DATENSCHUTZAKTUELL Professional
JAN I 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

WIE HOCH IST DAS BUSSGELDRISIKO? SO FINDEN SIE EINE ANTWORT

Viel Erfolg in 2026!

Liebe Leserin, lieber Leser,

in nicht mal zwei Wochen ist es so weit: Das neue Jahr 2026 ist da. Und klar ist schon jetzt: Auch 2026 wird der Datenschutz Ihr Unternehmen und Sie auf Trab halten. Denn: Es wird sich so einiges im Datenschutz tun. Da wäre etwa die angedachte „Vereinfachung" der Datenschutz-Grundverordnung. Ob es für Ihr Unternehmen und Sie wirklich einfacher wird? Das muss sich zeigen.

Das heißt zugleich für Sie: Langeweile wird 2026 nicht aufkommen. Vielmehr werden Sie manche Herausforderung meistern müssen. Doch keine Sorge. „Datenschutz aktuell" lässt Sie nicht allein. Ich wünsche Ihnen viel Erfolg und alles Gute für das neue Jahr.

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 pragmatisch umsetzen lässt.

Inhalt

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
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, Bonn

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

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

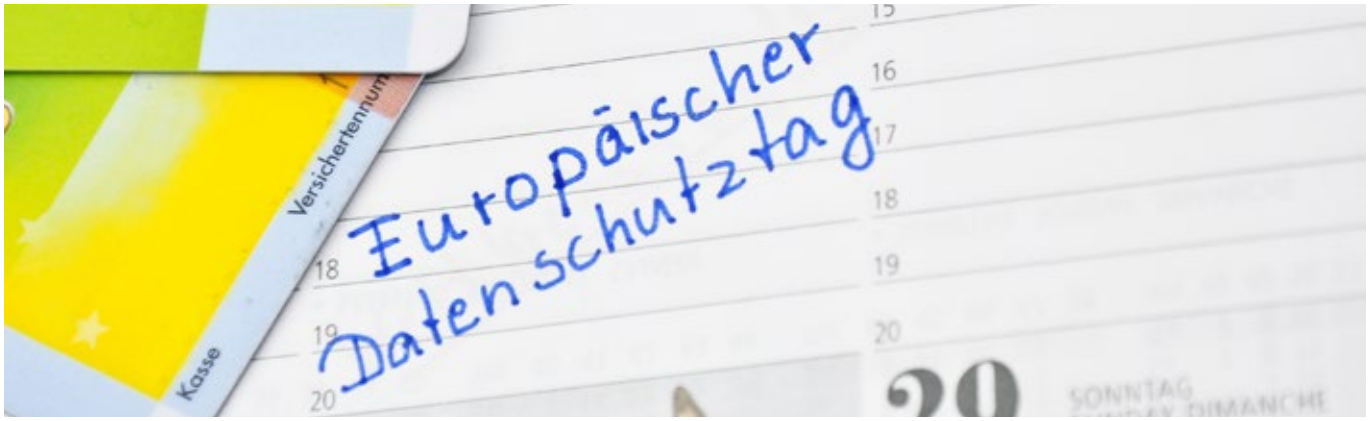
Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: AdobeStock_peterschreiber.media; S. 1: AdobeStock_ Marco2811

Erscheinungsweise: 26-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.



Nutzen Sie diesen Jahrestag, um für den Datenschutz zu sensibilisieren.

Der 28.1.2026 ist ein guter Tag für Awareness

Als Datenschutzprofi wissen Sie nur zu gut: Datenschutz ist kein Selbstläufer. Umso wichtiger ist, dass Sie immer wieder den Datenschutz thematisieren und ins Gespräch bringen. Willkommener Anlass für eine Information können Jahrestage sein, beispielsweise der Europäische Datenschutztag.

Nutzen Sie den Jahrestag

Bis zum 28.1.2026 ist es noch ein Weilchen hin. Also haben Sie genug Zeit, um sich Gedanken zu machen, was Sie an diesem Tag in Sachen Awareness in Ihrem Unternehmen machen können. Denken Sie an Folgendes:

- **Kurze Awarenessveranstaltungen**
  Peilen Sie hier kurze Termine zur Wissensvermittlung an. Informieren Sie vor Ort oder virtuell in 20 Minuten zu wichtigen Themen. Das kann das Erkennen von und das richtige Verhalten bei Phishing sein. Sie könnten auch Tipps zum Datenschutz am Arbeitsplatz geben. Oder Sie geben Führungskräften fünf wichtige Praxistipps mit auf den Weg. Eventuell können Sie sich auch Unterstützung von anderen Profis holen, etwa aus der IT-Abteilung. Dann haben Sie mit den Veranstaltungen weniger Aufwand.
- **Anonyme Sprechstunde**
  Nicht jeder traut sich, Ihnen Fragen zum Datenschutz zu stellen. Machen Sie es also auch denen leicht, die anonym bleiben wollen. Diese können Fragen per Hauspost einreichen oder in Ihr Postfach legen. Die Antworten geben Sie dann in der Sprechstunde.
- **Artikel im Intranet**
  Stellen Sie einige Tipps zusammen, die aus Ihrer Sicht wichtig sind. Zudem können Sie eine Liste mit interessanten bzw. wichtigen Links bereitstellen. Schauen Sie dazu, was die Aufsichtsbehörden im Zusammenhang mit dem Europäischen Datenschutztag anbieten. Wichtige Ratschläge finden Sie aber auch beim Bundesamt für Sicherheit in der Informationstechnik, etwa die „Tipps für den digitalen Alltag".
- **Videobotschaft**
  Warum Datenschutz wichtig ist, können Sie als Datenschutzbeauftragter am besten erklären. Achten Sie hier darauf, dass Sie kurzweilig einige wichtige Aspekte ansprechen. Manche Idee können Sie auch aus dem abgedruckten Muster entnehmen und leicht adaptieren. Weitere Idee: Eventuell hat eine Botschaft mehr Wirkung, wenn Sie von wichtigen Personen im Unternehmen kommt. Vielleicht können Sie die Unternehmensleitung für ein kurzes Statement gewinnen. Noch mehr Eindruck machen Sie, wenn Sie viele mit einem Satz sagen lassen, warum Datenschutz für sie wichtig ist.
- **Datenschutzfrühstück**
  Sie kennen die Weisheit, dass man mit Speck Mäuse fängt. Das können Sie auch für Ihre Sache zunutze machen. Organisieren Sie einige Häppchen, belegte Brötchen oder Brezeln und Getränke. Das lockt so manchen an, auch wenn Datenschutz nicht gerade zu seinen Lieblingsthemen zählt.
- **E-Mail an die Mitarbeiter**
  Auch mit einer E-Mail können Sie geschickt das Thema Datenschutz promoten. Hier ist wichtig, dass Sie Praxisnähe beweisen und einige leicht umsetzbare Tipps geben. Dann wird auch mitgemacht.

