DATENSCHUTZAKTUELL
MAI II 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

FÜHRERSCHEIN-KONTROLLE: PRÜFEN SIE, OB ALLES PASST

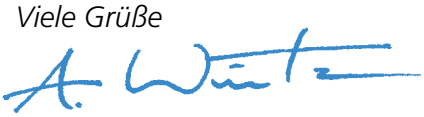
Spielen Sie drei Szenarien durch

Liebe Leserin, lieber Leser,

sind Sie als Datenschutzbeauftragter eher Einzelkämpfer? Bestimmt fallen Ihnen typische Situationen ein, an denen Ihnen das besonders auffällt. So z. B., wenn Sie eine Entscheidung treffen müssen, dazu jedoch keine anderen Meinungen einholen können.

Hier ist es hilfreich, wenn Sie Varianten durchspielen. So beispielsweise drei Szenarien: Eins zielt auf das Normale ab, sprich, es läuft wie üblich. Spielen Sie dann noch ein bestmögliches und ein Worst-Case-Szenario durch. Schätzen Sie dann noch ein, welches dieser Szenarien am wahrscheinlichsten ist. Dem entsprechend können Sie dann Ihr Handeln wirkungsstark ausrichten.

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

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

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: Adobe Stock | Kzenon; Seite 1: Adobe Stock | blende11.photo

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.

Bei einer Datenpanne kommt es darauf an, schnell richtig zu reagieren.

Fördern Sie richtiges Verhalten bei Datenpannen

Wo Menschen arbeiten, kann auch etwas schiefgehen. Doch im Datenschutz können solche Pannen schnell zum großen Problem werden, etwa für Betroffene, aber auch für Ihr Unternehmen. Und wenn es dann doch passiert ist, muss richtig reagiert werden. Hier spielen die Führungskräfte eine wichtige Rolle.

Sensibilisieren Sie Vorgesetzte

Im Fall der Fälle, sprich bei einer Datenpanne, sollte nichts dem Zufall überlassen bleiben. Denn dann wird alles meist nur noch schlimmer, weil unvorbereitete Mitarbeiter eventuell kopflos reagieren. Um dem vorzubeugen, sollten Sie für Sensibilität sorgen. Schärfen Sie das Bewusstsein bei den Führungskräften. Denn diese treffen im Ernstfall Entscheidungen oder sind Anlaufstelle für die Mitarbeiter. Umso wichtiger ist, dass Vorgesetzte, wissen, worauf es ankommt. Geben Sie die richtigen Tipps.

Muster: Awarenessinfo für Führungskräfte zu Datenpannen

Liebe Kolleginnen und Kollegen mit Führungsverantwortung,

in unserem Unternehmen arbeiten wir alle täglich mit personenbezogenen Daten – von Kunden, Interessenten, Geschäftspartnern oder Beschäftigten. Diese Daten sind von großem Wert und wir müssen sie unbedingt schützen. Geraten sie in falsche Hände, kann das zum ernsten Problem für die Betroffenen, aber auch für unser Unternehmen werden.

Die Bedrohungslage ist real

Nicht nur das Bundesamt für Sicherheit in der Informationstechnik hat in seinem letzten Lagebericht festgestellt: Die Bedrohungen durch Hackerangriffe, Phishing und Ransomware-Aktionen sind hoch und nehmen weiter zu. Auch für unser Unternehmen kann niemand ausschließen, dass es irgendwann Opfer einer solchen Attacke wird. Geraten dann personenbezogene Daten in falsche Hände, haben wir eine ernst zu nehmende Datenschutzverletzung. Allerdings kann die auch ohne kriminelles Zutun passieren. Schon falsch versendete E-Mail-Anhänge oder ein falsch konfigurierter Server können schnell zu einer gravierenden Datenpanne führen.

Datenpannen haben es in sich

Sind personenbezogene Daten auf Abwegen, etwa weil Hacker Erfolg hatten, liegt regelmäßig eine Verletzung des Schutzes personenbezogener Daten vor. Das bedeutet für unser Unternehmen: Wir müssen nicht nur schnell handeln, um den Schaden für Betroffene und unser Unternehmen zu begrenzen. Unter Umständen müssen wir die Sache der zuständigen Datenschutzaufsichtsbehörde melden, und zwar unverzüglich bzw. spätestens binnen 72 Stunden. Zudem kann es bei besonders hohem Risiko für die Betroffenen erforderlich sein, dass wir auch die Betroffenen selbst informieren. Nehmen wir es mit dem Ganzen nicht so genau, kann es für unser Unternehmen richtig teuer werden. Der Gesetzgeber lässt Bußgelder in Millionenhöhe zu.

Sie sind als Führungskraft gefragt

Als Führungskraft tragen Sie nicht nur Verantwortung für den geschäftlichen Erfolg Ihres Bereichs oder Ihrer Abteilung. Sie führen Ihre Mitarbeiter und tragen zudem Verantwortung für die Verarbeitungen personenbezogener Daten in Ihrem Zuständigkeitsbereich. Zudem agieren Sie als Führungspersönlichkeit mit Ihrem Handeln und Ihren Entscheidungen als Vorbild. Umso wichtiger ist, dass Sie selbst Datenschutz leben und Ihren Mitarbeitern Orientierung geben. Das kann im Ernstfall der entscheidende Faktor sein, damit schnell, professionell und richtig gehandelt wird.

