroffenen Nutzenden nicht erfragen, sondern vielmehr erschleichen wollen.

- Betreiber von Websites stellen Optionen zur Auswahl dar mit vorab angekreuzten Kästchen.
- Die Cookie-Banner enthalten einen Link und keine Schaltfläche, um die Cookies abzulehnen. Dabei wird das Ablehnen erst durch Öffnen mehrerer Unterseiten möglich. Das verkompliziert und erschwert eine Ablehnung.
- Der „Akzeptieren“-Button ist deutlich hervorgehoben, die Schaltfläche „Alle akzeptieren“ ist gut sichtbar, Schaltflächen für das Ablehnen oder für andere Optionen dagegen nicht.
- Website-Betreiber bezeichnen Cookies als „wesentlich“ oder „unbedingt erforderlich“, die aber technisch nicht erforderlich sind und nur der Sammlung personenbezogener Daten dienen, sodass das Ablehnen optionaler Cookies diese nicht betrifft.

Tipp: Lieber verzichten als auf Tricks reinzufallen

Treffen Sie auf eine Website, die es komplizierter macht, optionale Cookies abzulehnen als sie zu akzeptieren, ist Vorsicht angesagt. Cookies, die nicht technisch erforderlich sind, um den gewünschten Onlinedienst zu erbringen, müssen freiwillig sein. Es muss umfassende Informationen darüber geben, wie sie genutzt werden sollen und was mit den auf diese Art gesammelten personenbezogenen Daten geschehen soll.

Cookie-Banner, die gegen die Vorgaben einer informierten und freiwilligen Einwilligung verstoßen, sind genau wie unvollständige oder feh-

lende Datenschutzerklärungen ein Warnzeichen. Wo immer möglich, verzichten Sie auf den Besuch solcher Websites.

2 OUTLOOK-EINLADUNG ZU BEWERBUNGSGESPRÄCHEN

An Gesprächen mit Bewerbern nehmen in einem Unternehmen normalerweise mehrere Personen teil. Eine Termineinladung über Outlook bringt die Akteure zusammen. Welche Informationen über den Bewerber oder die Bewerberin dürfen dabei im Outlook-Kalender und in der Outlook-Einladung enthalten sein?

Bewerbungsgespräche erfordern Terminvereinbarungen

Ein Unternehmen erhält immer wieder Vermittlungsangebote der Agentur für Arbeit. Die Termine für die nötigen Bewerbungsgespräche lässt es im Outlook-Kalender eintragen. Die Eintragungen enthalten immer den Namen des Bewerbers oder der Bewerberin und Angaben zu der Stelle, auf die sich das Vermittlungsangebot bezieht. In manchen Fällen kommen noch weitere Informationen hinzu. Vor allem wird festgehalten, ob der Bewerber früher schon einmal Vorstellungstermine versäumt hat.

Eintragungen im Outlook-Kalender sind rasch ein Problem

Das Unternehmen war unsicher, ob das alles so korrekt ist. Deshalb bat es das Bayerische Landesamt für Datenschutzaufsicht um Beratung. Die Antwort des Landesamts fällt differenziert aus.

Keine Probleme hat es damit, dass der Name des Bewerbers im Kalender und in der Einladung steht. Es hat auch nichts dagegen, dass das Stichwort „Bewerbungsgespräch“ enthalten ist. Bei allem, was darüber hinausgeht, sieht es aber erhebliche Probleme.

Zugriffs- und Löschungskonzept müssen funktionieren

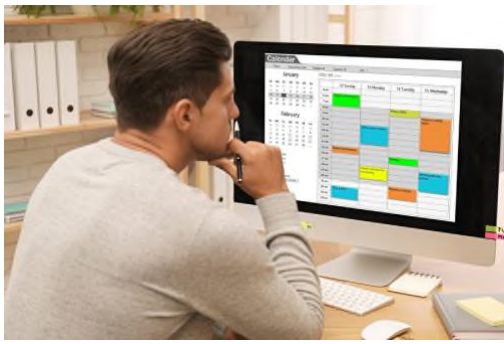
Unternehmen dürfen Daten von Personen, die sich bewerben, nur an einem Speicherort speichern, der dazu aus der Sicht des Datenschutzes geeignet ist. Dafür muss der Speicherort zwei Kriterien genügen:

