DATENSCHUTZAKTUELL
NOV II 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH



AI GENERATED

KEIN HEXENWERK: SO ERSTELLEN SIE IHREN TÄTIGKEITSBERICHT

AWARENESS
Neue Phishing-Tricks: Sorgen Sie jetzt für Awareness 1–2

KNOW-HOW
Prost Mahlzeit: Fördern Sie den Datenschutz in der Kantine 3



Von nichts kommt nichts

Liebe Leserin, lieber Leser,

das Sprichwort bringt etwas auf den Punkt, was auch im Datenschutz eine wichtige Rolle spielt: Setzt man sich nicht für eine Sache ein bzw. strengt man sich nicht an, kann aus der Sache nichts werden und der Erfolg bleibt aus.

So ist es auch, wenn es darum geht, dass etwa Ihre Unternehmensleitung Datenschutz ernst nehmen muss. Außerdem muss man Sie als Datenschutzbeauftragten mit den nötigen Mitteln ausstatten, damit Sie Ihrem Beratungs- und Kontrollauftrag nachkommen können. Spart man hier, erweist man dem Unternehmen und dem Datenschutz einen Bärendienst. Kommt es zu Pannen, wird es meist viel teurer.

Viele Grüße



Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz im Unternehmen pragmatisch umsetzen lässt.

Inhalt

Awareness
Neue Phishing-Tricks: Sorgen Sie jetzt für Awareness
Seiten 1–2

Know-how
Prost Mahlzeit: Fördern Sie den Datenschutz in der Kantine
Seite 3

Datenschutzbeauftragter
Kein Hexenwerk: So erstellen Sie Ihren Tätigkeitsbericht
Seiten 4–5

Know-how
Mit diesen 5 Tipps beraten Sie auch bei spontanen Fragen
Seite 6

Fragen an die Redaktion
Können wir Unterlagen zu Corona vernichten?
Seite 7

Was müssen wir bei der unzulässigen Videoüberwachung unternehmen?
Seite 7

Recht & Richtlinie
Das Vorliegen einer Einwilligung muss nachweisbar sein
Seite 8

Zu Ihrem Onlinebereich:
https://www.privacyxperts.de

Live-Talk:
https://t1p.de/live-talk

E-Mail-Beratung:
https://t1p.de/andreas-wuertz

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Michael Schrader, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | AI generated; Seite 1: Adobe Stock | Abdul

Erscheinungsweise: 36-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau



Selbst die beste Technik bietet keinen vollkommenen Schutz vor Cyberkriminellen.

Neue Phishing-Tricks: Sorgen Sie jetzt für Awareness

Die Unterwelt schläft nicht. Gerade Cyberkriminelle entwickeln immer wieder neue Maschen, um Menschen ein X für ein U vorzumachen und sie zu meist schwerwiegenden Fehlentscheidungen zu verleiten. Und leider ist es auch so, dass selbst beste Technik nicht davor schützt, dass Cyberkriminelle doch Erfolg haben. Sie nutzen nämlich die Schwachstelle Mensch. Genau hier müssen Sie ansetzen.

Lieber zu viel und zu oft als ein „Jetzt haben wir den Salat"

Wenn es um Cyberkriminelle und ihre Aktivitäten geht, sollte es nie dazu kommen, dass man in eine unangenehme oder gar gefährliche Situation gerät. Um den „Salat" in Sachen Cybercrime zu umgehen, ist vor allem eines wichtig: Alle Beschäftigten auf allen Ebenen brauchen das nötige Know-how, um eine entsprechende Angriffssituation zu erkennen. Zudem müssen sie wissen, wie sie sich dann richtig verhalten. Und hier ist keine Awareness-Aktivität zu viel.

Gerade neue Maschen müssen Sie vermitteln

Aktuell setzen Cyberkriminelle auf Links und URLs, die nur auf den ersten Blick echt und wie das Original aussehen. Dazu nutzen sie andere Zeichensätze, gerne Buchstaben aus lateinischen oder kyrillischen Buchstabensets, die den eigentlichen Buchstaben sehr ähneln. Da wird schnell aus einem A ein Å, wobei nicht jedem gleich ins Auge springt, dass hier etwas nicht stimmt.

§

Beruhigen Sie „genervte" Empfänger

Wenn Sie eine Awareness-Info per E-Mail verschicken, kann es passieren, dass Sie den einen oder anderen Empfänger haben, der Sie wegen der „ständigen" Informationen anmeckert. Das kann auch von ganz oben kommen. Reagieren Sie hier professionell. Äußern Sie, dass es gut sei, dass er bereits über so viel Wissen verfüge und dieses entsprechend anwenden könne. Allerdings lässt sich das nicht bei allen Beschäftigten voraussetzen. Außerdem ist eine Information per E-Mail das Mittel der Wahl, um möglichst viele Beschäftigte zu erreichen. Gerade bei kritischen Themen wie Phishing ist jeder Beschäftigte mit erhöhter Aufmerksamkeit ein Gewinn für das Unternehmen. Klar ist nämlich: Die „Human Firewall" im Unternehmen sollte möglichst keine Lücken aufweisen.

Entwickeln Sie Ihre Information mit diesem Muster

Über neue Tricks und Maschen können Sie im Handumdrehen informieren. Setzen Sie auf folgendes Muster und passen Sie dieses an die Bedürfnisse Ihres Unternehmens an. Um den Mehrwert Ihrer Informationskampagne zu steigern, sollten Sie Folgendes beherzigen:

- **Erhöhen Sie den Unternehmens- und Praxisbezug**
  Jedes Unternehmen funktioniert anders. Berücksichtigen Sie die Besonderheiten in Ihrem Unternehmen. Ergänzen Sie Ansprechpartner oder Prozesse für den Fall der Fälle.
- **Schneiden Sie die Information auf Zielgruppen zu**
  Sie können auch bei den Inhalten oder bei der Ansprache variieren. Bei Azubis kann ein Du Nähe und Vertrauen aufbauen.
- **Ergänzen Sie die Information durch eine informative Sprechstunde**
  Die müssen Sie nicht allein stemmen. Viele wertvolle Infos kann ein Kollege der IT-Abteilung liefern.

Muster: Information „Neue Tricks von Cyberkriminellen“

Betreff: Vorsicht, diese Tricks von Cyberkriminellen sollten Sie kennen!