So bekommen wir Datenpannen in den Griff

Datenschutz funktioniert nur, wenn alle an einem Strang ziehen. Das ist umso wichtiger, wenn es zu brenzligen Situationen kommt. Gerade im Fall von Datenpannen ist es wichtig, dass Sie und Ihre Mitarbeiter richtig reagieren. Damit Ihnen das leichter fällt, habe ich Ihnen einige Tipps zusammengestellt:

Ruhe bewahren

Ist eine Datenpanne passiert, ist der Schock erst einmal groß. Und dennoch ist wichtig: Vermeiden Sie Hektik und unüberlegtes Handeln. Vermeiden Sie Panik bei sich und Ihren Mitarbeitern. Schließlich ist Panik nie ein guter Berater. Schlimmstenfalls werden die falschen Entscheidungen getroffen. Und die können die Situation noch verschlimmern. Daher: Bewahren Sie einen kühlen Kopf. Beruhigen Sie auch Ihr Team. Handeln Sie lieber nach der Devise: Eile mit Weile. Gehen Sie ruhig und strukturiert vor. Treffen Sie alle Entscheidungen überlegt und mit Bedacht.

Stoppen Sie die Panne

Wurde eine Datenpanne erkannt oder liegen starke Indizien für eine solche vor, ist wichtig: Beenden Sie schnellstmöglich das Schadensereignis. Gibt es etwa ein Datenleck, fließen eventuell Daten so lange ab, wie es nicht gestopft ist. Handeln ist hier oberstes Gebot und abwarten ist keine Option. Sind Sie sich nicht sicher, was zu tun ist, holen Sie sich Rat von den Profis. Im Datenschutz steht Ihnen der Datenschutzbeauftragte zur Verfügung. Für alles rund um die IT sprechen Sie mit den Profis der IT-Abteilung.

Erfassen Sie schnell die Situation

Damit die zuständigen Stellen sich schnell einen Überblick verschaffen können, ist wichtig, dass Sie die erforderlichen Informationen liefern können. Am besten nutzen Sie strukturierte W-Fragen:

- Was ist konkret passiert?
- Wann ist es passiert?
- Wer hat was wann bemerkt?
- Wessen Daten sind betroffen?
- Welche Daten sind betroffen?
- Welches Ausmaß hat der Vorfall?
- Was wurde bereits unternommen?

Sofortige Meldung an den Datenschutzbeauftragten

Stellen Sie eine Panne fest oder vermuten Sie deren Vorliegen, müssen Sie schnellstens den Datenschutzbeauftragten informieren. Machen Sie das immer, wenn Daten im Spiel sind. Prüfen Sie nicht selbst, ob keine Datenschutzrelevanz besteht, weil die Daten nicht personenbezogenen sind. Hier steckt der Teufel oft im Detail. Gemeinsam mit dem Datenschutzbeauftragten wird auch geprüft, ob es sich um einen meldepflichtigen Vorfall handelt oder ob Betroffene zu informieren sind. Dabei ist jedoch wichtig: Warten ist keine Option. Es gelten strenge Meldefristen gegenüber der Datenschutzaufsichtsbehörde. Das sind bei Datenpannen grundsätzlich maximal 72 Stunden.

Schalten Sie die IT Abteilung unverzüglich ein

Datenpannen können rein technisch bedingt sein. Denken Sie beispielsweise an eine Fehlkonfiguration. Doch auch bei einem Hackerangriff oder einer Ramsomware-Attacke steht häufig das Technische im Mittelpunkt. Hier ist dann die IT-Abteilung mit ihren geschulten Spezialisten der wichtigste Akteur. Die Kollegen helfen nicht nur dabei die Schadensursache zu finden bzw. das Schadensereignis zu stoppen. Sie leiten auch alle nötigen Maßnahmen ein, um das Funktionieren der IT zu sichern oder wiederherzustellen.

Kehren Sie nichts unter den Teppich

Für manchen mag es verlockend sein. Doch es ist keine gute Idee, einen Vorfall kleinzureden oder zu vertuschen. Auch mögliche Gefahren für Betroffene oder unser Unternehmen zu banalisieren ist schlecht. Darauf zu vertrauen, dass niemand etwas mitbekommen wird, kann ebenfalls richtig schiefgehen. Deshalb ist wichtig: Gehen Sie offen damit um, dass etwas passiert ist. Sie müssen sich hier weder schämen noch ernste Konsequenzen fürchten. Ganz im Gegenteil: Die Konsequenzen drohen gerade dann, wenn Sie schnelle Hilfe vereiteln oder dieser im Weg stehen.

Etablieren Sie eine positive Fehlerkultur

Es liegt nicht nur an Ihnen, ob im Fall der Fälle richtig gehandelt wird. Genauso entscheidend sind Ihre Mitarbeiter. Doch die dürfen keine Angst vor Konsequenzen haben, wenn sie Ihnen Auffälligkeiten oder gemachte Fehler melden. Vermitteln Sie Ihren Mitarbeitern zudem: Wer Vorfälle meldet, handelt genau richtig. Und das verdient die Anerkennung aller. Wer hingegen die Augen verschließt und schweigt, der gefährdet das ganze Unternehmen.

Dokumentieren Sie lückenlos

Auch wenn Sie etwa technische Probleme selbst lösen oder die durch einen Hackerangriff verursachte Datenpanne beheben können, gilt: Sichern Sie aussagekräftige Beweise, bevor Sie sich ans Arbeiten und Reparieren machen. Fragen Sie im Zweifel vorab bei IT-Abteilung und Datenschutzbeauftragtem nach. Schließlich können Beweise unerlässlich sein, wenn die Sache strafrechtlich verfolgt werden soll oder wenn es um eine Schadensregulierung durch eine Versicherung geht.

Sorgen Sie für Awareness

Viele Datenpannen beginnen mit einem einfachen Klick, und zwar auf einen Link oder einen Anhang einer Phishing-E-Mail. Sind die sensiblen Zugangsdaten erst einmal eingegeben, ist es häufig schnell zu spät. Die Kriminellen haben Zugriff und nehmen sich alles an Daten, was nicht niet- und nagelfest ist. Als Führungskraft können auch Sie viel dazu beitragen, dass es nicht zu solchen Vorfällen kommt. Sensibilisieren Sie Ihre Mitarbeiter immer wieder für Phishing-Angriffe. Besprechen Sie gemeinsam in einem Meeting, worauf zu achten ist, wie man sich richtig verhält und was zu tun ist, wenn etwas schiefgegangen ist.