- Zum einen muss ein Zugriffskonzept vorhanden sein. Es muss also genau definiert sein, wer auf die Daten zugreifen kann.
- Zum anderen muss für den Speicherort ein Löschkonzept bestehen. Es muss also feststehen, wann gespeicherte Daten wieder gelöscht werden. Sie dürfen nur so lange gespeichert werden, wie das erforderlich ist.

Bei Outlook-Kalendern ist das oft schwierig

Wichtig dabei: All dies darf nicht nur auf dem Papier stehen. Vielmehr muss es in der Realität auch tatsächlich „gelebt“ werden. Mit Recht bemerkt das Landesamt, dass diese beiden Kriterien bei Outlook-Kalendern in der Praxis kaum je erfüllt werden. Dies scheitert schon an den üblichen Vertretungsregelungen für Mail-Postfächer. Sie führen dazu, dass immer wieder auch solche Mitarbeiter Daten wahrnehmen können, die überhaupt nicht an Bewerbungsgesprächen beteiligt sind.

Outlook verleitet zu großzügigen Zugriffsregelungen



Aber auch die Kalenderfreigaben sind vielfach sehr großzügig ausgestaltet. Das soll Terminplanungen mit mehreren Beteiligten erleichtern. Es kann aber auch dazu führen, dass Mitarbeiter Zugriff auf Kalenderdaten haben, obwohl es nicht erforderlich wäre. Dasselbe gilt bei Gruppenpostfächern, auf die mehrere Personen Zugriff haben.

Ergänzende Unterlagen gehören nicht in Outlook-Kalender

Vor diesem Hintergrund will das Landesamt nichts davon wissen, dass Bewerbungsunterlagen, Gesprächsnotizen und Vorbereitungsvermerke für ein Bewerbungsgespräch im Outlook-Kalender gespeichert werden. Sie gehören aus seiner Sicht dort nicht hin, sondern vielmehr in die Obhut der Stelle, die für Personalangelegenheiten im Unternehmen zuständig ist. Sie kann den Personen einen Zugriff einräumen, die am konkreten Bewerbungsverfahren mitwirken.

Die Löschung aller Daten muss sichergestellt sein

Besonderen Wert legt das Landesamt auf die ordnungsgemäße Löschung der Daten nach dem Abschluss eines Bewerbungsverfahrens. Dabei sieht es durchaus, dass auch dann noch ein Zugriff auf Bewerberdaten erforderlich sein kann. Das gilt etwa, wenn Berichtspflichten des Unternehmens gegenüber der Agentur für Arbeit bestehen.

Der Auskunftsanspruch von Bewerbern geht sehr weit

In der Praxis sollte man sich die Frage stellen, ob man nicht sogar auf den Namen des Bewerbers im Outlook-Kalender verzichten sollte. Denn es kommt immer wieder vor, dass ein Bewerber Auskunftsansprüche nach Art. 15 DSGVO geltend macht.

Dies ist besonders häufig, wenn jemand die Stelle nicht bekommen hat und beispielsweise behauptet, das liege an einer Diskriminierung seiner Person. Viele Juristen sind der Auffassung, dass sich der Auskunftsanspruch dann auch auf die Eintragungen im Outlook-Kalender erstreckt.

Das kann großen Aufwand auslösen

Der Aufwand, der dadurch entsteht, ist erheblich. Das Unternehmen muss nämlich den gesamten Outlook-Kalender durchsuchen lassen. Außerdem ist unter Umständen eine Abfrage dazu erforderlich, welche Mitarbeiter Eintragungen daraus übernommen und lokal abgespeichert haben. Dies alles lässt sich vermeiden, wenn der Name des Bewerbers nicht in den Outlook-Kalender aufgenommen wird.

