Newsletter | Datenschutz

DDSB
www.deutsche-datenschutzberatung.de

Datenschutz *Kurier!*

Ihre Mitarbeiterzeitung zum Datenschutz

Liebe Leserin, lieber Leser,

Ausgabe 04/2020

es ist eine Alltagserfahrung: Was man schon lange in dieser oder jener Form macht, hinterfragt man nicht mehr. Damit nimmt man sich aber die Chance, etwas zu optimieren, auch im Datenschutz. Nur weil es im Unternehmen schon seit Jahren eine Geburtstagsliste der Mitarbeiterinnen und Mitarbeiter gibt, bedeutet das nicht, dass aus Sicht des Datenschutzes auch alles in Ordnung damit ist. Ähnliches gilt für die Vorbereitung von Meetings, ein weiteres Thema dieser neuen Ausgabe Ihres Datenschutz-Newsletters.

Geburtstagslisten – aber bitte datenschutzkonform

Gratuliert man freundlich, schaut so manches „Geburtstagskind“ eher süß-sauer als begeistert. Lässt man es bleiben, kann die Verstimmung genauso groß sein. Eine gute Geburtstagsliste hilft weiter. Natürlich muss sie datenschutzkonform sein. Was ist dabei zu beachten?

Personenbezug offensichtlich

Sie liegen in der Schublade des Chefsekretariats oder hängen in der Teeküche innen im Schrank. Manchmal findet man sie auch an einem Schwarzen Brett oder im Intranet. Gemeint sind Listen mit Geburtstagen. Dass es dabei immer um personenbezogene Daten geht, liegt auf der Hand. Damit kommt der Datenschutz ins Spiel. Aber was sind die Spielregeln?

Unmittelbare Vorgesetzte und Geschäftsleitung

Jedenfalls bei einem runden Geburtstag erwarten fast alle Mitarbeiterinnen und Mitarbeiter, dass der unmittelbare Vorgesetzte gratuliert. Alles andere würde als unhöflich empfunden. Vielfach wünscht bei einem solchen besonderen Anlass sogar die Geschäftsleitung (Geschäftsführer, Vorstand) alles Gute.

Erfasste Personen

Unmittelbare Vorgesetzte und Geschäftsleitung brauchen dafür die nötigen Angaben. Was „nötig“ ist, unterscheidet sich bei beiden. Bei der Geschäftsleitung geht es nicht ohne eine Liste aller Mitarbeiterinnen und Mitarbeiter des Unternehmens. Unmittelbare Vorgesetzte benötigen dagegen lediglich eine Liste der Mitarbeiterinnen und Mitarbeiter, die ihnen zugeordnet sind.

Konkreter Inhalt der Liste

Dass solche Listen Vornamen und Nachnamen enthalten müssen, liegt auf der Hand. Der genaue Geburtstag, bestehend aus Tag, Monat und Jahr, gehört selbstverständlich ebenfalls dazu. Aber auch eine Rubrik „Geschlecht“ erscheint jedenfalls bei der Geschäftsleitung gerechtfertigt. Denn sie gratuliert meist schriftlich. Und aus dem Vornamen ergibt sich das Geschlecht oft genug nicht eindeutig.

„Für das Arbeitsverhältnis erforderlich“

Rechtlich gesehen sind Geburtstagslisten für Geschäftsleitung und unmittelbare Vorgesetzte zur Durchführung des Arbeitsverhältnisses erforderlich. Damit ist ein gesetzliches Kriterium erfüllt, das den Umgang mit solchen Listen erlaubt. Auf eine Einwilligung der Mitarbeiterinnen und Mitarbeiter kommt es nicht an.

Fälle notwendiger Einwilligung

Anders sieht es aus, wenn Geburtstagslisten sonstigen Personen zur Verfügung stehen sollen. Das können Kolleginnen und Kollegen sein (etwa im selben Team), aber auch Kunden. Letzteres kommt vor allem in stark vertriebsorientierten Unternehmen vor. In solchen Geburtstagslisten dürfen nur Personen stehen, die darin eingewilligt haben.