Ich danke Ihnen für Ihre Unterstützung!

Ihr Ben Jamin

Betrieblicher Datenschutzbeauftragter

Schnelle Erstberatung gefällig? Setzen Sie auf diese Checkliste

Jeder Datenschutzbeauftragte kennt das: Da kommt ein unerwarteter Anruf oder man wird spontan auf eine neue Verarbeitung personenbezogener Daten angesprochen. Von Ihnen will man wissen, worauf es ankommt und was gerade unter Datenschutzaspekten von Bedeutung ist. Ratlos die Schultern zucken wäre jetzt die schlechteste Reaktion Ihrerseits. Denn schnell auf wichtige Punkte hinweisen können Sie immer.

Arbeiten Sie mit den Grundsätzen

Die Grundsätze der Verarbeitung in Art. 5 Datenschutz-Grundverordnung (DSGVO) sind Ihr Schweizer Messer, wenn es um Erstberatungen in Datenschutzfragen geht. Warum? Das ist schnell erklärt: Einerseits gelten die Grundsätze für alle Verarbeitungen personenbezogener Daten. Andererseits geht grundsätzlich alles Geregelte in der DSGVO auf die Grundsätze zurück bzw. gestaltet diese aus. Zudem kann ein Verstoß gegen die Grundsätze ziemlich teuer werden. Nutzen Sie also die folgende Checkliste, um den Kollegen die Grundsätze schnell zu erklären. Zudem können Sie mit Fragen aufzeigen, worauf es ankommt.

Checkliste: Datenschutzgrundsätze in der Erstberatung

Grundsatz	Das steckt dahinter	Typische Fragen
Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 Buchst. a DSGVO)	› Personenbezogene Daten dürfen nur verarbeitet werden, wenn es dafür eine Rechtsgrundlage gibt. Diese ergibt sich aus Art. 6 DSGVO, etwa zur Vertragserfüllung, Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung eines berechtigten Interesses oder auf Basis der Einwilligung. › Fehlt eine Rechtsgrundlage oder sind einzelne Voraussetzungen nicht erfüllt, ist die Verarbeitung unzulässig und muss unterbleiben.	› Auf welche Rechtsgrundlage wird die Verarbeitung gestützt? › Sind alle Voraussetzungen der Rechtsgrundlage erfüllt? › Sind die Rahmenbedingungen dokumentiert? › Sind bei Einwilligungen alle Anforderungen erfüllt (z. B. Art. 7, 8, 4 Nr. 11 DSGVO)?
Transparenz sowie Treu und Glauben (Art. 5 Abs. 1 Buchst. a DSGVO)	› Betroffene müssen schon bei der Erhebung der Daten wissen und absehen können, was mit ihren personenbezogenen Daten passiert. Es muss insbesondere transparent über relevante Rahmenbedingungen (z. B. Zwecke, Empfänger) informiert werden. › „Treu und Glauben" zielt darauf ab, dass die Verarbeitung fair gestaltet ist. Betroffene dürfen nicht getäuscht oder in die Irre geführt werden, etwa durch versteckte Klauseln oder ungünstige Voreinstellungen.	› Was wird zur Gewährleistung der Transparenz unternommen? › Wie, wann und in welchem Umfang wird der Betroffene über die Rahmenbedingungen informiert? › Wie wurden die Interessen der Betroffenen bei der Gestaltung der Verarbeitung berücksichtigt?
Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO)	› Grundsätzlich dürfen Daten nur für den Zweck verarbeitet werden, für den sie erhoben wurden. › Das Weiterverarbeiten für andere Zwecke ist nur unter besonderen Voraussetzungen zulässig, etwa auf Basis von Art. 6 Abs. 4 DSGVO. Hier muss z. B. der neue Zweck zum ursprünglichen kompatibel sein.	› Wurde der Zweck konkret festgelegt und dokumentiert? › Wie wird die Zweckbindung sichergestellt? › Kommt es zur Weiterverarbeitung der Daten für andere Zwecke? › Was passiert, wenn der Zweck erfüllt ist?
Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO)	› Der sparsame Umgang mit personenbezogenen Daten ist Datenschutzstandard. Hier gilt die Faustformel „So wenig wie möglich, so viel wie unbedingt erforderlich". › Nicht erforderliche Daten sind immer problematisch. Eventuell bedarf es einer spezifischen Rechtsgrundlage wie z. B. einer Einwilligung des Betroffenen.	› Welche Daten werden erhoben und sind diese für den Zweck erheblich und notwendig? › Ist das Minimalprinzip schon bei der Datenerfassung berücksichtigt? › Werden Datenbestände hinsichtlich ihrer Notwendigkeit überprüft?
Richtigkeit der Daten (Art. 5 Abs. 1 Buchst. d DSGVO)	› Falsche und veraltete personenbezogene Daten sind ein Problem. Sie können auch für Betroffene ein erhöhtes Schadensrisiko bergen. › Ggf. müssen unrichtige oder veraltete Daten korrigiert oder gelöscht werden (Art. 16 und 17 DSGVO).	› Welche Prozesse sind vorgesehen, um die Richtigkeit und Aktualität von Daten zu gewährleisten? › Inwieweit können entsprechende Ansprüche von Betroffenen umgesetzt werden?
Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO)	› Prinzipiell gilt: Personenbezogene Daten dürfen nur so lange verarbeitet werden, wie das für den Verarbeitungszweck erforderlich ist. › Ausnahmsweise darf nicht gelöscht werden, etwa wenn entsprechende Speicherpflichten bestehen.	› Welche Speicher- und Löschfristen sind für die verarbeiteten Daten vorgesehen? › Worauf basieren die entsprechenden Festlegungen? › Wie wird eine entsprechende Betroffenenanfrage geprüft und umgesetzt?
Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO)	› Dieser Grundsatz zielt darauf ab, angemessenen Schutz vor unbefugtem Zugriff, vor Verlust, Vernichtung oder Veränderung sicherzustellen. › Die wichtigsten Rahmenbedingungen ergeben sich aus Art. 32 DSGVO. Danach sind risikoangemessene Schutzmaßnahmen umzusetzen.	› Mit welchen Schutzmaßnahmen werden die Ziele aus Art. 32 DSGVO erreicht? › Sind die Maßnahmen risikoangemessen? › Sind die Maßnahmen auf der Höhe der Zeit und entsprechen sie dem Stand der Technik?