Awareness auf die Schnelle: So geht's!

Haben Sie nicht viel Zeit, um etwas zu organisieren? Dann sollten Sie sich dennoch den Europäischen Datenschutztag nicht als guten Aufhänger entgehen lassen. Schicken Sie doch eine E-Mail mit einigen Praxistipps an die Beschäftigten. Dabei ist wichtig: Bleiben Sie nah an der Zielgruppe. Orientieren Sie sich an diesem Muster:

Muster: E-Mail zum Europäischen Datenschutztag 2026

Heute ist Feiertag!

Liebe Kolleginnen und Kollegen,

heute ist der 28.1.2026. Und Sie fragen sich vielleicht: „Das soll ein Feiertag sein?" So ist es! Es ist Europäischer Datenschutztag. Eins ist sicher: Das ist kein Tag für trockene Paragrafen und erhobene Zeigefinger. Ganz im Gegenteil. An diesem Tag geht es darum, sich zu vergegenwärtigen, dass Datenschutz nicht nur eine Pflicht ist. Gelebter Datenschutz schützt nämlich viel mehr als Daten. Er sichert auch Reputation, Umsatz und Arbeitsplätze. Lassen Sie uns den Datenschutz zudem als eine Chance sehen, die Welt für unsere Kunden und für uns ein bisschen besser zu machen.

Warum gibt es diesen Jahrestag?

Seit 2007 wird jedes Jahr am 28.1. der Europäische Datenschutztag begangen. Er erinnert an die Unterzeichnung der Konvention 108 des Europarats am 28.1.1981 – den ersten europäischen Mindeststandard zum Schutz personenbezogener Daten. Und das ist ein Meilenstein im Hinblick auf den Schutz persönlicher Daten und der Privatsphäre, weil hier vieles seinen Anfang nahm.

Warum sollten Sie heute aktiv mitmachen?

Klar ist: Datenschutz ist ein Gemeinschaftswerk. Er funktioniert nur, wenn alle mitmachen. Auch Sie! Denn gerade in der heutigen Zeit ist klar: Jeder Einzelne von uns ist ein wichtiger Schutzwall gegen Cyberkriminelle, Datenlecks, Imageschäden und hohe Bußgelder.

Doch damit nicht genug: Wenn wir immer wieder beweisen, dass wir mit Kundendaten verantwortungsvoll umgehen, schaffen wir die Basis für Vertrauen und langfristige Zusammenarbeit. Kunden bleiben Kunden und empfehlen uns weiter – und das sichert unser aller Arbeitsplätze.

Schon mit Kleinem können Sie Großes bewirken

Beim Datenschutz kommt es nicht immer nur auf das Anspruchsvolle, Komplizierte und Herausfordernde an. Auch mit kleinen Aktivitäten oder dem Integrieren einiger wichtiger Tipps in den Arbeitsalltag können Sie einen wichtigen Beitrag zum Datenschutz leisten. Wie wäre es beispielsweise mit den folgenden Tipps:

Tipp Nr. 1: Prüfen Sie, ob Hacker Ihre Daten haben

Zwar werden Sie nie ganz genau wissen, wer Ihre E-Mail-Adresse etwa für Phishing missbrauchen wird. Aber Sie können checken, inwieweit Ihre E-Mail-Adresse oder weitere teils sehr sensible Informationen bei Datenlecks wahrscheinlich in falsche Hände geraten sind oder bereits im Darknet zum Verkauf angeboten wurden.

Dazu können Sie den Service „Identity Leak Checker" des Hasso-Plattner-Instituts nutzen (https://t1p.de/s8j2) oder das Angebot von „Have I Been Pwned" unter https://t1p.de/iwe9. Gibt es bei Eingabe der E-Mail-Adresse einen Treffer, sollten Sie auf der Hut sein. Vielleicht werden an Ihre E-Mail-Adresse unter Verwendung weiterer erbeuteter Informationen Phishing-E-Mails geschickt. Probieren Sie doch auch mal Ihre private E-Mail-Adresse aus. Gibt es hier einen Treffer und sind etwa auch Passwörter vom Datenleck betroffen, sollten Sie am besten das Passwort für den betreffenden Account ändern.

Tipp Nr. 2: Machen Sie einen Passwort-Check

Nehmen Sie sich heute zehn Minuten Zeit. Prüfen Sie, wo Sie schwache Passwörter einsetzen oder Passwörter mehrfach verwenden. Denn genau das sollten Sie nicht machen. Ersetzen Sie schlechte Passwörter durch neue komplexe Passwörter. Für das Erzeugen komplexer Passwörter können Sie auf einen Passwortmanager setzen. Der hilft Ihnen auch, die individuellen und komplexen Passwörter zu managen und sicher aufzubewahren.

Machen Sie Kriminellen das Leben zusätzlich schwer. Nutzen Sie nach Möglichkeit weitere Faktoren zur Authentisierung, etwa kurzfristig generierte Codes oder die Zugriffsfreigabe in einer App. Ein Täter hat es damit schon erheblich schwerer, etwa Zugriff auf ein Benutzerkonto zu nehmen.

Tipp Nr. 3: Kontrollieren Sie, was die digitale Welt über Sie weiß

Vielleicht gehören Sie zu denjenigen Menschen, die das Thema Datenschutz als „überbewertet" ansehen, gerade weil Sie meinen, dass Sie nichts zu verbergen hätten. Doch zu verbergen hat jeder Mensch etwas, ganz sicher auch Sie. Denken Sie hier an Meinungen oder Vorlieben, egal in welchem Zusammenhang. Nicht immer ist es unerheblich, wenn jedermann darüber Bescheid wüsste. Bestimmt gibt es manches, von dem Ihr Vorgesetzter, Kollegen oder Nachbarn nichts wissen sollten. Daher ist wichtig: Gehen Sie immer sparsam mit Informationen über Sie um. Das gilt gerade für alles, was Sie im Internet oder in sozialen Netzwerken von sich geben und über sich mitteilen. Denn: Was einmal veröffentlicht ist, lässt sich meist nur noch schwer einfangen, geschweige denn löschen. Daher: Löschen Sie nicht erforderliche Informationen über Sie.

Übrigens: Datensparsamkeit ist auch Schutz vor Cyberkriminellen. Geraten sensible Informationen über Sie in falsche Hände, können diese nicht nur für Phishing & Co. genutzt werden. Je nach Information kann man Ihren Ruf schädigen oder Sie gar mit der Drohung einer Veröffentlichung erpressen.