Liebe Kollegin,
lieber Kollege,

im hektischen Arbeitsalltag müssen wir alle viele Entscheidungen treffen, manchmal auch ziemlich schnell. Handlungsdruck kann gerade dann entstehen, wenn Vorgesetzte oder die Unternehmensleitung ein dringendes Anliegen haben. Doch auch wenn der Kalender oder das E-Mail-Postfach voll sind, nimmt man manches vielleicht nicht so genau unter die Lupe. Und das ist genau das, worauf es Cyberkriminelle abgesehen haben. Wenn es schnell gehen muss, werden Warnhinweise übersehen.

Auch Cyberkriminelle gehen mit der Zeit

Zwar gibt es sie noch: schlecht gemachte Phishing-E-Mails, denen der Warnhinweis „Nicht öffnen“ geradezu auf die Stirn geschrieben steht. Doch die Zeit schlecht gemachter Phishing-E-Mails ist eigentlich vorbei. Cyberkriminelle nutzen KI, Schreib- und Übersetzungstools, um E-Mails perfekt erscheinen zu lassen. Nicht anders sieht es aus, wenn es um das optische Erscheinungsbild oder falsche den echten Webseiten täuschend echt nachempfundene „Fake-Seiten“ geht.

Wichtig ist also, dass Sie auch mit Ihrem Wissen mit der Zeit gehen. Manche der folgenden Vorgehensweisen von Cyberkriminellen sind neu. Andere werden durch neue technische Möglichkeiten und KI noch überzeugender. Schauen Sie also genau hin, etwa bei den folgenden Vorgehensweisen:

Die Falle: Fast derselbe Buchstabe, aber die vollkommen falsche Adresse

Echt	Falsch
A	Å
C	Ċ
e	ė
I	İ
s	ș
Y	Y

Cyberkriminelle machen sich bei Webseiten und Links zunutze, dass es eine Vielzahl an Zeichensätzen gibt, etwa spezifische Zeichen für bestimmte Sprachen. So werden Buchstaben ausgetauscht, die ähnlich aussehen, aber an sich komplett unterschiedliche Zeichen sind. Das Ziel: Sie übersehen den Austausch der Buchstaben, weil der Link oder die Webseitenadresse bekannt und vertraut wirkt. Allerdings landen Sie bei einem Klick auf den Link auf einer Fake-Seite. Auf der sollen Sie Sensibles preisgeben, etwa Anmeldedaten.

So schützen Sie sich und unser Unternehmen: Schauen Sie nie nur auf den angezeigten Text zu einem Link oder zu einer Webseite. Bei einem Link bewegen Sie den Mauszeiger auf den Link, ohne auf diesen zu klicken. Schauen Sie dann genau hin, worauf der Link verweist. Ist Ihnen die Anzeige zu klein, können Sie bei Windows die Bildschirmlupe nutzen. Alternativ machen Sie einen Screenshot und vergrößern dann das Bildschirmfoto mit dem Linkverweis.

Die Falle: (Falsche) Videonachrichten vom (falschen) Chef oder Kollegen

Künstliche Intelligenz macht’s möglich. Auch der Cheftrick, der sogenannte CEO-Fraud, wird perfekter. Denn: Auch unser Management gibt Interviews, die etwa bei Videoplattformen veröffentlicht sind. Daneben finden sich Statements in Businessnetzwerken wie LinkedIn. Solch echtes Material ist Grundlage für Cyberkriminelle, um täuschend echt wirkende Video- oder Audioklone zu erstellen. Sind die Fälschungen gut gemacht, sind sie kaum von echtem Material zu unterscheiden. Solche Video- oder Audiofälschungen werden dann etwa in Video- oder Audiochats für Anrufe, für Nachrichten für Anrufbeantworter oder in Messengern genutzt, um Sie in die Falle zu locken. Sie sollen Ihren Augen und Ohren trauen und das Falsche als echt akzeptieren. Ihr Pflichtbewusstsein und Ihre Hilfsbereitschaft werden brutal ausgenutzt. Und Sie sollen natürlich das machen, was die Cyberkriminellen der Fälschung in den Mund gelegt haben. Oft sollen Sie Sensibles preisgeben, Daten und Dokumente an jemanden verschicken oder eine Zahlung veranlassen.

So schützen Sie sich und unser Unternehmen: Weil Videos und Stimmen täuschen können, müssen Sie besonders auf die Situation, die Umstände und den Inhalt, sprich das Geforderte, achten. Fragen Sie sich immer: Kann das sein? Wird vom üblichen Vorgehen oder von bestehenden Prozessen oder Vorgaben abgewichen? Warum sollen ausgerechnet Sie die richtige Anlaufstelle für das Geforderte sein, gerade wenn es über Ihnen Kollegen gibt, die von Rang oder Aufgabe eher die richtigen Adressaten sein müssten? Passt hier etwas nicht, sollten Sie nie das Geforderte umsetzen. Fragen Sie bei Vorgesetzten oder Kollegen nach und holen Sie deren Einschätzung ein. Fragen Sie auch beim richtigen Absender nach, und zwar über die im Adressbuch hinterlegten Kontaktinformationen. Eine andere Kontaktaufnahme, etwa die in einem Chat angegebenen Möglichkeiten, sind tabu. Immer!

Die Falle: Falsche Sicherheitsabfragen

Häufig sind Sie hier schon halb in die Falle getappt. Sie haben einen Link zu einer Fake-Seite geklickt oder sind auf andere Weise auf eine solche Seite geraten. Dort finden Sie ein Pop-up vor, das etwa verifizieren will, ob Sie ein Mensch sind, und Sie sollen anschließend sensible Daten angeben oder einen angezeigten Code in die Eingabeaufforderung des Computers (z. B. Windows-Eingabeaufforderung CMD) kopieren. Machen Sie das, nimmt das Unheil seinen Lauf. Schließlich öffnen Sie Cyberkriminellen oder Schadsoftware Tür und Tor.

So schützen Sie sich und unser Unternehmen: Brechen Sie solche Anforderungen ab. Schließen Sie die Seite und geben Sie Aufforderungen nicht nach, auch wenn sie angeblich von einem Sicherheitsteam stammen. Sprechen Sie vor jeder Aktivität mit den Kollegen unseres Cybersecurity-Teams.

Bitte bedenken Sie immer:

Erst zweimal denken und dann überlegt handeln: Lassen Sie sich nie unter Druck setzen. Nehmen Sie sich die Zeit, um alles Relevante zu durchdenken.

Vier Augen und Ohren sehen und hören mehr: Klären Sie mit Kollegen und Vorgesetzten die Frage: Kann das wirklich sein?

Im Zweifel nachfragen: Fragen Sie nie durch Rückantwort beim angeblichen Absender nach. Starten Sie die Kontaktaufnahme über die hinterlegten Möglichkeiten aus unserem internen Adressbuch.