Freiwilligkeit der Einwilligung

Natürlich muss eine Einwilligung stets freiwillig erfolgen. Das ist sicher nicht der Fall, wenn man dem neuen Azubi schon am ersten Tag die Angaben zu seinem Geburtstag geradezu abnötigt. Der nur scheinbar freundliche Hinweis „Wir stehen da alle drin, das gehört bei uns dazu!“ macht es nur schlimmer, nicht besser.

Mögliche technische Lösung

Eine technische Lösung könnte so aussehen: Im Intranet steht eine Mini-Datenbank „Geburtstagsliste“. Wer möchte, trägt sich dort mit seinen Geburtstagsdaten ein. Selbst gesetzte „Haken“ erlauben den Zugriff nur für das eigene Team, die Abteilung, alle im Unternehmen oder auch für Lieferanten und Kunden.

Meetings datenschutzkonform organisieren

Wer Meetings organisiert, muss den Datenschutz im Blick haben. Das überrascht viele. Aber manchmal geht es in Meetings um heikle Dinge. Oft spricht man über Personen oder über Dinge, die Personen betreffen. Grund genug, sich einige Gedanken zu machen. Aber auch das „Drumherum“ vor und nach einem Meeting verdient Aufmerksamkeit.

Einladung zum Meeting

Schon bei der Einladung kann einiges schiefgehen. Oft erfolgt die Einladung über eine Rundmail. Sie geht an eine Kontaktgruppe, die im Mail-Adressbuch hinterlegt ist. Der Mail-Verteiler muss dann wirklich noch aktuell sein. Mitarbeiter, die längst an ganz andere Stellen im Unternehmen gewechselt sind, haben darin nichts mehr zu suchen. Nehmen Sie die nächste Einladung per Rundmail also zum Anlass, sich den Verteiler einmal genau anzusehen.

Vorsicht bei „an“, „Cc“ und „Bcc“

Kein Problem ist es beim internen Meeting einer Arbeitsgruppe, wenn alle Adressaten den vollständigen Verteiler sehen können. Er kann dann im Adressfeld „an“ stehen. Denn oft besteht eine wichtige Information gerade darin, wer alles zu dem Meeting eingeladen ist. Das gilt allerdings nicht immer. Denn Meeting und Meeting ist nicht dasselbe. Wenn etwa die Einladung für eine Personalversammlung an die ganze Belegschaft geht, gehört die Adressliste selbstverständlich in das Feld „bcc“. Dann ist sie für die Adressaten nicht offen sichtbar. Überlegen Sie also vorher, ob die Adressaten den ganzen Verteiler der Einladung sehen sollen oder nicht.

Doodle oder nicht?

Doodle ist praktisch und sehr beliebt. Es hat aber eine Schwachstelle: Wer auf eine Terminabfrage zugreifen will, muss einen Link aufrufen, den er bekommen hat. Dieser Link darf nicht in unrechte Hände geraten. Darauf muss man unbedingt achten. Denn Daten über Termine sind keineswegs immer so harmlos, wie viele glauben. Wer wann mit wem spricht und wer wann dafür Zeit hat, kann eine sehr interessante Information sein.

Alternativen zu Doodle gibt es durchaus, und zwar kostenlose. Beispiele dafür sind „dudle“ von der Technischen Universität Dresden und der „DFN-Terminplaner“. Beide sind vor allem im Wissenschaftsbereich weit verbreitet. Es handelt sich allerdings um Software, die man auf dem Rechner installieren muss. Das setzt in Unternehmen normalerweise eine entsprechende Genehmigung der EDV voraus. Bitte beachten Sie die Regelungen, die dafür im Unternehmen bestehen!

Teilnehmerlisten bei internen Meetings

Bei einer internen Besprechung etwa zum Thema „Absatzplanung 2021“ kann jeder Teilnehmer eine Teilnehmerliste erhalten. In sie gehören die Namen und die dienstlichen Kommunikationsdaten der Besprechungsteilnehmer. Nur so können sie später noch einmal zuverlässig miteinander Kontakt aufnehmen, wenn das nötig ist. Der Zweck einer solchen Besprechung erfordert es geradezu, dass alle eine Teilnehmerliste erhalten.