3 VERPFLICHTUNG AUF DAS DATENGEHEIMNIS 2.0

Allgemein vorgeschrieben ist die Verpflichtung auf das Datengeheimnis durch die DSGVO nicht. Das verblüfft viele, denn nach wie vor gehört sie zu den Ritualen bei der Einstellung. Aber was ist, wenn neue Mitarbeitende die Unterschrift unter die Verpflichtungserklärung verweigern?

Die DSGVO regelt nur einen Spezialfall ausdrücklich

Wer das Stichwort „Verpflichtung auf das Datengeheimnis“ in der DSGVO finden will, muss genau hinsehen. Es taucht lediglich an einer Stelle auf. Nur für Beschäftigte von Auftragsverarbeitern sieht die DSGVO eine ausdrückliche Verpflichtung auf die Wahrung des Datengeheimnisses vor (siehe Art. 28 Abs. 3 Nr. 2b DSGVO). Für andere Beschäftigte ist eine solche förmliche Verpflichtung nicht vorgesehen. Das bedeutet keineswegs, dass die DSGVO das Datengeheimnis gering schätzen würde – im Gegenteil.

Diese Regelung soll denkbare Zweifel ausschließen

Für die DSGVO ist es völlig selbstverständlich, dass es so etwas wie ein Datengeheimnis gibt und dass Beschäftigte es generell beachten müssen. So selbstverständlich, dass sie es nur

für den Spezialfall „Beschäftigte von Auftragsverarbeitern“ ausdrücklich hervorhebt. Denn hier könnten sich Zweifel ergeben. Schließlich verarbeiten diese Beschäftigten Daten, die nicht ihrem Arbeitgeber „gehören“, sondern dessen Kunden. Und zu diesen Kunden stehen die Mitarbeiter des Auftragsverarbeiters in keinem eigenen vertraglichen Verhältnis.

Das Datengeheimnis gilt unabhängig davon allgemein

Bei der Verpflichtung auf das Datengeheimnis geht es darum, dass ein Unternehmen seine datenschutzrechtliche „Rechenschaftspflicht“ erfüllen will. Diese Rechenschaftspflicht ist in Art. 5 Abs. 2 DSGVO festgelegt. Sie besagt: Es genügt nicht, dass ein Unternehmen die Vorgaben der DSGVO einhält. Das Unternehmen muss vielmehr jederzeit nachweisen können, dass dies tatsächlich so ist.

„Wer schreibt, der bleibt“

Zur Einhaltung der DSGVO gehört es, dass ein Unternehmen seinen Mitarbeitern verdeutlicht, welche Pflichten sie im Datenschutz haben. Das erfordert Schulung, Information und Belehrung. Dass so etwas stattgefunden hat, muss schriftlich dokumentiert sein. Denn sonst könnte ein Unternehmen vieles behaupten, ohne dass es nachprüfbar wäre.

Die Verpflichtung ist ein Instrument der Dokumentation

Ein bewährtes Instrument der Dokumentation ist die Verpflichtung von Beschäftigten auf das Datengeheimnis. Aus ihr entstehen für die Beschäftigten keine Pflichten, die nicht ohnehin vorhanden wären. Insofern haben sie auch keinen sachlichen Grund, die Unterschrift unter eine solche Verpflichtung zu verweigern.

Beschäftigte sind zur Unterschrift nicht verpflichtet

Andererseits können sie gerade deswegen auch nicht zu einer Unterschrift gezwungen werden. Es gibt dafür schlicht keine Rechtsgrundlage. Niemand muss durch seine Unterschrift die Beachtung von Pflichten bestätigen, wenn eine solche Bestätigung nirgends gesetzlich angeordnet ist. Schließlich käme auch niemand auf die Idee, von Beschäftigten beispielsweise eine schriftliche Bestätigung dafür zu fordern, dass sie niemals etwas am Arbeitsplatz stehlen werden. Das Verbot, Dinge zu stehlen, gilt völlig unabhängig von einer solchen Unterschrift.