Tipp Nr. 4: Sichern Sie sich für den Fall der Fälle ab

Haben Hacker & Co. Erfolg, legen sie Systeme lahm oder verschlüsseln zwecks Lösegelderpressung Daten. Oder es geht ihnen einfach nur darum, Schaden anzurichten. Eine wichtige „(Über-)Lebensversicherung" sind hier Datensicherungen, sprich Back-ups. Machen Sie von allem Wichtigen regelmäßig Back-ups oder sichern Sie Daten an mehreren Orten bzw. auf unterschiedliche Weise. Achten Sie dabei darauf, dass die Sicherungen selbst vor unbefugtem Zugriff geschützt sind. Nutzen Sie spezielle Back-up-Spftware, sollten Sie unbedingt auch einmal testen, ob Sie im Fall der Fälle auf die gesicherten Daten zugreifen oder diese wiederherstellen könnten. Das beste Back-up bringst Ihnen nichts, wenn auch Sie keinen Zugriff mehr auf die Daten haben.

Tipp Nr. 5: Machen Sie sich mit relevanten Prozessen vertraut

Früher oder später kann es auch Sie treffen: Da geht vielleicht eine Phishing-E-Mail ein, die Sie zunächst nicht als solche erkennen, oder Sie finden plötzlich auf Ihrem Computer verschlüsselte Dateien. Im Fall der Fälle müssen Sie richtig reagieren. Wichtig ist also, dass Sie wissen, was zu tun ist. Auf der Intranetseite des Datenschutzbeauftragten sind unter „Hilfe im Notfall" alle wichtigen Verhaltensregeln zusammengestellt. Egal, ob Phishing-E-Mail, Verschlüsselungstrojaner oder seltsames Verhalten von Computer, Smartphone & Co.: Sie finden hier maßgeschneiderte Vorgehensweisen, an denen Sie sich orientieren sollten. Setzen Sie am besten direkt ein Lesezeichen in Ihrem Browser.

Danke für Ihre Unterstützung und viel Erfolg beim Umsetzen! Bei Fragen: Melden Sie sich einfach!

Ihr Datenschutzbeauftragter

Arno Nym

Gerade zum Jahreswechsel sinnvoll: der Impressums-Check

Eventuell gibt es bei Ihrem Unternehmen mit dem neuen Jahr Veränderungen bei der Unternehmensleitung. Und vielleicht wird mancher Anpassungsbedarf übersehen, was schnell zum Problem werden kann. So z. B. beim Thema Impressum.

Pflichtangaben ergeben sich aus § 5 DDG

Wer digitale Dienste (z. B. Webseiten, Apps, Auftritte in sozialen Netzwerken) anbietet, muss bestimmte Informationen zur Verfügung stellen. Diese ergeben sich aus § 5 Digitale-Dienste-Gesetz (DDG). Diese Regelung kennen Sie vielleicht schon. Früher fanden Sie die nämlich im Telemediengesetz (TMG). Je nach Situation eines Anbieters müssen verschieden umfangreiche Informationen gegeben werden.

Gehen Sie wie folgt vor

Eine Prüfung können Sie im Handumdrehen vornehmen. Beispielsweise folgendermaßen:

- **Schritt 1 – sammeln Sie zunächst relevante Informationen:** Stellen Sie die nötigen Informationen zusammen. Hier kann auch der Blick in offizielle Unterlagen oder Quellen sinnvoll sein, etwa das Handelsregister. Gehen Sie dann die einzelnen Punkte von § 5 DDG durch.
- **Schritt 2 – führen Sie bei Webseiten eine Sichtprüfung durch:** Nutzen Sie die abgedruckte Checkliste für eine eingehende Prüfung.
- **Schritt 3 – testen Sie die Apps Ihres Unternehmens:** Auch hier muss alles passen. Prüfen Sie ebenfalls anhand der Checkliste, ob alle Aspekte eingehalten sind.
- **Schritt 4 – dokumentieren Sie Abweichungen:** Halten Sie Unzulänglichkeiten fest. Praktischerweise können Sie hier auch auf Screenshots oder Bildschirmvideos setzen.
- **Schritt 5 – sprechen Sie mit den zuständigen Kollegen:** Bitten Sie die Kollegen um einen kurzen Austausch. Erläutern Sie Ihre Feststellungen und übergeben Sie die Sache zur weiteren Erledigung.

Checkliste: Passt alles im Impressum?

Prüfpunkt	Das sollten Sie beachten	In Ordnung?
Wie ist die Seite mit den Pflichtinformationen bezeichnet?	› Im deutschsprachigen Raum ist „Impressum" wohl am weitesten verbreitet. Allerdings ist auch gegen „Anbieterkennzeichnung" nichts einzuwenden. Problematischer kann es mit Begriffen werden, die sich einem Seitenbesucher nicht auf Anhieb erschließen, etwa „Kontakt" oder „Hilfe". › Richtet sich das Angebot auch an anderssprachige Seitenbesucher, sollte es auch für das Impressum weitere Sprachversionen geben. Z. B. im Englischen ist hier aber nicht „Imprint" angesagt, sondern „Legal notice".	○ Ja ○ Nein
Ist die Seite mit der Anbieterkennzeichnung leicht zu finden bzw. zu erkennen?	› Hier kommt es auf die Auffindbarkeit bzw. Sichtbarkeit an, sprich, wo der Link zur Seite verortet ist. Üblicherweise ist das ganz oben oder ganz unten auf der Seite. › Achten Sie auch auf die Schriftgröße und Farbe. Der Eindruck des Versteckens darf sich nicht aufdrängen. › Eine Nutzung von Symbolen kann in Sachen Auffindbarkeit zum Problem werden.	○ Ja ○ Nein
Bedarf es maximal zwei Klicks, um die Informationen zu erreichen?	› Probieren Sie aus, wie einfach Sie die Informationen erreichen können. Das Unterbringen im „Keller" der Webseite ist genauso problematisch wie eine ggf. erforderliche „Klickorgie". Mehr als zwei Klicks sollten nicht benötigt werden. › Versuchen Sie, die Informationen von verschiedenen Unterseiten aus zu erreichen. Auch hier darf es keine Erschwernis geben.	○ Ja ○ Nein
Besteht ständige Verfügbarkeit der Informationen?	› Setzen Sie bei Ihrem Test auf verschiedene gängige Browser. Testen Sie beispielsweise, ob die betreffende Seite in Chrome, Edge, Firefox oder Safari richtig angezeigt wird und auch die Links zu den Informationen funktionieren. › Ein Test auf Tablets oder Smartphones kann zudem zeigen, ob die Mobilversionen eines Webangebots auch tatsächlich so funktionieren wie gedacht. Nicht selten kommt es hier zu Problemen, die behoben werden müssen.	○ Ja ○ Nein
Sind die Angaben vollständig?	› Orientieren Sie sich dazu an den Vorgaben des § 5 DDG. Achten Sie hier auch auf Kleinigkeiten wie ganz ausgeschriebene Vornamen von Vertretungsberechtigten. › Müssen besondere Angaben gemacht oder Links gesetzt werden, etwa zu speziellen Rechtsvorschriften, sollten Sie prüfen, ob diese funktionieren.	○ Ja ○ Nein
Sind nur erforderliche personenbezogene Informationen enthalten?	› Es handelt sich um Pflichtangaben, die auch zum Teil personenbezogen sind. Insofern lässt sich die Verarbeitung auf Art. 6 Abs. 1 Satz 1 Buchst. c Datenschutz-Grundverordnung i. V. m. § 5 DDG stützen. › Finden Sie aus Ihrer Sicht nicht erforderliche Informationen, sollten Sie deren Notwendigkeit mit den zuständigen Kollegen klären. Schließlich müssen auch Datenschutzverstöße vermieden werden.	○ Ja ○ Nein
Bestehen Gesetzesreferenzen und sind diese aktuell?	› Halten Sie Ausschau nach Bezügen zu veralteten Gesetzen. Das TMG gibt es nicht mehr, vielmehr nur noch das DDG. › Empfehlen Sie, nicht erforderliche Referenzen zu streichen. „Impressum" reicht, ein „nach § 5 DDG" ist nicht nötig.	○ Ja ○ Nein
Müssen anderswo Anpassungen vorgenommen werden?	› Gibt es relevante Änderungen beim Impressum, sind meist auch anderswo Überarbeitungen nötig. › Haben Sie insbesondere ein Auge auf die Allgemeinen Geschäftsbedingungen oder die Datenschutzhinweise mit den Informationen zum Verantwortlichen.	○ Ja ○ Nein