Wenn es passiert ist: unbedingt melden! Niemand macht Ihnen einen Vorwurf. Melden Sie sofort, auch wenn Sie nur den Verdacht haben, Cyberkriminellen auf den Leim gegangen zu sein. Ihr Kontakt: cyberteam@muster-firma.xyz oder über die Cyberhotline unter der -1234.

Herzlichen Dank für Ihre Unterstützung und Ihren Beitrag zur Sicherheit unseres Unternehmens.

Ihr Datenschutzbeauftragter

Tim Buktu

Prost Mahlzeit: Fördern Sie den Datenschutz in der Kantine

Auch wenn es um den Datenschutz an sich gut bestellt ist, staunt mancher Datenschutzbeauftragter, dass es doch noch den einen oder anderen weißen Fleck auf der Datenschutzlandkarte gibt. So ist es vielleicht auch bei Ihnen, wenn Ihr Unternehmen über eine Kantine oder eine Cafeteria verfügt. Machen Sie sich also daran, die mögliche Lücke auf der Karte zu schließen.

Machen Sie den gemeinsamen Check

Unter Umständen stoßen Sie bei der Leitung der Kantine oder der Cafeteria zunächst auf Unverständnis. Schließlich meint man, dass man doch mit Daten nicht viel am Hut haben dürfte. Beharren Sie dennoch zumindest auf einem ersten Gespräch. Schnell dürfte sich zeigen, dass personenbezogene Daten doch eine Rolle spielen. Wichtige Themen finden Sie in der folgenden Checkliste.

Checkliste: Wichtige Datenschutzthemen in der Kantine

Aspekt	Hintergrund	Besprochen?
Welche Verarbeitungen gibt es überhaupt?	› Lassen Sie die Kollegen erzählen, wo mit Daten gearbeitet wird. Dabei ist wichtig, dass Sie zunächst keine Einordnung machen, ob es sich um personenbezogene Daten handelt. › Erklären Sie, was personenbezogene Daten sind, und betrachten Sie bei Bedarf erneut die genannten Verarbeitungen.	○ Ja ○ Nein
Sind alle Verarbeitungstätigkeiten dokumentiert?	› Idealerweise haben Sie einen Auszug der relevanten und von den Kollegen verantworteten Verarbeitungstätigkeiten dabei. Prüfen Sie, inwieweit die Angaben vollständig und aktuell sind. › Passt etwas nicht, sollten Sie freundlich um eine zeitnahe Ergänzung oder Aktualisierung bitten.	○ Ja ○ Nein
Welche internen Regelungen gibt es?	› Das können Datenschutzregeln sein, etwa zum Umgang mit Daten von Besuchern oder Lieferanten. › Daneben sollten Sie auch prüfen, inwieweit es Betriebsvereinbarungen gibt. Häufig werden hier umfassende Regelungen getroffen, etwa zu Bezahlmethoden, Auswertungen und Analysen. Gerade Einschränkungen sind auch für die datenschutzrechtliche Zulässigkeit von Bedeutung.	○ Ja ○ Nein
Inwieweit werden bei jeder Verarbeitung die Grundsätze der Verarbeitung umgesetzt?	› Die Grundsätze aus Art. 5 Abs. 1 Datenschutz-Grundverordnung (DSGVO) gelten für alle Verarbeitungen personenbezogener Daten, auch wenn sie eher unbedeutend erscheinen. › Legen Sie den Fokus auf Rechtmäßigkeit, Zweck(bindung), Speicherbegrenzung und Transparenz.	○ Ja ○ Nein
Wie steht es um den Datenschutz beim Bezahlsystem?	› Kassen- und Zahlungssysteme haben es oft in sich und können auch Beschäftigte zum gläsernen Kunden machen. Doch das passt meist nicht zum Minimalprinzip. › Prüfen Sie konkret die Erforderlichkeit für den verfolgten Zweck im Zusammenhang mit der Rechtsgrundlage. Unter Umständen wird auch manches verarbeitet, was für den verfolgten Zweck (z. B. Abbuchung) nicht erforderlich ist. › Verkaufsanalysen gehen in de Regel anonym und ohne Personenbezug.	○ Ja ○ Nein
Inwieweit werden besondere Kategorien personenbezogener Daten verarbeitet?	› Es ist unter Juristen umstritten, inwieweit eine Unverträglichkeitsinformation schon als Gesundheitsdatum im Sinne von Art. 9 Abs. 1 DSGVO gilt. Raten Sie hier dazu, lieber auf Nummer sicher zu gehen und das entsprechend anzunehmen. › Für besondere Kategorien gilt ein grundsätzliches Verarbeitungsverbot. Meist geht es nur mit der Einwilligung des Betroffenen. Achten Sie hier nicht nur auf Art. 6 Abs. 1 Satz 1 Buchst. a, Art. 7, Art. 4 Nr. 11 DSGVO. Auch § 26 Abs. 2 Bundesdatenschutzgesetz ist relevant.	○ Ja ○ Nein
Welche Auswertungen und Analysen finden statt?	› Auch hier spielen Erforderlichkeit und Minimalprinzip eine wichtige Rolle. Schauen Sie sich die Auswertungen und die Berechtigungen an. › Hier lohnt zudem der Blick in Betriebsvereinbarungen. Die können Beschränkungen vorsehen.	○ Ja ○ Nein
Welche Dienstleister werden eingesetzt?	› Lassen Sie sich einen Überblick geben und bewerten Sie die Rollen der Beteiligten. › Prüfen Sie gemeinsam, inwieweit Vereinbarungen erforderlich und geschlossen sind.	○ Ja ○ Nein
Wie steht es um technische und organisatorische Schutzmaßnahmen?	› Art. 32 DSGVO ist auch in der Kantine oder Cafeteria eine wichtige Vorschrift. Risikoangemessene Schutzmaßnahmen sind zwingend. › Haben Sie auch ein Auge auf das Organisatorische. Wichtig sind beispielsweise auch Schulungen, bei denen wichtige Basics vermittelt werden.	○ Ja ○ Nein
Welche Schutzmaßnahmen sind vor Ort ergriffen?	› Prüfen Sie vor Ort, wie es um Clean Desk und Clear Screen etwa im Büro der Kantinenleitung steht. › Nehmen Sie in diesem Zusammenhang auch die Entsorgungsmöglichkeiten unter die Lupe. Schließlich fällt oft viel Papier mit Personenbezogenem an, etwa auch Unterlagen von Lieferanten oder Dienstpläne.	○ Ja ○ Nein
Inwieweit kommt Videoüberwachung zum Einsatz?	› Jede Videoüberwachung muss datenschutzrechtlich vertretbar sein. Maßstab ist hier die DSGVO. › Halten Sie Ausschau nach überwachten Tabubereichen, etwa dem Speisebereich für Gäste, Pausen- und Aufenthaltsräumen für das Personal, Sanitärbereichen und Umkleiden. Hier ist eine Überwachung regelmäßig nicht zulässig.	○ Ja ○ Nein

Kein Hexenwerk: So erstellen Sie Ihren Tätigkeitsbericht

Wie steht es eigentlich um Ihren Tätigkeitsbericht als Datenschutzbeauftragter? Wenn Sie hier nur mit einem „Gute Frage!“ antworten können, weil noch wenig bis gar nichts passiert ist, dann sollten Sie sich sputen. Schließlich ist es bis zum Jahresende nicht mehr lange hin.