Führerscheinkontrolle: Prüfen Sie, ob alles passt

Vielleicht gibt es ihn auch in Ihrem Unternehmen: den Außendienst, der etwa für Lieferungen, das Erbringen von Dienstleistungen oder für die Fahrt zum Kunden ein Fahrzeug des Unternehmens nutzt. Eventuell gibt es auch Beschäftigte mit Geschäftswagen. Bei allen ist gleich: Die dürfen nur genutzt werden, wenn der Fahrer eine Fahrerlaubnis hat. Und die muss Ihr Unternehmen prüfen.

Darum muss Ihr Unternehmen kontrollieren

Einfach mal die Mitarbeiter mit dem Firmenwagen oder dem unternehmenseigenen Klein-Lkw von A nach B fahren lassen und darauf vertrauen, dass der Mitarbeiter die nötige Fahrerlaubnis besitzt, ist nicht zu empfehlen. Das hat verschiedene Gründe: Einer ist § 21 Abs. 1 Straßenverkehrsgesetz. Danach können sowohl Fahrer als auch Halter eines Fahrzeugs zur Verantwortung gezogen werden, wenn die erforderliche Fahrerlaubnis fehlt. Weiterer Grund: Passiert etwas, kann das Ärger und hohe Kosten mit sich bringen. Unter Umständen kann eine Versicherung die Regulierung des Schadens ganz oder teilweise verweigern.

Vieles kann im Datenschutz schiefgehen

Bei der Kontrolle der Fahrerlaubnis heißt es genau hinschauen und nicht selten steckt der Teufel im Detail. Einige Beispiele für typische Stolperfallen gefällig? Nehmen Sie einfach nur einige Grundsätze der Verarbeitung personenbezogener Daten:

- **Rechtmäßigkeit und Transparenz:** Ohne Rechtsgrundlage keine Verarbeitung. Eventuell sind einzelne Voraussetzungen nicht erfüllt, etwa hapert es mit der Erforderlichkeit. Unter Umständen fehlt es an der Nachvollziehbarkeit für den Betroffenen, etwa an den nötigen Informationen nach Art. 13 Datenschutz-Grundverordnung (DSGVO).
- **Datenminimierung:** Das Minimalprinzip wird bei Kontrollen der Fahrerlaubnis oft missachtet. So bedarf es regelmäßig keiner Kopie des Führerscheins. Selbst wenn man diese für nötig erachtet, dürfen viele enthaltene Informationen nicht verarbeitet werden. Schwärzen nicht notwendiger Informationen ist ein Muss.
- **Speicherbegrenzung:** Sind Mitarbeiter ausgeschieden, müssen auch die Kontrollinformationen gelöscht werden. Zwar muss das nicht sofort passieren, weil für den Nachweis auch noch nach dem Ausscheiden Relevanz besteht. Wird jedoch bei einer Wiederholungsüberprüfung (z. B. alle sechs Monate) festgestellt, dass die Person nicht mehr Mitarbeiter ist, können die entsprechenden Nachweisinformationen gelöscht werden.

Prüfen Sie, was Sache ist

Läuft etwas im Datenschutz schief, sollte das schleunigst geändert werden. Um Problematischem auf die Spur zu kommen, können Sie die nachfolgende Checkliste einsetzen. Die kann Sie einerseits bei einer Datenschutzkontrolle, sprich bei einem Audit, unterstützen. Andererseits können Sie die Checkliste bei einem Gespräch mit den zuständigen Kollegen, etwa aus der Personalabteilung oder dem Fuhrparkmanagement, nutzen.

Checkliste: Führerscheinkontrolle und Datenschutz

Aspekt	Hintergrund	Geprüft und in Ordnung?
Welche Regelungen und Zuständigkeiten gibt es im Unternehmen?	› Beschaffen Sie sich entsprechende Regelwerke und Arbeitsanweisungen. › Machen Sie eine erste Bestandsaufnahme insbesondere im Hinblick auf Regelungsinhalt, Vollständigkeit und Aktualität. › Klären Sie einerseits, wer den Prozess an sich verantwortet. Das kann etwa ein Fuhrparkmanagement, die Personalabteilung oder manchmal auch das Facility Management sein. Prüfen Sie, wer die Prüfung und Dokumentation der Prüfung konkret durchführt.	○ Ja ○ Nein
Ist eine entsprechende Verarbeitungstätigkeit im Verzeichnis nach Art. 30 Abs. 1 DSGVO enthalten?	› Im Verzeichnis nach Art. 30 Abs. 1 DSGVO müssen alle Verarbeitungstätigkeiten enthalten sein, die Ihr Unternehmen verantwortet. › Eventuell sind die Führerscheinkontrolle und Dokumentation Teil einer anderen Verarbeitungstätigkeit oder eines Verarbeitungsprozesses. Manchmal können Sie auch unter „Fuhrparkmanagement“ oder „Geschäftswagenleasing“ fündig werden. › Machen Sie bezüglich der Angaben einen Aktualitäts- und Vollständigkeitscheck.	○ Ja ○ Nein
Auf welche Rechtsgrundlage wird die Verarbeitung „Führerscheinkontrolle“ gestützt?	› Es sind grundsätzlich mehrere Rechtsgrundlagen denkbar. So z. B., um den (Arbeits-)Vertrag mit dem Beschäftigten durchzuführen (Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO). Möglich ist auch, die Kontrolle auf ein überwiegendes berechtigtes Interesse (Vermeidung von versicherungs- und strafrechtlicher Haftung) zu stützen (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO). › Beruft man sich auf ein „überwiegendes berechtigtes Interesse“, lassen Sie sich die erforderliche Interessenabwägung zeigen. Hier müssen viele Interessen berücksichtigt sein, etwa auch, dass nur unbedingt erforderliche persönliche Informationen erfasst und verarbeitet werden.	○ Ja ○ Nein