Neuer BSI-Bericht: Machen Sie auf das Cyberrisiko aufmerksam

Vielleicht geht es Ihnen wie manchem Datenschutzbeauftragten: Sie reden sich den Mund fusselig, doch irgendwie scheint sich niemand so wirklich für die Gefahren durch Cyberkriminelle zu interessieren. Viel bringen kann in einer solchen Situation, wenn Sie auf „Meinungsverstärker" setzen, etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI) und seinen aktuellen Lagebericht für 2025.

Wegschauen bringt nichts

Auch wenn mancher in den Führungsetagen es praktizieren mag: Den Kopf in den Sand stecken und hoffen, dass Cyberkriminelle kein Interesse am eigenen Unternehmen haben, ist geradezu grob fahrlässig. Das zeigt auch der Bericht des BSI „Die Lage der IT-Sicherheit in Deutschland 2025", der die Entwicklungen vom 1.7.2024 bis 30.6.2025 darstellt.

Das können Sie aus dem Lagebericht folgern

Um es auf den Punkt zu bringen: Die Lage ist nicht rosig. Aus dem Bericht können Sie beispielsweise folgende Erkenntnisse gewinnen:

- **Die Sicherheitslage bleibt angespannt**
  Es gibt aus BSI-Sicht keinen Grund zur Entwarnung. Doch nicht nur Cyberkriminalität selbst und geopolitische Aspekte führen zu einer Zuspitzung. Ein Problem ist vor allem der unzureichende Schutz vor Angriffen. Die Zahl der Angriffe, Vorfälle und Störungen ging nicht zurück.
- **Immer mehr Schwachstellen**
  Erschreckende Zahlen: Im Berichtszeitraum wurden im Durchschnitt täglich 119 Schwachstellen festgestellt, die Cyberkriminelle ausnutzen können. Das ist eine Steigerung von 24 % gegenüber dem Vorjahr. Zwar sank die Zahl der neuen Malware-Varianten um 9 %. Es wurden aber noch immer täglich durchschnittlich 280.000 neue Schadprogramm-Varianten bekannt.
- **Cyberkriminelle arbeiten immer professioneller**
  Cyberkriminelle arbeiten nicht nur arbeitsteilig und verwenden beispielsweise vorgefertigte Bausteine, Schadprogramme oder Angebote spezialisierter Krimineller. Sie nutzen auch schnell Sicherheitslücken aus, um erfolgreiche Angriffe auszuführen. Insgesamt führt die Professionalisierung dazu, dass mehr, schneller und professioneller angegriffen wird.
- **Erfolgsmodell Ransomware**
  Wie im Vorjahr wurden dem Bundeskriminalamt rund 950 Ransomware-Angriffe bekannt. Daraus resultierten meist auch Datenlecks, und zwar in 72 % der anzeigten Fälle.
- **Kleine und mittelständische Unternehmen sind bevorzugte Opfer**
  Gerade kleine und mittelständische Unternehmen (KMU) sind einem erhöhten Risiko ausgesetzt, Opfer von Cyberkriminellen zu werden. Diese nehmen die KMU gerade deshalb in den Fokus, weil es dort meist mit den Sicherheitsmaßnahmen, den erforderlichen Ressourcen oder dem nötigen Know-how hapert. Zudem werden die Gefahren und potenziellen Risiken in KMU meist unterschätzt. Die Folge: Rund 80 % der Angriffe mit Ransomware richteten sich gegen KMU. Ein weiterer Grund: Oft wählen Cyberkriminelle Opfer nicht nach dem höchsten Erpressungspotenzial aus, sondern nach den schwächsten Sicherheitsvorkehrungen.
- **Das Web ist Angriffsfläche Nummer 1**
  Hier ist die Lage aus Sicht des BSI besorgniserregend. Zu oft wurden bereits bekannte Schwachstellen erst spät oder überhaupt nicht behoben. Zudem wurde bei rund 61 % der über deutsche Domains erreichbaren Webseiten weiterhin das weniger sichere IPv4-Protokoll verwendet. Auch waren zu 47 % der erreichbaren IP-Adressen sensible und sicherheitskritische Informationen etwa über Scan-Dienstleister abrufbar. Diese können auch Schlüsse auf Sicherheitslücken zulassen.
- **Zunahme der digitalen Sorglosigkeit**
  Bedenklich ist auch folgende Feststellung des BSI: Dass gerade auch Verbraucher in Sachen Schutz und Resilienz aktiv werden müssen, liegt zwar auf der Hand. Allerdings sinkt bei Verbrauchern der Bekanntheitsgrad von Schutzmaßnahmen. Zudem werden sie weniger angewendet. Das gilt gerade für sichere Passwörter.

Hier finden Sie den Bericht

Sie wollen sich selbst mit den Ergebnissen des BSI-Lageberichts vertraut machen? Kein Problem. Diesen finden Sie im Onlineangebot des BSI über diesen Link: https://t1p.de/num38. Dort lesen Sie auch viele Übersichten und grafische Darstellungen.

Regelmäßig besteht hohe Datenschutzrelevanz

Mancher meint: Cyberkriminellen geht es um das schnelle Geld und gerade nicht um personenbezogene Daten. Doch meist liegt man hier vollkommen falsch. Einerseits kann ein Unternehmen als Verantwortlicher für die personenbezogenen Daten leichter erpresst werden. Andererseits können etwa gestohlene persönliche Informationen verwendet werden, um einzelne Betroffene zu schädigen.