Bereiten Sie jetzt schon Ihren Bericht vor

Vielleicht meinen Sie, dass Sie einen Bericht doch mal schnell an einem Nachmittag erstellen und im Januar der Unternehmensleitung präsentieren können. Das sollten Sie lieber bleiben lassen. Denn Flickwerk oder ein schlampiger Bericht schaden Ihrem Ansehen und Ihrem Thema. Starten Sie früh in die Vorbereitung. Das stresst Sie nicht nur weniger. Sie haben auch das professionellere und ausgereifte Ergebnis rechtzeitig erstellt.

Darum ist ein Tätigkeitsbericht sinnvoll

Datenschutzbeauftragte in Unternehmen brauchen zwar an sich keinen Tätigkeitsbericht erstellen. Eine entsprechende Anforderung kennt die Datenschutz-Grundverordnung (DSGVO) nicht. Und dennoch sollten Sie die Vorteile eines Berichts nicht unterschätzen, sodass sich die Arbeit immer lohnt:

- Sie geben einen Statusbericht ab und können aufzeigen, wie es um den Datenschutz in Ihrem Unternehmen steht. Das hilft der Leitung, Risiken einzuschätzen und ggf. gegenzusteuern.
- Besteht Handlungsbedarf, können Sie diesen konzentriert ganz oben im Unternehmen adressieren. Das kann Ihnen vor allem dann helfen, wenn Sie weiter unten auf taube Ohren stoßen oder man es mit dem Datenschutz beharrlich nicht so genau nehmen will.
- Ein Tätigkeitsbericht ist Ihr Aushängeschild schlechthin. Schließlich können Sie zeigen, was Sie machen, wie professionell Sie agieren und wie wichtig Sie als Datenschutzbeauftragter für Ihr Unternehmen sind. Sie können sich also auch als Profi empfehlen, wenn die deutsche Benennungspflicht für Datenschutzbeauftragte wieder auf die Anforderungen der DSGVO reduziert werden sollte.

So gehen Sie bei Ihrem Bericht vor

Planvoll vorgehen ist nicht so schwer und aufwendig. Setzen Sie auf folgende Schritte:

1. Klären Sie den Rahmen und Schwerpunkte: Legen Sie Form, Umfang und Zielgruppe genauso fest wie die Schwerpunktthemen, sprich die Kapitel, Ihres Berichts. Eine Auswahl möglicher Schwerpunktthemen finden Sie in der Checkliste.
2. Sichten Sie Material und Quellen: Durchforsten Sie insbesondere Ihr E-Mail-Postfach, den Kalender, Protokolle und Audits nach Berichtenswertem.
3. Legen Sie sich einen Themenspeicher an: Sammeln Sie Relevantes in einer Liste. Gute Alternative: Nutzen Sie Post-its an der Wand oder Tafel. Das fördert die Übersichtlichkeit und das leichtere Verschieben von Einzelthemen.
4. Führen Sie ein Brainstorming durch: Notieren Sie Einfälle zu spezifischen Fragen wie „Was ist Besonderes im Datenschutz passiert?“, „Wo sind die größten Herausforderungen?“, „Wo besteht Optimierungsbedarf?“.
5. Treffen Sie eine Auswahl: Sie können nicht alles im Bericht unterbringen. Stellen Sie zusammen, was wichtig, relevant und von Interesse für die Unternehmensleitung ist.
6. Formulieren Sie Ihren Bericht: Machen Sie sich eine Gliederung mit Stichpunkten und gehen Sie dann ans Formulieren.
7. Optimieren Sie Ihr Werk: Der erste Wurf ist oft nicht der beste. Schauen Sie sich Ihr Werk mit etwas zeitlichem Abstand an. Oft findet man so etwas, was verbessert werden sollte.

§

Setzen Sie auf diese 5 Tipps beim Schreiben

Kurz und bündig: Ausufernde Berichte liest niemand. Beschränken Sie sich auf maximal zehn bis 15 Seiten oder Präsentationsfolien. Packen Sie Übersichten, Listen oder weitergehende Informationen in eine Anlage.

Ein Satz – ein Gedanke: Ihr Bericht muss schnell lesbar und leicht zu erfassen sein. Arbeiten Sie mit Hauptsätzen. Vermeiden Sie zu lange oder zu viele (Neben-)Sätze.

Zahlen, Daten, Fakten: Setzen Sie auf Belegbares. Können Sie etwas konkret nachweisen, sollten Sie Zahlen, Ergebnisse oder andere Belege aufnehmen. „Gefühlte“ Fakten können schnell nach hinten losgehen, wenn sie keine belastbare Grundlage haben.

Keine Textwüsten: Achten Sie auf eine gute Lesbarkeit. Grafiken, Bilder oder wichtige Botschaften bzw. Zitate können das Layout auflockern. Auch Zwischenüberschriften oder Auflistungen sind hilfreich. Passt ein Text nicht auf eine Seite, reduzieren Sie den Text und nicht die Schriftgröße.

Fehler vermeiden: Wer schreibt, dem können Fehler passieren, etwa bei Rechtschreibung, Grammatik oder Logik. Und unter Umständen erkennt man die Fehler selbst nicht mehr. Lassen Sie daher Ihren Bericht gegenlesen. Setzen Sie auf KI bei der Erstellung, müssen Sie auch selbst auf die Fehlersuche gehen.

Wählen Sie die passenden Themenschwerpunkte aus

Es gibt keine zwingende Struktur für Ihren Bericht. Daher: Wählen Sie aus der folgenden Checkliste die Schwerpunkte aus, die für Ihr Unternehmen und Sie besonders relevant sind.