Wie wird bei den betroffenen Mitarbeitern für die nötige Transparenz gesorgt?	› Für Betroffene muss nachvollziehbar sein, was mit ihren personenbezogenen Informationen passiert. Die nötigen Informationen ergeben sich aus Art. 13 DSGVO. › Gibt es eine generelle Information zur Verarbeitung von Beschäftigtendaten, sollten Sie prüfen, ob das Thema „Führerscheinkontrolle" abgedeckt ist.	○ Ja ○ Nein
Was wird konkret im Zusammenhang mit einer Fahrerlaubnis dokumentiert?	› Lassen Sie sich erläutern, wie der Prozess funktioniert, und zwar von Anfang bis Ende. Spielen Sie einfach das Ganze an einem fiktiven Beispiel durch. › Schauen Sie sich vorhandene Dokumentationen an. In der Regel reicht eine Stichprobe aus. Stellen Sie hier jedoch Defizite fest, heißt es: genauer hinschauen!	○ Ja ○ Nein
Werden Kopien von Führerscheinen erstellt und abgelegt?	› Stellen Sie hier sofort die Frage nach dem Warum. Regelmäßig dürften Kopien an sich nicht erforderlich sein. Die Vorlage eines amtlichen Führerscheins, die Prüfung relevanter Merkmale und Angaben sowie das Festhalten der Prüfung an sich reichen aus. › Räumt man ein, dass es Kopien gibt, sollten Sie sich diese konkret anschauen. Dabei kann man Ihnen das nicht verweigern. Schließlich sind von Ihrem Kontrollauftrag alle personenbezogenen Informationen im Unternehmen erfasst.	○ Ja ○ Nein
Inwieweit ist bei Kopien das Minimalprinzip umgesetzt?	› Führerscheine können auch Sensibles enthalten (z. B. gesundheitliche Einschränkungen). Auch viele andere Informationen sind für eine Prüfung bzw. Dokumentation nicht erforderlich, etwa Foto und Unterschrift. Ihr Unternehmen muss nur prüfen, ob eine gültige Fahrerlaubnis besteht. › Wurden Schwärzungen gemacht, halten Sie die Kopie ins Licht. Können Sie das Geschwärzte lesen, ist die Schwärzung quasi nicht existent.	○ Ja ○ Nein
Kommen spezielle Softwarelösungen oder Kontrolleinrichtungen zum Einsatz?	› Eventuell wird spezielle Software zur Durchführung und Dokumentation der Kontrollen eingesetzt. Schauen Sie hier in Sachen Datenschutz genauer hin. › Vielleicht setzt man auch auf eine gewisse Automatisierung, etwa mit RFID-Aufklebern auf den Führerscheinen. Steht eine Kontrolle an, muss der Führerschein mit Aufkleber an ein Lesegerät gehalten werden. Bei solchen Verarbeitungen können im Hintergrund viele Daten verarbeitet werden. Lassen Sie sich die Sache konkret erklären. › Wird spezielle Software eingesetzt, sollten Sie auch ein Augenmerk auf Art. 25 DSGVO haben. Schon bei der Konzeption der Verarbeitung waren die datenschutzrechtlichen Rahmenbedingungen zu berücksichtigen. Ihr Stichwort: „Datenschutz durch Technikgestaltung und Voreinstellungen".	○ Ja ○ Nein
Inwieweit liegt eine einschlägige Betriebsvereinbarung vor?	› Gerade wenn Software eingesetzt wird, kann ein Mitbestimmungsrecht des Betriebsrats bestehen. So z. B. für technische Einrichtungen, mit denen die Beurteilung der Leistung und des Verhaltens von Arbeitnehmern möglich ist. › Schauen Sie unbedingt in die Betriebsvereinbarung. Nicht selten finden sich dort Aspekte, die für den Datenschutz und Ihre Prüfung von Relevanz sind. Denken Sie insbesondere an Zugriffsberechtigungen.	○ Ja ○ Nein
Welche Schutzmaßnahmen wurden im Hinblick auf Art. 32 DSGVO umgesetzt?	› Bitten Sie um die Vorlage eines entsprechenden Dokuments oder Sicherheitskonzepts für die Verarbeitung. › Prüfen Sie, inwieweit es tatsächlich eine Risikoanalyse gibt. Die ist nämlich Ausgangspunkt für die Festlegung risikoangemessener technischer und organisatorischer Schutzmaßnahmen. › Machen Sie zumindest eine stichprobenhafte Prüfung, ob Sie in einem Konzept festgelegte Maßnahmen auch tatsächlich umgesetzt vorfinden. Nicht selten tritt so zutage, dass Maßnahmen nicht oder nicht wie vorgesehen umgesetzt werden.	○ Ja ○ Nein
Inwieweit werden Dienstleister eingesetzt?	› Vielleicht setzt man auf Services anderer Anbieter, etwa eine App-Lösung oder Webanwendung. Das entlässt Ihr Unternehmen jedoch nicht aus seiner datenschutzrechtlichen Verantwortung für die verarbeiteten personenbezogenen Daten. › Prüfen Sie Aussagen zum Datenschutz kritisch. Nur weil ein „DSGVO-konform" werbewirksam präsentiert wird, darf dem nicht allzu viel Bedeutung beigemessen werden. › Regelmäßig dürfte ein Fall der Auftragsverarbeitung (Art. 28 DSGVO) vorliegen. Nehmen Sie den Vertrag genauer unter die Lupe. Prüfen Sie vor allem die vereinbarten Schutzmaßnahmen.	○ Ja ○ Nein
Ist die Umsetzung der Rechte der Betroffenen sichergestellt?	› Ihr Unternehmen muss die Betroffenenrechte (z. B. Auskunft, Löschung) für alle personenbezogenen Daten bzw. für alle Verarbeitungen umsetzen können. Das gilt auch für Verarbeitungen, die eher unscheinbar sind oder die mit Papier und Bleistift durchgeführt werden. › Prüfen Sie, inwieweit auch der Prozess und die Dokumentation der Kontrolle von Führerscheinen etwa bei der Suche nach relevanten Fundorten für personenbezogene Daten erfasst sind.	○ Ja ○ Nein
Wann werden die Informationen zur Kontrolle eines Führerscheins gelöscht?	› Hinterfragen Sie die vorgesehenen Löschfristen für Informationen rund um die Führerscheinkontrolle. Ist etwa eine halbjährliche Kontrolle der Führerscheine vorgesehen, fehlt es mit erneuter Durchführung einer Kontrolle am Dokumentationsinteresse bezüglich vorheriger Prüfungen. › Haben Sie auch ein Auge auf Ablagen oder Personalakten. Unter Umständen finden sich dort nicht mehr relevante Informationen. Diese müssen nach Art. 17 Abs. 1 Buchst. a DSGVO gelöscht werden.	○ Ja ○ Nein
Inwieweit sind kontrollierende Personen für wichtige Rahmenbedingungen sensibilisiert?	› Regelungen sind eine Sache. Eine ganz andere ist, ob sie auch tatsächlich befolgt werden. Machen Sie sich bei den zuständigen Personen und deren Vorgehen bei Kontrollen ein Bild. › Lassen Sie sich schildern, wie kontrollierende Personen für alles Wichtige sensibilisiert werden. Das ist besonders wichtig, wenn die Pflicht zur Kontrolle nicht zentralisiert ist und etwa von Vorgesetzten übernommen wird. › Gibt es Merkblätter oder Schulungsunterlagen, sollten Sie prüfen, inwieweit Datenschutzaspekte berücksichtigt sind.	○ Ja ○ Nein
Was passiert, wenn Mitarbeiter das Unternehmen verlassen?	› Spätestens bei einer Aktualisierungskontrolle sollte geprüft werden, ob Mitarbeiter nicht mehr im Unternehmen sind bzw. entsprechende Fahrzeuge nicht mehr nutzen dürfen. In beiden Fällen entfallen das Interesse und die Berechtigung, den Nachweis einer Fahrerlaubnis zu dokumentieren. › Machen Sie die Probe aufs Exempel und prüfen Sie, ob Sie Informationen zu Ehemaligen finden.	○ Ja ○ Nein