Zudem hat meist jeder erfolgreiche Angriff auch eine Datenschutzdimension. Denn klar ist: Jeder Hackerangriff, jeder Datendiebstahl und jeder Social-Engineering-Angriff bringen erhebliche Risiken

im Datenschutz mit sich. Dabei sind nicht einfach nur personenbezogene Daten „weg". In vielen Fällen handelt es sich um einen Vorfall, der nach Art. 33 Datenschutz-Grundverordnung (DSGVO) an die zuständige Datenschutzaufsichtsbehörde zu melden ist. Denn: Auch bei einem erfolgreichen Datendiebstahl kommt es zu einer Verletzung des Schutzes personenbezogener Daten. Damit ist jede Sicherheitsverletzung gemeint, die, ob unbeabsichtigt oder unrechtmäßig,

- zur Vernichtung,
- zum Verlust,
- zur Veränderung,
- zur unbefugten Offenlegung oder
- zum unbefugten Zugang

personenbezogener Daten führt (Art. 4 Nr. 12 DSGVO). Meldet das Unternehmen den Vorfall nicht binnen 72 Stunden nach Kenntnisnahme bzw. überhaupt nicht, kann das zu einem schmerzhaften Bußgeld führen (Art. 33, 83 Abs. 4 DSGVO).

Nutzen Sie den Lagebericht für Prüfungen und Gespräche

Probleme ignorieren hilft nicht weiter. Auch die Hoffnung, dass Cyberkriminelle einen großen Bogen um das Unternehmen machen, dürfte früher oder später enttäuscht werden. Vielmehr ist es wichtig, dass auch Sie als Datenschutzbeauftragter ein Auge auf denkbare Gefahren und Risiken haben. Der Lagebericht des BSI bietet Ihnen eine gute Grundlage, um mit relevanten Kollegen oder der Unternehmensleitung ins Gespräch zu kommen. Für Ihr Gespräch können Sie auch folgende Checkliste als Gedankenstütze nutzen. Zudem ist sie gut geeignet, um den Stand der Dinge in Ihrem Unternehmen genauer unter die Lupe zu nehmen.

Checkliste: Typische Aspekte und Diskussionspunkte zur Cybersecurity

Aspekt	Hintergrund	Geprüft und in Ordnung?
Ist das obere Management für Gefahren und Risiken sensibilisiert?	› Der Unternehmensleitung und dem oberen Management muss bewusst sein, dass auch das eigene Unternehmen im Fokus von Cyberkriminellen steht. Es stellt sich meist nicht die Frage, ob es angegriffen wird, sondern nur wann. › Angemessene Schutzmaßnahmen müssen Teil der Risikovorsorge sein. Dazu ist auch die Unternehmensleitung verpflichtet. Schließlich kann ein erfolgreicher Angriff schnell die Existenz des Unternehmens bedrohen. War man zu naiv oder blauäugig in Sachen Sicherheit unterwegs, kann das auch zur Haftung der Unternehmenslenker führen.	○ Ja ○ Nein
Verfügt das Unternehmen über das nötige Know-how?	› Abhängig davon, was Ihr Unternehmen macht, wie datenintensiv die Tätigkeit ist, wie schutzwürdig Systeme und Informationen sind sowie wie risikobehaftet das Ganze ist, muss Ihr Unternehmen über mehr oder weniger Spezialisten verfügen. › Machen Sie sich ein eigenes Bild. Sprechen Sie jedoch auch mit Fachabteilungen. Das kann beispielsweise die IT-Abteilung sein. Doch auch wenn es um das Business Continuity Management geht, sollten Sie auf fachkundige Einschätzungen setzen.	○ Ja ○ Nein
Welche Strategie verfolgt Ihr Unternehmen zum Schutz vor Cyberkriminellen?	› Hier geht es um das große Ganze. Um planvoll vorzugehen und beispielsweise Ressourcen und Mittel risikoorientiert einzusetzen, bedarf es einer übergeordneten Strategie. › Lassen Sie sich eine Strategie im Detail erklären. So können Sie Lücken, Fehlannahmen oder Unzulänglichkeiten am besten erkennen.	○ Ja ○ Nein
Wer ist für Schutz- und Abwehrmaßnahmen verantwortlich bzw. zuständig?	› Es sind nicht nur Regelungen und Anweisungen wichtig. Auch klare Verantwortungszuweisungen sind unerlässlich. › Gibt es in Regelungen entsprechende Zuweisungen, sollten Sie klären, inwieweit die Betroffenen von ihrem „Glück" wissen und ob diese die Verantwortung übernehmen bzw. die Aufgaben stemmen können.	○ Ja ○ Nein
Welche Sicherheitskonzepte bestehen?	› Konkrete Konzepte sind wichtig, um eine Strategie auszuformen und umzusetzen. › Prüfen Sie, für welche Gefahren oder Szenarien Schutz- oder Abwehrkonzepte entwickelt wurden. Besonders wichtig sind Konzepte für alles, was eine Verbindung ins Internet hat. › Kontrollieren Sie nicht nur die Schlüssigkeit solcher Konzepte. Untersuchen Sie risikoorientiert und stichprobenhaft, inwieweit die Maßnahmen angemessen und up to date sind. Gerade nicht mehr zeitgemäße Schutzmaßnahmen sind schon ein Risiko an sich. › Zu den Sicherheitskonzepten zählt auch eine gute Back-up-Strategie. Back-ups können die Lebensversicherung für Ihr Unternehmen sein, wenn Daten von Kriminellen zwecks Lösegelderpressung verschlüsselt werden.	○ Ja ○ Nein
Wie erfolgt die Umsetzung der Konzepte?	› Hinterfragen Sie die praktische Umsetzung. Lassen Sie sich konkret erklären, wie man vorgeht. › Besprechen Sie, inwieweit ausreichend Ressourcen zur Verfügung stehen. Ist etwa das Budget der limitierende Faktor, kann auch das die Risikosituation erheblich verschlechtern.	○ Ja ○ Nein
Ist die im Unternehmen eingesetzte IT sicher und aktuell?	› Nehmen Sie insbesondere die IT in den Fokus, die eine Verbindung zum Internet unterhält. Das geht vom Computer über das Smartphone bis hin zum großen Entwicklungsnetzwerk. › Gerade veraltete Computer, Betriebssysteme oder Software können ein erhebliches Sicherheitsproblem sein. Hier besteht dringender Handlungsbedarf.	○ Ja ○ Nein
Inwieweit können Gefahren erkannt und schnell behoben werden?	› Hier geht es vor allem um Prävention und Früherkennung. Werden Angriffsversuche nicht erkannt, hat ein Krimineller alle Zeit der Welt, um sämtliche Möglichkeiten auszuprobieren. › Hinterfragen Sie hier auch, inwieweit Pläne und Prozesse für Vor-, Not- und Krisenfälle bestehen. Diese müssen nicht nur gut durchdacht und praxistauglich sein. Besprechen Sie auch, inwieweit diese ausprobiert wurden, idealerweise unter möglichst realen Bedingungen.	○ Ja ○ Nein
Wie steht es um die Awareness von Beschäftigten?	› Auch das BSI hat festgestellt, dass die digitale Sorglosigkeit zunimmt. Dem sollte im Unternehmen gegengesteuert werden, etwa durch konkrete Informationen, Schulungen oder Awarenessaktivitäten. › Tauschen Sie sich mit Kollegen aus anderen Bereichen aus (z. B. im Bereich IT oder Cybersecurity), wie diese die Situation und den Handlungsbedarf wahrnehmen.	○ Ja ○ Nein

Wie hoch ist das Bußgeldrisiko? So finden Sie eine Antwort

Wenn es um Datenschutz geht, ist bei Entscheidern oft eines nicht weit: die Frage, ob dies oder jenes zu einem Bußgeld führen kann. Oder ob Ihr Unternehmen bußgeldgefährdet ist, wenn man es mit dieser oder jener Anforderung der Datenschutz-Grundverordnung nicht so genau nimmt. Fragt man Sie, müssen Sie um eine Antwort nicht verlegen sein.