Checkliste: Mögliche Themenschwerpunkte für Ihren Tätigkeitsbericht

Schwerpunkt	Das ist wichtig	Aufnehmen?
Management Summary	› Geben Sie auf maximal einer Seite einen Überblick über das Wichtigste, was Sie vermitteln wollen. › Beschränken Sie sich auf zwei bis fünf Sätze pro wichtigem Aspekt. › Arbeiten Sie ggf. mit einem Ampelsystem. Das spart Text und jeder weiß dennoch, was mit den Farben gemeint ist. › Heben Sie auch Handlungs- und Entscheidungsbedarf hervor.	○ Ja ○ Nein
Situation des Datenschutzbeauftragten	› Beschreiben Sie kurz Ihre Rolle und Funktion. Machen Sie deutlich, dass Sie unabhängiger Berater und Kontrolleur sind und das Unternehmen bei der Wahrnehmung seiner Verantwortung unterstützen. › Geben Sie einen Überblick über Ihre Kapazitäten, insbesondere zeitliche und finanzielle Ressourcen. › Gibt es zukünftig einen höheren Unterstützungsbedarf, sollten Sie den hier klar adressieren.	○ Ja ○ Nein
Entwicklung wichtiger Rahmenbedingungen	› Unter Umständen gab es rechtliche Veränderungen, die besonders für Ihr Unternehmen von Bedeutung sind und auch Auswirkungen auf den Datenschutz haben können. So z, B. die Umsetzung der NIS-2-Richtlinie der EU durch das deutsche BSI-Gesetz. › Denken Sie aber auch an einschlägige Rechtsprechung oder Äußerungen von Datenschutzaufsichtsbehörden, die für Ihr Unternehmen oder dessen Geschäftstätigkeit von großer Relevanz sind.	○ Ja ○ Nein
Situation des Datenschutzes im Unternehmen	› Schätzen Sie ein, wie es um den Datenschutz bestellt ist. › Benennen Sie größere Baustellen, bei denen ggf. mehr Unterstützung der Unternehmensleitung erforderlich ist. › Gab es wichtige Änderungen im Unternehmen, etwa Umstrukturierungen oder eine neue Geschäftsführung, können Sie die damit einhergehenden Herausforderungen darstellen.	○ Ja ○ Nein
Tätigkeitsschwerpunkte im Berichtszeitraum	› Listen Sie auf, wo Sie Ihre Schwerpunkte gesetzt haben. Das kann auch ein Überblick dazu sein, wie Sie die zur Verfügung stehende Zeit aufgewendet haben. › Arbeiten Sie mit Diagrammen. Das macht die Anteile der Schwerpunkte anschaulich und lockert Ihren Bericht auf. › Erwähnen Sie auch, wenn Sie Schwerpunkte neu setzen mussten, sodass Sie Ihre ursprüngliche Planung nicht umsetzen können. Ggf. werden dadurch auch manche Themen in der Priorität weiter nach hinten rutschen.	○ Ja ○ Nein
Projekte und Beratungen	› Hier können Sie meist gut mit Zahlen arbeiten. Zeigen Sie auf, wie viele Projekte Sie betreut haben, welche abgeschlossen wurden oder wo Ihr Rat noch gefragt ist. › Gab es Verarbeitungen mit hohen Risiken, dürfte eine Datenschutz-Folgenabschätzung nötig gewesen sein. Stellen Sie dar, wie Sie hier unterstützt haben und wie man Ihre Beratung beim weiteren Vorgehen berücksichtigt hat. › Hier ist auch Raum für Positives. Geben Sie einen Überblick, bei welchen Vorhaben man Sie frühzeitig eingebunden hat bzw. wo die Zusammenarbeit besonders gut funktioniert hat.	○ Ja ○ Nein
Anfragen zum Datenschutz	› Stellen Sie dar, welche Anfragen mit Datenschutzrelevanz es gab. Das sind etwa Anfragen von Betroffenen, die ihre Rechte geltend machen. › Eventuell gab es auch Nachfragen von Partnern, Auftraggebern oder Aufsichtsbehörden. Lassen Sie diese nicht unerwähnt, weil sie meist auch viel Arbeit bei Ihnen verursacht haben dürften.	○ Ja ○ Nein
Datenschutzvorfälle und -pannen	› Listen Sie auf, in welchen Bereichen was schiefging, welche Folgen das hatte und welche Konsequenzen daraus gezogen wurden. Insbesondere können Sie den abgeleiteten Handlungsbedarf sowie den Stand der Umsetzungsmaßnahmen darstellen. › Musste eine Meldung an die Datenschutzaufsicht bzw. eine Information von Betroffenen erfolgen, sollten Sie hierüber informieren. › Erläutern Sie, welche Schlussfolgerungen Sie aus den Vorfällen und Pannen ziehen. Besteht Handlungsbedarf bei der Leitung, müssen Sie diesen benennen.	○ Ja ○ Nein
Audits und Kontrollen	› Geben Sie einen Überblick über die Prüfungsschwerpunkte im Berichtszeitraum. Setzen Sie zudem auf Zahlen, etwa die Anzahl der durchgeführten Prüfungen sowie die Zahl der Prüfungen ohne, mit mittleren oder gravierenden Mängeln. › Listen Sie auf, welche Defizite besonders auffällig waren, etwa aufgrund ihrer Schwere oder ihrer Häufigkeit. › Auch abgeleitete Maßnahmen sowie den Stand ihrer Umsetzung können Sie berichten.	○ Ja ○ Nein
Awareness und Schulungen	› Stellen Sie dar, welche Aktivitäten es Ihrerseits gab und wie viele Beschäftigte Sie erreicht haben. Vergessen Sie hier nicht auch kleine Aktivitäten, etwa Awareness-E-Mails oder Vor-Ort-Besuche in Abteilungen. › Zeigen Sie auf, welche Lücken durch Ihre Schulungen geschlossen und welchen Risiken damit reduziert wurden. › Erwähnen Sie auch, wo es noch Nachholbedarf gibt bzw. was Sie zukünftig in den Fokus rücken möchten.	○ Ja ○ Nein
Besondere Risiken	› Haben Sie im Rahmen Ihrer Tätigkeit neue oder besondere Risiken festgestellt, sollten Sie diese ansprechen. › Nehmen Sie eine Bewertung nach dem Schema „Schadenspotenzial x Eintrittswahrscheinlichkeit vor". › Empfehlen Sie Maßnahmen und deren zügige Umsetzung.	○ Ja ○ Nein
Handlungsbedarf und Empfehlungen	› Machen Sie deutlich, was aus Ihrer Sicht jetzt ansteht. Gibt es etwas von der Unternehmensleitung zu entscheiden, sollten Sie das hier adressieren. › Sind Anpassungen bei Ihren Ressourcen nötig, sollten Sie das hier nochmals erwähnen, damit der Handlungsdruck verdeutlicht wird. › Geben Sie eventuell auch einen Ausblick, welche Schwerpunkte Sie in 2027 setzen wollen, um das Thema Datenschutz vorwärtszubringen.	○ Ja ○ Nein
Fazit	› Erwähnen Sie zum Schluss auch Positives, etwa was Sie bei Ihrer Arbeit besonders beeindruckt hat, z. B. Engagement von Mitarbeitern im Datenschutz. › Liegt im Datenschutz noch vieles im Argen, können Sie dennoch ggf. eine positive Tendenz ausmachen. Natürlich brauchen Sie nichts beschönigen. › Bedanken Sie sich für die Unterstützung und gute Zusammenarbeit. Trifft das auf die Unternehmensleitung nicht zu, nennen Sie positive Beispiele aus dem Unternehmen.	○ Ja ○ Nein