Teilnehmerlisten bei Schulungsveranstaltungen

Ganz anders sieht es etwa bei Schulungsveranstaltungen mit externen Teilnehmern aus. Selbstverständlich ist hier eine interne Liste möglich, auf der jeder Teilnehmer unterschreibt. Sie kann Verwendung finden, um Teilnehmerbestätigungen und Rechnungen für die Schulungsgebühren zu erstellen. Nicht in Ordnung wäre es dagegen, jedem Teilnehmer eine Liste mit allen anderen Teilnehmern auszuhändigen. Das ist normalerweise nicht erforderlich, um das Ziel einer solchen Veranstaltung zu erreichen. Tauschen Teilnehmer ihre Kommunikationsdaten trotzdem untereinander aus, ist es ihre Privatangelegenheit.

Tücken bei Telefonkonferenzen

Telefonkonferenzen gehören inzwischen zum Alltag. Virtuelle Konferenzräume dafür gibt es im Internet kostenlos. Achten Sie aber einmal darauf, was Ihr Lieblingsanbieter zum Thema Datenschutz sagt. Gar nichts? Dann existiert bei ihm Datenschutz wahrscheinlich auch nicht.

Wichtig ist vor allem: Lässt sich der Konferenzraum „abriegeln“, wenn ihn alle Teilnehmer betreten haben? Sonst besteht die Gefahr, dass sich Unbefugte einklinken und mithören. Generell sollte man darauf achten, dass der Konferenzanbieter ein Sicherheitszertifikat einer anerkannten Organisation vorzuweisen hat. Dann dürften zumindest keine groben Schwachstellen vorhanden sein.

Videokonferenz – aber sicher!

Sicherheit kann ein sehr trügerisches Gefühl sein. Wer an einer Videokonferenz teilnimmt, meint subjektiv, dass er buchstäblich „alles überblicken“ kann. Aber was ist, wenn sich ein Unbefugter einklinkt und unbemerkt die ganze Konferenz verfolgt? Hier kommt das Thema „Verschlüsselung“ ins Spiel.

Verschlüsselung ist nicht gleich Verschlüsselung

Manche Anbieter setzen eine „Ende-zu-Ende-Verschlüsselung“ ein. Bei ihr können nur die Teilnehmer der Konferenz selbst die Daten wahrnehmen, sprich die Bilder sehen und die Sprache hören. Sie bietet mehr Sicherheit als eine reine „Transportverschlüsselung“. Bei dieser ist es zumindest technisch möglich, dass „Datentransporteure“, die für die Übermittlung der Daten sorgen, die Daten entschlüsseln. Damit stellt sich die Frage, ob man sich mit weniger zufriedengeben soll, wenn man auch mehr Sicherheit haben kann. Dafür gibt es keine allgemein verbindlichen Vorgaben der Datenschutz-Aufsichtsbehörden. Anlass zum Nachdenken besteht aber allemal.

Videoüberwachung am Arbeitsplatz: Wann ist sie berechtigt?

Niemand wird gern beobachtet. Doch es gibt Gründe für eine Videoüberwachung am Arbeitsplatz. Datenschutz-Aufsichtsbehörden haben nun klargestellt, wann eine Videoüberwachung erlaubt ist.

Konkrete Vorgaben zur Videoüberwachung

Videoüberwachung wird seit vielen Jahren kontrovers diskutiert. Auf der einen Seite stehen staatliche Stellen, aber auch Unternehmen, die gern die Videoüberwachung ausweiten würden. Denn sie sehen darin einen Gewinn für die Sicherheit. Auf der anderen Seite stehen zum Beispiel die Datenschützer, die Videoüberwachung als Eingriff in die Privatsphäre sehen und deshalb so weit wie möglich begrenzen möchten.