Mit Risiken ist es immer so eine Sache

Fragt man Sie nach dem Bußgeldrisiko, etwa wenn man eine Verarbeitung auf eine wacklige Rechtsgrundlage stützen will, können Sie „juristisch sauber" antworten, indem Sie sagen: „Es kommt ganz darauf an." Wie bei allen Risiken lässt sich meist nämlich auch beim Bußgeldrisiko nicht mit Sicherheit sagen, ob und unter welchen Umständen sich dieses realisiert.

Allerdings können Sie mit den Kollegen stets Aspekte oder Faktoren durchsprechen, die ein Bußgeld wahrscheinlicher machen können. Dazu können Sie die folgende Checkliste nutzen. Je öfter Sie mit einem Ja antworten müssen, desto höher steigt das Risiko.

Checkliste: Faktoren, die ein Bußgeld wahrscheinlicher machen können

Faktoren	Erläuterungen	Trifft zu?
Die Verarbeitung umfasst viele Betroffene oder es werden viele personenbezogene Daten verarbeitet.	Je umfassender eine Verarbeitung ist, desto größer können auch die Risiken werden, dass etwas schiefgeht. Damit erhöht sich auch grundsätzlich das Risiko, dass es zu einem Bußgeld kommen kann.	○ Ja ○ Nein
Es findet eine Verarbeitung von besonderen Kategorien personenbezogener Daten statt.	Sensible Informationen müssen besonders geschützt werden. Werden sie gestohlen oder geraten sie in falsche Hände, kann das erhebliche negative Auswirkungen auf die Betroffenen haben. Waren etwa die Schutzmaßnahmen unzureichend, kann das eher zu einem Bußgeld führen.	○ Ja ○ Nein
Die Branche, die Geschäftstätigkeit oder die Verarbeitung stehen im Fokus von Medien oder Aufsichtsbehörden.	Ist Ihr Unternehmen in einer Branche tätig, in der es unter Datenschutzaspekten viele schwarze Schafe gibt, kann auch das Risiko steigen, dass man bei Ihrem Unternehmen genauer hinschaut. Werden schwere Defizite festgestellt, kann man an Ihrem Unternehmen ein Exempel statuieren wollen.	○ Ja ○ Nein
Es kommen risikobehaftete Technologien zum Einsatz.	Denken Sie hier beispielsweise an künstliche Intelligenz oder neue Verarbeitungsmethoden. Gerade wenn die Dinge nicht ausgereift sind, kann eher etwas schiefgehen.	○ Ja ○ Nein
Die Verarbeitung der Daten kann erhebliche Beeinträchtigungen des Persönlichkeitsrechts mit sich bringen.	Betrachten Sie die Auswirkungen auf Betroffene. Nicht nur besondere Datenkategorien können schwer beeinträchtigen. Auch Finanzinformationen können zum Problem für Betroffene werden, wenn diese bei den Falschen landen.	○ Ja ○ Nein
Anforderungen zum Datenschutz werden absichtlich ignoriert oder missachtet.	Nimmt man Datenschutz nicht ernst oder überschreitet man absichtlich Grenzen, kann das schnell nach hinten losgehen. Wird ein Verstoß publik, kann ein Bußgeld ggf. unausweichlich sein.	○ Ja ○ Nein
Die konkrete Verarbeitung ist dem Datenschutzbeauftragten bislang unbekannt.	Wissen Sie von nichts, waren Sie wahrscheinlich auch nicht eingebunden. Eventuell hat man wichtige Aspekte zum Datenschutz erst gar nicht berücksichtigt.	○ Ja ○ Nein
Wie sich die Verarbeitung konkret gestaltet, ist unklar.	Kann man die Verarbeitung nicht konkret beschreiben und fehlen auch im Verzeichnis von Verarbeitungstätigkeiten die erforderlichen Informationen, kann das darauf hindeuten, dass es bei der Verarbeitung drunter und drüber geht.	○ Ja ○ Nein
Inwieweit der Schutzbedarf festgestellt, Gefahren identifiziert und Risiken abgeleitet wurden, ist unklar.	Es muss bei jeder Verarbeitung ausgemacht werden, was zu schützen ist und welche Risiken bestehen. Ferner müssen Maßnahmen in diesem Zusammenhang ergriffen werden, etwa um hohe Risiken zu reduzieren. Passiert hier nichts, kann das eher zum Verstoß oder zur Panne führen. Das wiederum erhöht das Bußgeldrisiko.	○ Ja ○ Nein
Die Verarbeitung findet im Internet statt oder hat eine Verbindung ins Internet.	Cyberkriminelle werden in aller Regel über das Internet aktiv. Insofern sind entsprechende Schutzmaßnahmen erforderlich, damit eine Verarbeitung bzw. die betreffenden Daten sicher sind. Defizite rächen sich – früher oder später.	○ Ja ○ Nein
Es ist unklar, inwieweit eingebundene Dienstleister in Sachen Datenschutz und Datensicherheit zuverlässig sind.	Auch beim Dienstleister muss Datenschutz einen hohen Stellenwert haben. Er muss vorgegebene Schutzmaßnahmen auch tatsächlich umsetzen. Passt es hier nicht, kann das auch zum Problem für Ihr Unternehmen werden.	○ Ja ○ Nein
Die Datenverarbeitung findet im Ausland statt, wobei das Datenschutzniveau unklar ist.	Auch in Drittstaaten muss ein angemessenes Datenschutzniveau sichergestellt sein. Wurde hier nichts geprüft und nichts geregelt, kann das zum Bußgeld führen.	○ Ja ○ Nein
Beschäftigte sind nicht angemessen angewiesen, informiert oder geschult.	Fehlt es an Weisungen, am nötigen Wissen oder der erforderlichen Sensibilität, kann leicht etwas schiefgehen, auch ohne Absicht. Auch damit kann sich ein Unternehmen ein Bußgeld einhandeln.	○ Ja ○ Nein

Wie müssen wir beim Datenmissbrauch reagieren?