Mit diesen 5 Tipps beraten Sie auch bei spontanen Fragen

Auch alte Hasen im Datenschutz wissen: Viel Datenschutz-Know-how zu haben und es richtig anzuwenden ist eine Sache. Eine andere ist, alles Notwendige so zu vermitteln, dass es ankommt und auch umgesetzt wird. Zudem kann entscheidend sein, dass Sie professionell auftreten, gerade auch dann, wenn man Sie spontan auf ein Thema anspricht.

Lassen Sie sich nicht hetzen

Auch wenn es schnell gehen soll oder Sie eine spontane Einschätzung geben müssen, sollten Sie stets versuchen, etwas Zeit zum Nachdenken zu gewinnen. Schließlich gilt: Hastiges Nachdenken kann zu Fehleinschätzungen führen. Nehmen Sie sich also etwas Zeit, kommen Sie mit dem Kollegen ins Gespräch und behalten Sie die Situation im Griff. Beherzigen Sie zudem die folgenden Tipps. Die geben Ihnen Sicherheit und helfen Ihnen dabei, ganz Profi in der Beratung zum Datenschutz zu sein.

Tipp Nr. 1: Klären Sie, worum es überhaupt geht

Oft gibt es zunächst nur spärliche Informationen, vielleicht einige Sätze zum Anliegen oder Vorhaben. Bitten Sie den Kollegen, in die Details zu gehen. Manchmal ist sogar ein Start bei Adam und Eva erforderlich. Denn nur wenn Sie wissen, worum es ansatzweise geht, können Sie sich erste grobe Vorstellungen zur Problemlage und zu möglichen Knackpunkten im Datenschutz machen.

Um etwas Zeit zum Nachdenken zu gewinnen, können Sie auch aktiv nachfragen. Schon die Frage „Wer hat mit welchen personenbezogenen Daten was genau und in welcher Weise vor?" sorgt bei Ihrem Gesprächspartner für einiges an Beschäftigung. Zudem zwingen Sie ihn dazu, Ihnen viele wichtige Informationen zu liefern, die für Ihre Einschätzung von großer Bedeutung sind.

Übrigens: Wird es zu komplex oder ist die Sache undurchsichtig, versuchen Sie, einen Gesprächstermin zu vereinbaren. Im Vorfeld können Sie einige allgemeine Fragen stellen, die man für den Termin vorbereiten kann.

Tipp Nr. 2: Verfolgen Sie den risikobasierten Ansatz

Bestimmt trifft das auch bei Ihnen zu: Sie haben nur begrenzte Ressourcen. Insofern ist Risikoorientierung ein Muss, auch bei Ihrer Beratung. Nicht alle an Sie gerichteten Fragen sind gleich wichtig und dringend. Manches Problem ist nicht so bedeutsam, dass die Lösung nicht noch etwas warten könnte. Das müssen Sie so natürlich niemandem sagen und für Verärgerung sorgen. Machen Sie in einem solchen Fall deutlich, dass es aktuell vorrangige Beratungen gibt. Sie kommen aber gerne auf den Kollegen und sein Anliegen zurück. Bieten Sie beispielsweise direkt eine Termineinladung für ein Gespräch an.

Tipp Nr. 3: Lassen Sie sich nicht festnageln

Gerade bei Einschätzungen zwischen Tür und Angel sollten Sie stets der besonderen Situation Rechnung tragen: Sie sind von der Anfrage und ggf. auch vom Thema überrascht. Vielleicht versucht man auch, Sie unter Druck zu setzen und zu einer schnellen Einschätzung zu bewegen. Machen Sie dann unbedingt klar: Sie geben eine erste Einschätzung ab. Bei genauerer Betrachtung der Sache kann Ihre Einschätzung auch anders ausfallen. Umso wichtiger ist, dass Sie Ihre Einschätzung unter den Vorbehalt einer genaueren und eingehenderen Prüfung stellen. Dazu ist meist jedoch noch erforderlich, dass Sie über alle relevanten Informationen verfügen. Die müssen nicht Sie sich beschaffen. Die muss man Ihnen zur Verfügung stellen.

Haben Sie Sorge, dass man Ihr Statement doch als finale Aussage auffassen könnte, ist unerlässlich: Schicken Sie dem Kollegen schnellstmöglich eine E-Mail, in der Sie nochmals deutlich machen, dass Sie nur eine erste Einschätzung gegeben haben. Diese unterliegt dem Vorbehalt einer genaueren Prüfung.

Tipp Nr. 4: Geben Sie Ihre Einschätzung schriftlich

Stellt sich ein Sachverhalt komplex dar oder bedarf Ihre Einschätzung einer eingehenden Prüfung der Rechtslage, sollten Sie eine mündliche Einschätzung im Nachgang zum Gespräch verschriftlichen. Teilen Sie Ihrem Gesprächspartner mit, was Sie verstanden haben und auf welcher Informationsbasis Sie Ihre Einschätzung vorgenommen haben. Geben Sie diese schriftlich wieder, damit es später keine Diskussionen dazu gibt, was Sie gesagt oder was Sie wie eingeschätzt haben.

Dabei ist wichtig: Warten Sie nicht zu lange mit Ihrer schriftlichen Stellungnahme. Sonst vergisst man oft schnell wichtige Aspekte oder die Erinnerung spielt Ihnen einen Streich. Das kann auch Ihrem Gesprächspartner so gehen. Können Sie sich nicht direkt an die Stellungnahme machen, sollten Sie sich zumindest wichtige Punkte des Gesprächs für später notieren.