Mit diesen 7 Tipps arbeiten Sie sofort zielorientierter

Wer wenig Zeit für seine Aufgaben als Datenschutzbeauftragter zur Verfügung hat, der kann ein Lied davon singen: Oft kommt vieles zu kurz, manchmal verzetteln man sich bei der Erledigung selbst einfacher Aufgaben und hier und da wächst einem manches über den Kopf. Das Ruder können Sie herumreißen. Arbeiten Sie strikt ziel- und ergebnisorientiert.

Diese 7 Tipps helfen garantiert

Sie fragen sich, wie Sie denn bloß zielorientierter arbeiten könnten? Das Grübeln können Sie sich sparen. Die folgenden sieben Tipps tragen ganz automatisch dazu bei, dass Ziel- und Ergebnisorientierung steigen:

1. Fragen Sie Löcher in den Bauch

Um zielorientiert arbeiten und vor allem beraten zu können, brauchen Sie viele Informationen. Trauen Sie sich also, schon im Vorfeld von Besprechungen Fragen zu stellen und Informationen einzufordern. Damit steigern Sie nicht nur Ihre eigene Effizienz, weil Sie sich besser vorbereiten können. Sie zwingen auch andere dazu, sich mit vielen Aspekten aktiv auseinanderzusetzen. Und manchmal passiert Folgendes: Der Termin wird verschoben, weil man erst einmal die eigenen Hausaufgaben erledigen muss. Also sparen Sie sich die Zeit für einen nicht zielführenden Termin.

2. Arbeiten Sie nach Plan

Idealerweise haben Sie für Ihre Arbeit als Datenschutzbeauftragter einen Fahrplan fürs komplette Jahr. Ist Ihnen klar, was Sie umsetzen wollen oder angehen müssen, fällt es leichter, das rechtzeitig in Angriff zu nehmen. Außerdem können Sie besser Prioritäten setzen, wenn etwas Unvorhergesehenes eintritt. Dabei ist klar: Sie müssen keinen komplexen Plan erstellen. Schon eine einfache Tabelle mit Themen kann ausreichen. Bewerten Sie diese unter Prioritätsgesichtspunkten und vergeben Sie einen realistischen Erledigungstermin. Überprüfen Sie regelmäßig den Stand der Dinge und passen Sie Ihre Liste bei Bedarf an.