Ein Vermerk über die Verweigerung genügt

Damit liegt auf der Hand, wie ein Unternehmen damit umgehen sollte, wenn ein Beschäftigter die Verpflichtung auf das Datengeheimnis nicht unterschreiben will. Es genügt, dass das Unternehmen die Weigerung in seinen Unterlagen vermerkt. Eine kurze Notiz „Unterschrift verweigert“ reicht aus. Zur Sicherheit sollte die Notiz mit einem Datum versehen sein und den Namen oder das Namenskürzel desjenigen enthalten, der die Verpflichtung vornehmen wollte.

Der Vermerk dient der Dokumentation

Damit hat das Unternehmen seine Dokumentationspflicht erfüllt. Und der Beschäftigte kann sich nicht irgendwann darauf herausreden, er habe seine Pflichten nicht gekannt. Ein ausdrücklicher Hinweis an den Beschäftigten, dass die Verweigerung der Unterschrift an seinen Pflichten nicht das Geringste ändert, kann dabei sinnvoll sein.

Der Begriff „Beschäftigte“ ist hier sehr weit zu fassen

Die dauerhaft Beschäftigten bilden in Unternehmen normalerweise die Kerngruppe der Personen, die auf das Datengeheimnis verpflichtet werden. Selbstverständlich müssen jedoch auch befristet Beschäftigte, Azubis, Praktikanten und Leiharbeiter die Vorgaben der DSGVO beachten. Gerade für sie ist das möglicherweise nicht so selbstverständlich wie für die Kernbelegschaft. Sie müssen deshalb unbedingt ebenfalls verpflichtet werden.

4 DIE GROSSE FRAGE: löschen, aufbewahren oder archivieren?

Einerseits sollen bestimmte Geschäftsdokumente noch in vielen Jahren verfügbar sein und müssen „archiviert“ werden. Andererseits kennen Sie vom Datenschutz die Löschpflichten. Was gilt denn nun? Zu frühes Löschen ist ebenso zu vermeiden wie eine zu lange Aufbewahrung.

Lücken im Archiv des Unternehmens

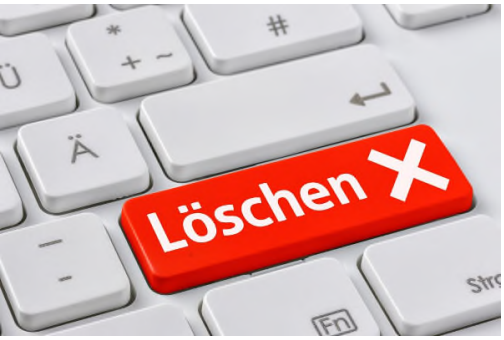
Man stelle sich vor, jemand greift auf das digitale Archiv des Unternehmens zu, um einen Kundenvertrag einzusehen, der vor fünf Jahren abgeschlossen wurde. Doch das Archivsystem meldet, dass es den betreffenden Vertrag nicht finden kann. Wenn das Archivsystem korrekt arbeitet, gibt es offenbar Fehlstellen im Archiv.

Wie kann es dazu kommen?

- Entweder hat niemand daran gedacht, dass es Aufbewahrungsvorgaben für die Kundenverträge gibt. Niemand hat also vor fünf Jahren den digitalen Kundenvertrag in das Archivsystem eingestellt.
- Oder jemand hat den Kundenvertrag gelöscht, vielleicht um dem Datenschutz gerecht zu werden, da es doch nach DSGVO für betroffene Personen (Kunden) ein Recht auf Löschung und somit für das Unternehmen eine Löschpflicht gibt.

Löschung versus Aufbewahrung

So manche Lücke im Unternehmensarchiv kann durch einen missverstandenen Datenschutz entstehen, wenn ein Dokument, das eigentlich noch für Jahre aufbewahrt werden sollte, stattdessen gelöscht wird.