Tipp Nr. 5: Stellen Sie klar – Sie sind Berater, nicht Entscheider

Wird man als Datenschutzbeauftragter zwischen Tür und Angel „überfallen", sind das nicht selten Fälle, in denen anscheinend alles nur von Ihnen und Ihrer „Entscheidung" abhängt. So sollen Sie etwas „genehmigen" oder „freigeben". Passiert das nicht, muss dieses oder jenes gestoppt werden. Räumen Sie mit solch falschen Vorstellungen schnell auf. Machen Sie immer klar: Ihr gesetzlicher Auftrag ist im Wesentlichen auf das Beraten in Datenschutzfragen und auf das Kontrollieren der Umsetzung beschränkt. Sie geben Hinweise und machen Vorschläge zur Einhaltung der einschlägigen Regelungen. Die Entscheidung über eine konkrete Umsetzung liegt beim Unternehmen bzw. dessen Führung.

Können wir Unterlagen zu Corona vernichten?

FRAGE: Die Personalabteilung hat sich bei mir gemeldet. Sie hätte gerne meine Einschätzung als Datenschutzbeauftragter zu Unterlagen, die im Zusammenhang mit der Coronapandemie erstellt wurden. Ich habe mir die Unterlagen angeschaut. Teilweise handelt es sich um Impfzertifikate von Mitarbeitern, die aus meiner Sicht keine Relevanz mehr haben. Können wir diese vernichten?

ANTWORT: Solche Unterlagen waren zwar während der Coronapandemie erforderlich, um etwa den Impfstatus nachzuweisen und vor Ort im Unternehmen arbeiten zu können. Die diesbezügliche Verarbeitung ließ sich auf die speziellen gesetzlichen Regelungen stützen, und zwar in Verbindung mit Art. 6 Abs. 1 Satz 1 Buchst. c Datenschutz-Grundverordnung (DSGVO). Unter Umständen ließ sich eine Verarbeitung auch auf § 26 Abs. 3 Bundesdatenschutzgesetz oder das überwiegende berechtigte Interesse des Unternehmens stützen, sprich auf Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO.

Klären Sie die Erforderlichkeit

Unabhängig von der Rechtsgrundlage stellte sich immer die Frage der Erforderlichkeit. Nur wenn eine Verarbeitung bestimmter Informationen für einen konkreten Zweck erforderlich war, kann sie auch zulässig sein. Das ist auch heute nicht anders: Bezüglich der von Ihnen vorgefundenen Daten sollten Sie den Kollegen immer die Frage stellen: Ist die Verarbeitung der Informationen noch erforderlich?

Meist wird man das verneinen. Die entsprechenden speziellen Regelungen im Infektionsschutzgesetz gibt es nicht mehr. Auch sind inzwischen die im Zusammenhang mit Corona geschaffenen besonderen gesetzlichen Vorgaben nicht mehr in Kraft. Fehlt es an einer Rechtsgrundlage bzw. an der Erforderlichkeit einer Verarbeitung, ist die Folge klar. Aus Art. 17 Abs. 1 Buchst. a DSGVO ergibt sich, dass personenbezogene Daten zu löschen sind, wenn sie für die bei der Erhebung festgelegten Zwecke nicht mehr notwendig sind.

Sie müssen das Ganze nicht entscheiden

Geht es um Fragen rund um Aufbewahrungs- oder Löschpflichten, wendet man sich gerne an den Datenschutzbeauftragten. Doch Sie sind mit Ihrer Prüfung meist schnell durch. Dreh- und Angelpunkt sind personenbezogene Daten und Art. 17 DSGVO. Aus dieser Vorschrift ergibt sich, wann zu löschen ist bzw. wann eben nicht. Letzteres kann der Fall sein, wenn es eine Aufbewahrungspflicht gibt. Und die ergibt sich meist aus einer gesetzlichen Vorschrift. Die müsste eigentlich den Kollegen bekannt sein, denn meist wird hierauf die Verarbeitung gestützt. Eventuell kann in diesem Zusammenhang ein Blick in das Verzeichnis von Verarbeitungstätigkeiten weiterhelfen. Ansonsten sollten Sie die Kollegen bitten, sich auf die Suche zu machen.

Unzulässige Videoüberwachung: Was müssen wir tun?

FRAGE: Ich habe kürzlich die Videoüberwachung in unserem Bürogebäude überprüft. In den Fluren sind Kameras, die bei einem Einbruch Beweismittel liefern sollen. In der Betriebsvereinbarung steht, dass diese Kameras nur außerhalb der Geschäftszeiten in Betrieb sind. Tatsächlich fand die Aufzeichnung rund um die Uhr statt. Ich habe empfohlen, rechtmäßige Zustände herzustellen. Das wurde auch umgesetzt. Müssen wir nun noch die Aufsichtsbehörde, den Betriebsrat oder die Beschäftigten informieren?

ANTWORT: Es ist schon mal eine gute Sache, dass Sie auf die unzulässige Verarbeitung hingewiesen haben und die Verarbeitung entsprechend angepasst und das problematische Bildmaterial gelöscht wurde. Schließlich ist es unter Umständen zu einer unzulässigen Dauerüberwachung von Beschäftigten gekommen.

Damit ist jedoch schon alles Wesentliche erledigt. Zu einer Datenpanne, sprich Verletzung der Sicherheit der verarbeiteten Daten, ist es nicht gekommen. Insofern bestehen keine Melde- und Informationspflichten nach Art. 33 (Meldung an Aufsichtsbehörde) und 34 Datenschutz-Grundverordnung (Benachrichtigung von Betroffenen). Im Hinblick auf den Betriebsrat kann es die Pflicht zur vertrauensvollen Zusammenarbeit jedoch gebieten, dass man den ggf. versehentlichen Verstoß gegen die Betriebsvereinbarung anspricht. Hier kann dann auch gemeinsam entschieden werden, ob man zwecks Transparenz die Beschäftigten informiert.

Das Vorliegen einer Einwilligung muss nachweisbar sein

Als Profi ist Ihnen bestimmt geläufig: Will Ihr Unternehmen einen E-Mail-Newsletter verschicken, bedarf es grundsätzlich der vorherigen ausdrücklichen Einwilligung des Inhabers der E-Mail-Adresse. Oft kommt hier das Double-Opt-in-Verfahren (DOI-Verfahren) zum Einsatz. Und dennoch muss hier einiges bedacht werden, wie ein Urteil des Verwaltungsgerichts (VG) Düsseldorf vom 27.7.2026 (Az. 29 K 9714/24) zeigt.