3. Setzen Sie risikobasiert Schwerpunkte

Ihre Aufgaben als Datenschutzbeauftragter ergeben sich grundsätzlich aus Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Im Wesentlichen beraten Sie in allen Fragen des Datenschutzes und kontrollieren dessen Umsetzung. Und dabei fordert der Gesetzgeber von Ihnen in Art. 39 Abs. 2 DSGVO: Gehen Sie risikoorientiert vor. Schließlich sind Ihre Beratung und Ihre Kontrollen dort am nötigsten, wo die größten Risiken lauern.

Eine wichtige Maßnahme zur entsprechenden Schwerpunktsetzung ist folgende: Bei jeder neuen Beratung oder Kontrollidee Ihrerseits machen Sie eine kurze Risikobewertung. Betrachten Sie die Schutzwürdigkeit der Daten, das Schadenspotenzial und die Eintrittswahrscheinlichkeit. Setzen Sie mit Ihrer Tätigkeit dann dort an, wo das Risikopotenzial am größten ist.

4. Nutzen Sie To-do-Listen zur Steuerung

Egal, ob Sie diese auf Tages-, Wochen- oder Monatsebene führen: Aufgabenlisten, neudeutsch To-do-Listen, sollten Sie zu einem Ihrer wichtigsten Hilfsmittel machen. Notieren Sie alle offenen Aufgaben an einem zentralen Ort. Dazu können Sie beispielsweise Bordmittel Ihres Computers, des E-Mail-Programms oder Smartphones nutzen und entsprechende Listen verwalten. Aber es gibt auch Alternativen, damit Sie alles Relevante am Arbeitsplatz immer direkt vor Augen haben: Arbeiten Sie mit Klebezetteln. Erstellen Sie sich an der Wand vor dem Schreibtisch verschiedene „Klebezonen", etwa mit „Wichtig und dringend" oder „Diese Woche erledigen". Kleben Sie dann Ihr To-do in die passende Zone.

5. Vergessen Sie Multitasking

Deutsche Forscher wollen kürzlich herausgefunden haben: Das menschliche Gehirn ist einfach nicht für Multitasking gemacht, sprich eben nicht für das gleichzeitige Abarbeiten mehrerer Aufgaben. Und wer ehrlich zu sich ist, kann die Erkenntnis nur bestätigen. Wird parallel an mehreren Dingen gearbeitet, kommt meist nichts Gutes dabei heraus. Es passieren Fehler oder die Qualität leidet erheblich. Und das wäre gerade in Ihrem Job als Datenschutzbeauftragter ein großes Problem. Schließlich hängt von Ihrer Expertise und Ihrer Einschätzung oft viel ab.

Daher: Arbeiten Sie nach Möglichkeit konzentriert eine Sache nach der anderen ab. Ist das nicht möglich, sollten Sie zumindest versuchen, saubere Schnitte zu machen und Teilergebnisse zu sichern. Dann können Sie später auf einer soliden Basis neu einsteigen.

6. Lernen Sie, Nein zu sagen

Auch das ist wichtig: Sie müssen Ihre Aufgabenwahrnehmung und die diesbezügliche Qualität sichern und manches ablehnen. Akzeptieren Sie vor allem kein „Das macht der schon", wenn man Ihnen Arbeit über den Zaun wirft. Sagen Sie in solchen Fällen professionell Nein. Erklären Sie, warum Sie sich nicht um eine Sache kümmern können. Und sind Sie nicht zuständig, spielen Sie den Ball sofort zurück.

7. Schärfen Sie Ihr Rollenbewusstsein

Machen Sie sich immer klar: Sie beraten und kontrollieren. Zum Entscheiden und Umsetzen sind andere berufen. Führen Sie sich immer wieder vor Augen, was zu Ihrer Rolle und Ihren Aufgaben zählt. Damit vermeiden Sie unnötige Aufwände und können sich mehr auf Ihre Ziele konzentrieren.

Muss ich für das Einhalten der Betriebsvereinbarung sorgen?

FRAGE: Bei uns wurde zwischen Arbeitgeber und Gesamtbetriebsrat eine Rahmenvereinbarung zum Datenschutz geschlossen. Anscheinend ist man nun der Ansicht, dass ich als Datenschutzbeauftragter die Umsetzung der Betriebsvereinbarung in Angriff nehme. Ich frage mich aber: Muss ich für die Einhaltung sorgen?

ANTWORT: Zunächst ist wichtig, dass Sie sich Grundsätzliches in Bezug auf kollektivrechtliche Vereinbarungen zwischen Arbeitgeber und Betriebsrat, etwa Betriebsvereinbarungen, vor Augen führen. Solche Vereinbarungen dokumentieren die Regelung einer Situation, etwa aufgrund des Mitbestimmungsrechts aus § 87 Abs. 1 Betriebsverfassungsgesetz (BetrVG). Wer diese Vereinbarungen umsetzen muss, ergibt sich konkret aus § 77 Abs. 1 BetrVG. So ist es grundsätzlich Sache des Arbeitgebers, die gemeinsamen Vereinbarungen umsetzen. Das gilt nur dann nicht, wenn im Einzelfall etwas anderes vereinbart ist.

Sie sind weder Arbeitgeber noch Verantwortlicher

Fakt ist: Sie sind nicht der Arbeitgeber und damit in kollektivrechtlicher Sicht nicht der Kopf des Unternehmens. Auch sind Sie nicht als Verantwortlicher im datenschutzrechtlichen Sinne anzusehen. Denn dieser entscheidet über die Zwecke und Mittel der Verarbeitung. Und genau das dürfen Sie als Datenschutzbeauftragter nicht übernehmen. Schon wenn Sie Teilfunktionen des Verantwortlichen erfüllen, kann das dazu führen, dass Sie Ihre Aufgaben aus Art. 39 Abs. 1 DSGVO nicht unabhängig wahrnehmen können. Interessenkonflikte darf es nach Art. 38 Abs. 6 Satz 2 DSGVO nicht geben.