Kaum ein Thema gibt so viel Anlass zu Beschwerden und zu Überprüfungen im Datenschutz wie die Videoüberwachung. Dabei stellt sich die Frage, was rechtlich zulässig ist und was nicht. Da die seit Mai 2018 wirksame Datenschutz-Grundverordnung (DSGVO) keine speziellen Regeln zur Videoüberwachung enthält,

müssen die datenschutzrechtlichen Anforderungen an den Einsatz von Videoüberwachung aus den allgemeinen Regelungen des Datenschutzrechts abgeleitet werden. Das ist vor allem eine große Herausforderung für die Unternehmen, die Videoüberwachung rechtskonform einsetzen möchten, wie die Aufsichtsbehörden für den Datenschutz betonen.

Die nationalen Datenschutz-Aufsichtsbehörden im Europäischen Datenschutzausschuss haben nun eine Leitlinie zum datenschutzkonformen Einsatz von Videoüberwachung beschlossen. Die Leitlinie will auf ein möglichst hohes Datenschutzniveau für betroffene Personen hinwirken und gleichzeitig für die Unternehmen klare und handhabbare Vorgaben machen.

Videoüberwachung muss verhältnismäßig sein

Die Leitlinie betont den Grundsatz der Verhältnismäßigkeit, sprich: Für die Videoüberwachung muss es eine fundierte Begründung geben, sie darf keine übertriebene Maßnahme sein. Wenn zum Beispiel ein Arbeitgeber sagt, er habe gute Gründe für die Videoüberwachung, müssen diese auch objektiv vorliegen. Will sich ein Unternehmen zum Beispiel vor Betrugsfällen und Diebstahl besser schützen und deshalb die Videoüberwachung vornehmen, so müssen konkrete Anhaltspunkte für die Befürchtungen bestehen. Betrug oder Beschädigungen müssen tatsächlich eine konkrete Gefahr darstellen. Mitarbeitende dürfen also nicht grundlos unter Generalverdacht gestellt und mittels Videoaufzeichnung überwacht werden.

Wann Videoüberwachung erlaubt ist und wann nicht

Die Leitlinie zur Videoüberwachung nennt eine Vielzahl von Beispielen, die illustrieren können, wann eine Videoüberwachung übertrieben ist und wann man von einem legitimen Einsatz ausgehen kann.

Ein Ladenbesitzer möchte einen neuen Laden eröffnen und ein Videoüberwachungssystem installieren, um Vandalismus zu verhindern. Durch die Vorlage von Statistiken kann er zeigen, dass in der direkten Nachbarschaft ein hohes Risiko für Vandalismus besteht. Auch Erfahrungen aus Nachbargeschäften sind hilfreich. Es ist nicht erforderlich, dass ein Schaden an dem neuen Geschäft selbst aufgetreten ist, solange Schäden in der Nachbarschaft auf eine Gefahr hindeuten und somit ein Hinweis auf ein berechtigtes Interesse sein können. Es reicht aber nicht aus, eine nationale oder allgemeine Kriminalitätsstatistik vorzulegen, ohne das betreffende Gebiet oder die Gefahren für dieses spezielle Geschäft zu analysieren.

Ein privates Parkhaus hat wiederkehrende Probleme mit Diebstählen in den geparkten Autos dokumentiert. Der Parkplatz ist ein offener Bereich und lässt sich von jedermann leicht erreichen, ist jedoch deutlich mit Schildern und Straßensperren gekennzeichnet, die den Bereich umgeben. Das Parkhaus hat ein berechtigtes Interesse (Verhinderung von Diebstählen in den Autos der Kunden), den Bereich während der Tageszeit zu überwachen, in der Probleme auftreten.

Ein Restaurant beschließt, Videokameras in den Toiletten zu installieren, um die Sauberkeit der sanitären Einrichtungen zu kontrollieren. In diesem Fall haben die Rechte der betroffenen Personen eindeutig Vorrang vor dem Interesse des Unternehmens. Daher darf das Restaurant dort keine Kameras installieren.

Ein Arbeitgeber darf, um Streikende zu identifizieren, keine Aufzeichnungen aus der Videoüberwachung verwenden, die eine Demonstration zeigen.