FRAGE: Ein Mitarbeiter in unserem Unternehmen hat Kundendaten an einen Bekannten weitergegeben, damit dieser sich nach Gründung einer eigenen Firma leichter einen Kundenstamm aufbauen kann. Bemerkt wurde das, als Werbung an Adressen aus Kontrolldatensätzen geschickt wurde. Aus unserer Sicht liegt hier ganz klar ein Datenschutzverstoß vor. Allerdings stellen sich uns nun einige wichtige Fragen: Sind wir für den Datenmissbrauch als eigentlich für die Daten verantwortliche Stelle haftbar? Müssen wir dem betreffenden Mitarbeiter kündigen, wo ihm doch aufgrund der unterschriebenen Verpflichtungserklärung bewusst war, dass eine eigenmächtige Verarbeitung personenbezogener Daten verboten ist?

ANTWORT: Wahrscheinlich ist es zunächst noch erforderlich, dass die Umstände und der Sachverhalt detailliert geklärt werden. So sollte geprüft werden, inwieweit dem betreffenden Mitarbeiter bewusst war, dass er etwas Unerlaubtes macht. Wichtig ist in diesem Zusammenhang, was in der Verpflichtungserklärung stand, deren Kenntnisnahme der Mann mit seiner Unterschrift bestätigt hat. Ferner ist relevant, ob und wenn ja welche Schulungen stattfanden. Zudem sollten Sie klären, welche Vorschriften, Regelungen oder (An-)Weisungen zum Umgang mit personenbezogenen Daten es gab.

Mitarbeiterexzess dürfte vorliegen

Stellt sich heraus, dass der Mitarbeiter Weisungen ignoriert und personenbezogene Daten zu eigenen Zwecken bzw. für Zwecke Dritter verarbeitet hat, ist die Sache ziemlich klar: Es ist zu einem sogenannten Mitarbeiterexzess gekommen. Der Mitarbeiter hat eigenmächtig die Grenzen des Erlaubten überschritten. Datenschutzrechtlich gesehen hat er eigenmächtig selbst über Zwecke und Mittel der Verarbeitung personenbezogener Daten entschieden. Insofern kann das Verhalten des Arbeitnehmers auch nicht mehr dem Arbeitgeber zugerechnet werden. Er ist also selbst zum Verantwortlichen geworden, sodass für ihn die Rahmenbedingungen der Datenschutz-Grundverordnung (DSGVO) greifen. Das gilt eben auch für das Erfordernis, nur rechtmäßige Verarbeitungen durchzuführen. Weil jedoch keine rechtmäßige Verarbeitung stattgefunden hat, ist er auch für den Verstoß verantwortlich und haftet entsprechend. Kommt es zu einem Bußgeldverfahren durch die Datenschutzaufsichtsbehörde, dürfte man dieses in erster Linie an den betreffenden Mitarbeiter richten. Ihr Unternehmen wäre aus der Schusslinie.

Über die Konsequenzen müssen nicht Sie entscheiden

Welche Konsequenzen im Hinblick auf den Mitarbeiter denkbar sind, ist in erster Linie eine arbeitsrechtliche Frage. Hier ist entscheidend, wie gravierend der Verstoß und wie groß ein eventueller Vertrauensverlust zum Mitarbeiter ist. Zudem stellt sich die Frage, ob aufgrund der Schwere des Pflichtverstoßes von einem wichtigen Grund im Sinne des § 626 Bürgerliches Gesetzbuch auszugehen ist. Ist dies der Fall, kann dies Ihr Unternehmen zu einer außerordentlichen Kündigung berechtigen. Dabei ist wichtig: Welche Konsequenzen man zieht, ob man eine Abmahnung oder eine ordentliche bzw. außerordentliche Kündigung ausspricht, ist allein Sache des Arbeitgebers. Schon deshalb, um als Datenschutzbeauftragter in keinen Interessenkonflikt zu kommen, sollten Sie die Prüfung der und die Entscheidung über arbeitsrechtliche Konsequenzen voll dem Arbeitgeber überlassen.

Gibt es die DIN 66399 nicht mehr?

FRAGE: Bei uns müssen größere Datenmengen datenschutzkonform und dokumentiert vernichtet werden. Dazu wollen wir einen Dienstleister beauftragen. Bislang gab es doch zur Orientierung bei der Auswahl die DIN 66399. Nun habe ich gehört, dass diese DIN-Norm nicht mehr gelten soll. Auf diese verweist aber der favorisierte Dienstleister in seinem Sicherheitskonzept. Gibt es die DIN 66399 tatsächlich nicht mehr?

ANTWORT: Hier bietet es sich an, dass Ihr Unternehmen zunächst mit dem Anbieter spricht. Ggf. hat Ihr Unternehmen nämlich noch ein zwischenzeitlich minimal veraltetes Dokument erhalten, in dem auf die DIN 66399 Bezug genommen wird. In der Tat ist es nämlich so, dass die im Zusammenhang mit datenschutzkonformer Vernichtung von Daten und Datenträgern gerne referenzierte DIN 66399 zurückgezogen wurde. Anstelle der deutschen Norm gilt nun die internationale Norm ISO/IEC 21964. Diese ist im Wesentlichen inhaltsgleich zur bisherigen DIN-Norm. Daher: Sind Maßnahmen umgesetzt bzw. können die Standards der bisherigen Norm eingehalten werden, spricht zumindest eine nicht nachgezogene Anpassung der Norm nicht gegen einen Dienstleister.

Auskunft muss nicht binnen einem Monat gegeben werden

Es gibt Gerichtsentscheidungen, von denen Sie als Datenschutzbeauftragter einfach gehört haben sollten. Und nicht selten sind es Entscheidungen, die eher unscheinbar daherkommen und auf den ersten Blick eher wenig mit Datenschutz zu tun haben. So ist es auch bei einer Entscheidung des Verwaltungsgerichts (VG) Düsseldorf (Beschluss vom 5.9.2025, Az. 29 K 6375/25).

Darüber hatte das VG zu entscheiden

Ein Bürger (der spätere Kläger) wollte gegen eine Behörde vorgehen, wahrscheinlich weil diese aus seiner Sicht nicht aktiv wurde, eben nicht rechtzeitig die von ihm gewünschte Auskunft erteilte und somit nicht den begehrten Verwaltungsakt vornahm.

Zeitlich war die Sache wie folgt einzuordnen: Seinen Anspruch auf Auskunft nach Art. 15 Datenschutz-Grundverordnung (DSGVO) machte der Bürger am 16.5.2025 geltend. Die Behörde teilte dem Bürger am 20.5.2025 mit, dass sein Schreiben zur geforderten Auskunft eingegangen sei, sein Anliegen geprüft werde, allerdings die Klärung Zeit in Anspruch nehmen könne. Dann zog sich die Sache wohl hin.