Das war passiert

Ein Mann meldete sich bei der Datenschutzaufsichtsbehörde in Nordrhein-Westfalen. Er beschwerte sich, dass er am 12.4.2020 unerwünschte Werbe-E-Mails eines Unternehmens auf seine private E-Mail-Adresse erhalten habe. Seine E-Mail-Adresse hätte er hierfür nie bereitgestellt. Die Aufsichtsbehörde, die spätere Beklagte, nahm Kontakt zum werbenden Unternehmen, dem späteren Kläger, auf. Die Behörde stellte Fragen zum konkreten Fall.

Der Anwalt des Klägers beantwortete die Fragen der Aufsichtsbehörde. Der Mann hätte die Webseite am 29.6.2019 besucht und seine E-Mail-Adresse für den Erhalt von Werbe-E-Mails angegeben. Zudem hätte er die Einverständniserklärung angeklickt. Die Bestätigungs-E-Mail könne man aber nicht vorlegen, weil man diese aus Datenschutzgründen nicht speichere.

Aufsichtsbehörde fordert DOI-Verfahren

Im Juni 2022 hörte die Aufsicht den Kläger zum beabsichtigten Erlass einer Anweisung an. Die Behörde wollte den Kläger verpflichten, ein DOI-Verfahren einzusetzen, das Verfahren schriftlich zu beschreiben und der Aufsicht vorzulegen. Der Anwalt des Klägers antwortete hierzu, dass man bereits ein solches DOI-Verfahren implementiert hätte, und legte eine Prozessbeschreibung vor. Ende Oktober 2022 machte die Behörde deutlich, dass ein wirksames DOI-Verfahren eine vollständige Dokumentation der Einwilligung, deren Speicherung und eine Möglichkeit zum Ausdrucken umfasse.

Mann erhält erneut Werbung

Mitte Februar 2024 passierte dann Folgendes: Der Mann, der sich schon einmal bei der Aufsicht wegen E-Mail-Werbung beschwerte, erhielt erneut Werbung vom Kläger. Also wandte er sich mit einer neuen Beschwerde an die Aufsichtsbehörde. Er hätte nie die Webseite des Klägers besucht und auch keine Einwilligung erteilt. Die Aufsichtsbehörde forderte den Kläger zur erneuten Stellungnahme und Beantwortung von Fragen auf. Der Kläger teilte der Behörde mit, dass eine Einwilligung des Mannes vorliege.

Behörde spricht Verwarnung aus

Nach den Antworten des Klägers entschloss sich die Aufsicht zu einer Verwarnung. Aus ihrer Sicht konnte der Kläger keine Einwilligung als Grundlage für die Verarbeitung personenbezogener Daten nachweisen. Das werbende Unternehmen wollte das nicht akzeptieren und klagte vor dem VG Düsseldorf gegen den Bescheid.

So entschied das VG

Der Bescheid ist rechtmäßig ergangen. Es bestehen weder formelle Bedenken, noch fehlt es an der materiellen Rechtmäßigkeit. Der Kläger ist nicht in seinen Rechten verletzt.

Die Voraussetzungen für eine Verwarnung sind gegeben. Der Kläger konnte nicht die Einwilligung des Beschwerdeführers in die Verarbeitung seiner personenbezogenen Daten nachweisen. Art. 7 Abs. 1 Datenschutz-Grundverordnung (DSGVO) macht zur Vorgabe, dass ein Verantwortlicher erteilte Einwilligungen nachweisen können muss. Ein solcher Nachweis wurde aber nicht erbracht. Insbesondere wurde kein Ausdruck einer Bestätigungs-E-Mail vorgelegt, welcher das Absenden dieser E-Mail aus dem E-Mail-Konto des Beschwerdeführers belegt.

In diesem Zusammenhang reicht es nicht aus, wenn E-Mail-Adresse, IP-Adresse und Zeitstempel festgehalten werden. Diese Informationen eignen sich nicht als Nachweis. Gerade eine IP-Adresse ist nicht einem bestimmten Nutzer zugeordnet. Vielmehr handelt es sich nur um die Adresse eines Geräts, über das sich ein Anschlussinhaber ermitteln lässt. Das muss nicht der Nutzer sein. Auch lassen Datenpakete keine Einwilligung erkennen..

Kein Nachweis, keine Einwilligung

Eine Einwilligung gilt als nicht bzw. nicht wirksam erteilt, wenn ein Verantwortlicher diese nicht nachweisen kann. Es kommt zu den gleichen Rechtsfolgen wie bei einer tatsächlich fehlenden Einwilligung. Es fehlt an der Rechtmäßigkeit der Verarbeitung. Die Beweislast liegt beim Verantwortlichen, sodass dieser sich nicht auf entgegenstehende Umstände beim Betroffenen berufen kann.

Verwarnung war verhältnismäßig

Die Verwarnung ist als Rechtsfolge nicht zu beanstanden. Die Aufsichtsbehörde hat ihr Ermessen fehlerfrei ausgeübt und die mildeste Abhilfemaßnahme nach Art. 58 Abs. 2 DSGVO gewählt.

§

Diesen Schluss können Sie ziehen

Setzt auch Ihr Unternehmen auf das DOI-Verfahren, um Einwilligungen in Werbe-E-Mails zu dokumentieren, muss eine Einwilligung tatsächlich nachweis- und im Zweifel ausdruckbar sein. Das Dokumentieren von E-Mail-Adresse, IP-Adresse und Zeitstempel einer Anmeldung reicht nicht aus.

Die digitale Lösung für Ihre Pflichtschulungen

Arbeitssicherheit & Datenschutz

Schützen Sie Ihr Unternehmen vor Datenskandalen, hohen Strafzahlungen und Arbeitsunfällen, indem Sie geprüfte Schulungsunterlagen für Präsenz-, Online- oder E-Learning-Einheiten nutzen, den Lernfortschritt über kompakte Dashboards auf Mitarbeiter- oder Gruppenebene überwachen und Schulungen standortübergreifend zentral verwalten.



Testen Sie skillsforwork kostenlos



Compliance & ESG

Mit jährlich aktualisierbaren, individuell anpassbaren E-Learnings zu Compliance-, ESG- & KI-Compliance-Themen sensibilisieren Sie Ihre Mitarbeitenden wirksam durch alltagsnahe, interaktive Lerninhalte und sichern zugleich eine lückenlose Dokumentation des Lernfortschritts.

Cyber Security

Wirksame Awareness-Schulungen und individuell anpassbaren Phishing-Simulationen sensibilisieren Ihre Mitarbeitenden nachhaltig, während monatliche Reports Ihnen jederzeit einen klaren Überblick über das Sicherheitslevel Ihres Unternehmens geben.

skillsforwork

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn

Vorschau:

Last-Minute-Maßnahmen im Datenschutz

Unternehmensumzug: Achten Sie auf diese Punkte