Ein Unternehmen hat Schwierigkeiten mit seiner Zutrittskontrolle, es kommt wiederholt zu unerlaubtem Betreten. Das Unternehmen setzt Videoüberwachung ein, um diejenigen zu erwischen, die rechtswidrig eintreten. Ein Besucher widerspricht der Verarbeitung seiner Daten durch das Videoüberwachungssystem. Das Unternehmen kann den Widerspruch jedoch in diesem Fall mit der Erklärung ablehnen, dass das gespeicherte Filmmaterial aufgrund einer laufenden internen Untersuchung benötigt wird. Es hat daher zwingende berechtigte Gründe, die Verarbeitung der personenbezogenen Daten fortzusetzen.

Es kommt also immer darauf an, dass es ein wirklich berechtigtes Interesse an der Videoüberwachung gibt und dass kein unnötiger Eingriff in die Privatsphäre der Betroffenen stattfindet.

Was es mit Anonymisierung auf sich hat

Anonyme Daten lassen keinen Rückschluss auf eine konkrete Person mehr zu. Für Datenschützer ist Anonymisierung deshalb ein Königsweg zum Datenschutz. Doch viele Unternehmen glauben, Anonymisierung mache Daten wertlos. Das stimmt aber nicht.

Die Frage des Personenbezugs

Unter anonymen Daten versteht man Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass sich die betroffene Person nicht oder nicht mehr identifizieren lässt, so die Datenschutz-Grundverordnung (DSGVO).

Der Bundesdatenschutzbeauftragte erläutert anonyme Daten etwas greifbarer: Eine Anonymisierung von Daten liegt vor, wenn der Personenbezug von Daten derart aufgehoben ist, dass er sich nicht oder nur unter unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskräften wiederherstellen lässt.

Anonymisierung hat weitreichende Folgen: Die Grundsätze des Datenschutzes gelten nur für Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Datenschutz-Grundverordnung betrifft somit nicht die Verarbeitung anonymer Daten.

Muss es personenbezogen sein?

Wer also mit anonymen Daten arbeitet, hat dem Datenschutz Genüge getan, so scheint es. Das sollte für Unternehmen verlockend klingen, die oftmals den Aufwand für Datenschutzmaßnahmen beklagen. Doch Anonymisierung ist bei vielen Unternehmen nicht beliebt, denn sie fürchten, ohne Personenbezug hätten die Daten keinen Wert mehr.

Der Bundesdatenschutzbeauftragte zum Beispiel sieht dies anders: Für viele Forschungsprojekte und Geschäftsmodelle ist es ausreichend, anonyme Datensätze zu analysieren, deren abstrakter Gehalt erhalten bleibt, der Personenbezug jedoch aufgehoben wird. Anonyme Daten haben also durchaus einen Wert für Datenanalysen und entsprechende Geschäftsmodelle.

Anonymisieren oder nicht

Die Menge der verfügbaren personenbezogenen Daten steigt exponentiell an. Ihre Aussagekraft über das Verhalten der Menschen nimmt zu. Die Analyse von Datenbeständen und die Auswertung der daraus resultierenden Erkenntnisse werden zu einem immer wichtigeren Bestandteil der modernen Wirtschaft, Wissenschaft und Forschung. Fragt sich ein Unternehmen nun, ob es denn zur Anonymisierung greifen sollte oder nicht, sollte es zuerst überlegen, ob die Verarbeitung der personenbezogenen Daten ohne die Anonymisierung überhaupt erlaubt ist.

Wie der Bundesdatenschutzbeauftragte erklärt, gebietet der Grundsatz der Datenminimierung oftmals, die personenbezogenen Daten nur in anonymisierter Form zu verarbeiten. Unter Datenminimierung versteht man, dass die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Anders gesagt: Werden die Daten für einen bestimmten Zweck nicht zwingend benötigt, soll man auf diese verzichten. Dieser Verzicht wird dann durch die Anonymisierung möglich. Die Anonymisierung kann sogar die Voraussetzung für eine Datenverarbeitung sein, wenn die Verarbeitung bei bestehendem Personenbezug datenschutzrechtlich unzulässig wäre.