Weil die Behörde nicht wie gewünscht aktiv wurde, wollte der Bürger eine Untätigkeitsklage anstrengen. Die reichte er am 23.6.2025 ein, also nach Ablauf der aus Art. 12 DSGVO bekannten Monatsfrist. Allerdings fehlte es am Geld. Daher beantragte er Prozesskostenhilfe. Die wurde nicht gewährt, was sich aus dem Beschluss des VG Düsseldorf ergibt.

So entschied das VG

Der Antrag auf Prozesskostenhilfe war insgesamt abzulehnen. Vom Kläger wurden keine Belege zu seiner wirtschaftlichen Situation, etwa der Bescheid über Bürgergeld, eingereicht. Zudem hätte nach Ansicht des VG die beabsichtigte Klage keine Aussicht auf Erfolg gehabt.

Das liegt unter anderem daran, dass der Kläger seine Untätigkeitsklage verfrüht eingereicht hatte. Grundsätzlich ergibt sich aus § 75 Satz 2 Verwaltungsgerichtsordnung, dass vor Ablauf von drei Monaten seit Beantragung eines Verwaltungsakts keine Klage wegen Untätigkeit erhoben werden kann. Als der Kläger seine Klage erhob, war diese Dreimonatsfrist noch nicht abgelaufen.

Dreimonatsfrist greift voll

Besondere Umstände, die zu einer Verkürzung der Frist führen, lagen nicht vor. Das hätten etwa schwere und unverhältnismäßige Nachteile sein können, wenn die Frist nicht verkürzt werden würde. Solche Umstände wurden aber nicht vom Kläger geltend gemacht.

Zwar können als besondere Umstände auch spezialgesetzliche Fristen in Betracht kommen. Allerdings muss nicht entschieden werden, ob die sich aus Art. 12 Abs. 3 Satz 1 DSGVO ergebende Monatsfrist als eine spezialgesetzliche kürzere Bearbeitungsfrist anzusehen ist. Der Grund: Die Behörde ist ihrer Pflicht zur Unterrichtung des Klägers über die ergriffenen Maßnahmen im Zusammenhang mit dem Auskunftsantrag rechtzeitig nachgekommen.

Verantwortliche müssen nur Aktivwerden bestätigen

Aus Art. 12 Abs. 3 Satz 1 DSGVO ergibt sich für Verantwortliche die Pflicht, über die auf Antrag gemäß den Art. 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich zu informieren, wobei dies in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags erfolgen muss. Dabei bezieht sich diese Frist nur auf eine Statusmeldung über die im Zusammenhang mit dem Antrag ergriffenen Maßnahmen. Es wird von der gesetzlichen Regelung keine Frist zur Erfüllung der sich aus Art. 15 bis 22 DSGVO ergebenden Rechte oder Ansprüche vorgegeben. Diese Sichtweise ergibt sich insbesondere aus dem Wortlaut der Regelung, wobei die englische Sprachfassung „provide information on action taken" noch deutlicher ist. Zudem ergibt sich aus Erwägungsgrund 59 zur DSGVO lediglich, dass Verantwortliche verpflichtet sein sollen, den Antrag eines Betroffenen spätestens binnen eines Monats zu beantworten.

Art. 12 DSGVO enthält keine Bearbeitungsfrist

Das lässt sich nicht dem Wortlaut von Art. 12 Abs. 3 Satz 1 DSGVO entnehmen. Außerdem spricht der EU-Gesetzgeber etwa bei der Informationspflicht nach Art. 14 Abs. 3 Buchst. a DSGVO ausdrücklich von einer Erledigungsfrist von einem Monat. Daneben ergeben die Regelungen in Art. 16 und 17 DSGVO im Hinblick auf eine unverzügliche Umsetzung nur einen Sinn, wenn mit Art. 12 Abs. 3 Satz 1 DSGVO keine Erledigungsfrist gemeint ist. Ansonsten wäre das „unverzüglich" in Art. 16 und 17 DSGVO überflüssig.

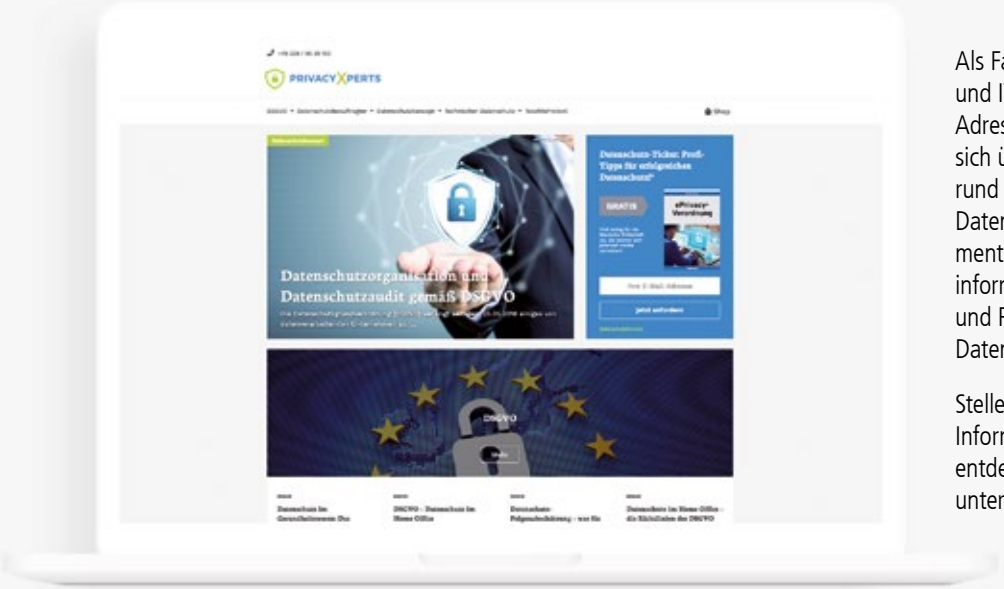
Mit Schreiben vom 20.5.2025 hatte die Behörde über den Status der Anfrage informiert. Sie bestätigte den Eingang des Schreibens, kündigte die Prüfung des Anliegens an und stellte eine ggf. längere Bearbeitungsdauer in Aussicht. Über eine Eingangsbestätigung hinaus wurden insofern auch die ergriffenen Maßnahmen beschrieben. Weil auch die Auskunft sodann erteilt wurde, bestand kein Anlass zu einer verfrühten Untätigkeitsklage.

§

Das können Sie aus dem Beschluss folgern

Es ist gut vertretbar, Betroffenenanfragen grundsätzlich nicht innerhalb eines Monats bearbeitet sein müssen. Art. 12 Abs. 3 Satz 1 DSGVO sieht vom Wortlaut her nur vor, dass unverzüglich und auf jeden Fall innerhalb eines Monats über die ergriffenen Maßnahmen zu informieren ist.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter **www.privacyxperts.de/shop**

Schnell und effektiv Mitarbeiter schulen!

Jetzt Mitarbeiterinformation bestellen

https://t1p.de/gmxhs

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