Auch wenn es so scheint – die Löschpflichten und die Pflichten zur Aufbewahrung und Archivierung stehen nicht im Widerspruch zueinander:

- Gelöscht werden müssen personenbezogene Daten zum Beispiel, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind.
- Müssen sie aber noch aufbewahrt werden, weil es Aufbewahrungs- oder Archivierungspflichten gibt, und es bestehen keine anderen Gründe für die Löschung (wie eine unerlaubte Verarbeitung der Daten), dann tritt die Löschpflicht erst ein, wenn die Pflicht zur Aufbewahrung oder Archivierung abgelaufen ist.

Es ist also immer ein Abgleich zwischen gesetzlichen und vertraglichen Aufbewahrungspflichten und dem Datenschutz bzw. zwischen dem Archiv- und dem Datenschutzrecht erforderlich.

Aufbewahren ist nicht identisch mit Archivieren

Das eigentliche Archivrecht betrifft öffentliche Archive, die wie das Gedächtnis öffentlicher Einrichtungen zu sehen sind. Die sogenannte „Verarbeitung für im öffentlichen Interesse liegende Archivzwecke“ gehört zu den Ausnahmen von der Löschverpflichtung nach DSGVO. Sie setzt besondere Prüfungen voraus, was bei einer Löschung, die eine betroffene Person wünscht, passieren soll.

Archiviert ein Unternehmen etwas, dann ist damit eine langfristige Aufbewahrung gemeint, um vertragliche oder gesetzliche Vorgaben zu erfüllen. Dies fällt nicht unter die Ausnahmen von der Löschverpflichtung. Denn in aller Regel besteht kein öffentliches Interesse an einer Archivierung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Archivierung als

„elektronische Langzeitspeicherung“. Aus rechtlicher Sicht ist der Begriff „Archivierung“ in Deutschland durch die Archivgesetze des Bundes und der Länder definiert. „Archivierung“ im rechtlich korrekten Sinn betrifft allein Unterlagen der öffentlichen Verwaltung.

Ein Unternehmen sollte also nicht fälschlicherweise davon ausgehen, dass sich das eigene Archiv von den Löschpflichten aus dem Datenschutz einfach ausnehmen ließe.

Wissen Sie, wann gelöscht und wann aufbewahrt oder archiviert wird?
Machen Sie den Test!

Dokumente im Unternehmensarchiv müssen nicht gelöscht werden. Stimmt das?

1. Nein, Ausnahmen von der Löschpflicht gibt es nur für im öffentlichen Interesse liegende Archivzwecke.
2. Ja, Archive sind von der Löschpflicht im Datenschutz ausgenommen.

Lösung:

Die Antwort 1. ist richtig. Spricht ein Unternehmen von einem digitalen Archiv, dann ist damit die langfristige Aufbewahrung von Daten gemeint, um gesetzlichen und vertraglichen Aufbewahrungspflichten gerecht zu werden, zum Beispiel nach dem Steuerrecht und nach dem Handelsrecht. Öffentliche Archive hingegen unterliegen dem Archivrecht.

Wünscht eine betroffene Person die Löschung, muss immer sofort gelöscht werden. Ist das so?

1. Ja, mit dem Löschwunsch gibt es keine Grundlage mehr, um die Daten aufzubewahren.
2. Nein, die Löschung muss nur dann unverzüglich erfolgen, wenn es keine andere Rechtsgrundlage mehr für die weitere Speicherung gibt.

Lösung:

Die Antwort 2. ist richtig. Liegt zum Beispiel ein gültiger Kundenvertrag vor und sind zugehörige Rechnungen nach gesetzlichen Vorgaben noch aufzubewahren, muss der Löschwunsch erst nach dem Ablauf der Aufbewahrungspflichten erfüllt werden. Es gilt also: Personenbezogene Daten sind gemäß DSGVO auf Verlangen von betroffenen Personen grundsätzlich zu löschen. Müssen die Daten aber noch wegen rechtlicher Verpflichtungen wie dem Steuerrecht oder Handelsrecht aufbewahrt werden, hat dies eine aufschiebende Wirkung bis zum Ablauf der Aufbewahrungspflichten. Erst dann muss gelöscht werden.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de