Es stellt sich also mitunter gar nicht die Frage, ob man Anonymisierung durchführen sollte oder nicht, sondern es geht in bestimmten Fällen gar nicht anders: nämlich dann, wenn Unternehmen die Daten mit Personenbezug mangels rechtlicher Grundlage gar nicht verarbeiten dürfen. Bei der Auswertung großer Datenmengen, also sogenannten Big-Data-Analysen, sollen vielfach Daten zu anderen Zwecken verarbeitet werden als zu den Zwecken, für die sie erhoben wurden. Das ist in vielen Fällen aber nur möglich, wenn die Daten zuvor anonymisiert worden sind. Anonymisierung ist dann keine Kür, sondern die Voraussetzung.

Kennen Sie die Bedeutung von Anonymisierung? Machen Sie den Test!

Frage: Anonymisierung macht Daten wertlos. Stimmt das?

1. Nein, viele Analysen brauchen den Personenbezug gar nicht.
2. Ja, durch Anonymisierung werden Daten beliebig, sie verlieren ihren Bezug.

Lösung: Die Antwort 1 ist richtig. Wenn man zum Beispiel wissen will, ob ein Produkt bei Männern über 50 Jahren ankommt, muss man nicht wissen, wie diese Personen heißen. Es gibt andere Bezugspunkte für Daten als den Personenbezug. Es reichen Angaben, die sich nicht auf konkrete Personen beziehen.

Frage: Anonymisierung kann man machen, aber man muss es nicht. Stimmt das?

1. Es gibt keine Pflicht zur Anonymisierung.
2. In bestimmten Fällen kann man Daten nicht verarbeiten, wenn keine Anonymisierung stattgefunden hat.

Lösung: Die Antworten 1 und 2 sind richtig. Eine generelle Pflicht zur Anonymisierung gibt es nicht. Man kann personenbezogene Daten auch anders schützen. Doch es gibt Fälle, in denen nur anonyme Daten verarbeitet werden dürfen, die Anonymisierung also zur Pflicht wird. Das ist dann der Fall, wenn es keine Rechtsgrundlage zur Verarbeitung der personenbezogenen Daten gibt, man also zum Beispiel keine Erlaubnis hat, die Daten zu seinen Zwecken zu analysieren.

Betrugsversuche mit Hilfsanträgen

Unternehmen müssen auch in Zeiten von Corona mit Cyberkriminellen rechnen. Das Landeskriminalamt Baden-Württemberg warnt vor Betrugsversuchen im Zusammenhang mit den aktuellen Soforthilfemaßnahmen.

Foto: Talaj - stoc.adobe.com

Im Internet sind Seiten aufgetaucht, auf denen wegen der Corona-Krise in Bedrängnis geratene Unternehmen aufgefordert werden, ein Formular mit Daten zu befüllen und anschließend hochzuladen. Teilweise wurden Unternehmen gezielt telefonisch kontaktiert und explizit auf die entsprechende Seite im Internet hingewiesen. Der Anrufer gab sich dabei als Angehöriger der einzig offiziellen Stelle zur Abwicklung der Soforthilfe aus. Die Polizei stuft diese Vorgehensweise als Vorbereitungshandlung für spätere Straftaten ein und warnt eindringlich davor, persönliche und Unternehmensdaten auf solchen Fake-Seiten im Internet preiszugeben.

In diesem Zusammenhang wichtig: Den Antrag auf die Corona-Soforthilfe des Landes gibt es nur beim Wirtschaftsministerium. Die Daten werden dann auf der Webseite der IHKs und Handwerkskammern hochgeladen.

Impressum

Redaktion:

Andreas Peter Mückl (V.i.S.d.P.)
Sachverständiger Datenschutz u. Datensicherheit
ID No. 0000040772: Data protection Auditor (TÜV)

Anschrift:

DDSB GmbH
Untere Dornäcker 21, 72379 Hechingen
Telefon: 07471 5010-100 | E-Mail: hello@ddsb.de