Prüfen Sie, was konkret in der Vereinbarung steht

Bevor Sie über einen eventuell unzulässigen Eingriff in Ihre Funktion und Aufgaben als Datenschutzbeauftragter mit Arbeitgeber und Betriebsrat sprechen, ist eines wichtig: Schauen Sie sich die Betriebsvereinbarung konkret an. Prüfen Sie, was wirklich geregelt ist und inwieweit das tatsächlich Beeinträchtigungen für Sie mit sich bringt. Unter Umständen werden nämlich nur Aspekte zur Datenschutzorganisation geregelt. Vielleicht hat auch manches nur formellen Charakter, weil im Wesentlichen nur das wiederholt wird, was die gesetzlichen Rahmenbedingungen ohnehin vorsehen. Halten Sie etwas für problematisch, kann eine zweite Meinung hilfreich sein.

Suchen Sie das Gespräch

Stellen Sie fest, dass die Betriebsvereinbarung Sie und Ihre Arbeit unzulässig beeinträchtigt oder Ihnen Vorgaben gemacht werden, sollten Sie das Gespräch mit Arbeitgeber und Betriebsrat suchen. Diskutieren Sie die problematischen Passagen. Fordern Sie, dass es Anpassungen gibt oder zumindest die Betriebsvereinbarung um klarstellende Protokollnotizen ergänzt wird.

Was kann ich tun, wenn meine Weiterbildung verweigert wird?

FRAGE: Als Datenschutzbeauftragter habe ich regelmäßig Schulungen besucht, um mein Fachwissen auf dem Laufenden zu halten. Der neue Geschäftsführer hat jedoch ein generelles Sparprogramm ausgerufen. Dem ist nun auch meine Weiterbildung zum Opfer gefallen. Was kann ich nun bezüglich der verweigerten Weiterbildung unternehmen? Kann ich die irgendwie erzwingen?

ANTWORT: Erzwingen können Sie Ihre Weiterbildung nicht. Allerdings sollten Sie eventuell erneut das Gespräch suchen. Machen Sie sich für das Gespräch zum Ziel, Folgendes zu klären:

- **Welche Gründe haben zur Ablehnung geführt?** Sparzwänge sind als Grund sehr allgemein. Klären Sie, ob es an den Teilnahmegebühren, den Reise- und Übernachtungskosten oder an beidem lag. Das eröffnet Ihnen die Möglichkeit, hier neue Varianten ins Spiel zu bringen. Sind etwa Hotelkosten am Veranstaltungsort das Problem, können Sie ggf. eine kostenfreie Übernachtung bei Freunden vorschlagen.
- **Welche genehmigungsfähigen Möglichkeiten gibt es?** Sind Reisen nicht drin, können Sie an der Veranstaltung vielleicht auch virtuell teilnehmen. Das spart Kosten. Sind die Teilnahmekosten zu hoch, können Sie mit dem Veranstalter sprechen. Ggf. sind Rabatte drin, auch wenn die nirgendwo stehen.
- **Welche Alternativen kommen in Betracht?** Qualifikation und Know-how kann es auch kostengünstig geben. So können Sie sich selbst weiterbilden. Studieren Sie beispielsweise Leitfäden von Aufsichtsbehörden. Selbst mit neuen Fachbüchern können Sie sich viel neues Wissen aneignen. Auch kann es kostenfreie Veranstaltungen von Behörden geben.

VG Düsseldorf: Auskunft hat Vorrang vor Datenlöschung

Machen Betroffene Rechte nach der Datenschutz-Grundverordnung (DSGVO) geltend, kann das für Verantwortliche viel Aufwand bedeuten. Kein Wunder, dass mancher daran denkt, bei einer Anfrage vorhandene Daten zu löschen, um nichts mehr beauskunften zu können. So geht das nicht, meint das Verwaltungsgericht (VG) Düsseldorf in seiner Entscheidung vom 21.1.2026 (Az. 29 K 7470/24).

Der Sachverhalt

Eine Agentur, die spätere Klägerin, führte Werbekampagnen per E-Mail tätig. So führte die Agentur am 26.8.2022 eine Aktion durch, bei der auch ein Mann eine E-Mail erhielt. Dieser wandte sich an die Agentur. Er forderte die Agentur unter anderem auf, ihm mitzuteilen, woher die Agentur seine personenbezogenen Daten hätte.

Agentur reagiert nicht

Die Zeit verging, doch die Agentur reagierte zunächst nicht auf die Anfrage des E-Mail-Empfängers. Also erinnerte der Mann am 26.9.2022 die Agentur an sein Auskunftsersuchen. Am 29.9.2022 erhielt der Mann Antwort. Die Agentur übersandte ihm eine Datenschutzauskunft, und zwar ein 15-seitiges Dokument, das die Dokumentation eines Gewinnspiels enthielt. Zudem informierte die Agentur den Mann, dass sie dessen Daten aus der Datenbank gelöscht hätte. Außerdem bestätigte sie, dass sie die Daten nicht an Dritte weitergegeben hätte. Daraufhin teilte der Mann der Agentur mit, dass er nie eine Löschung forderte und dass seine Fragen nicht beantwortet worden seien.

Mann beschwert sich bei Aufsicht

Mit der ganzen Situation unzufrieden beschwerte sich der Mann bei der Datenschutzaufsichtsbehörde. Diese forderte Mitte Februar 2023 die Agentur zur Stellungnahme auf. Der Anwalt der Agentur teilte der Behörde mit, dass die Agentur Auskunft erteilt und die Daten gelöscht hätte. Weil man nun keine betreffenden Daten mehr habe, könne man auch keine Auskunft mehr darüber erteilen.

Behörde spricht Verwarnung aus

Nach vorheriger Anhörung sprach die Datenschutzaufsicht eine Verwarnung gegenüber der Agentur aus. Aus Sicht der Behörde hatte die Agentur personenbezogene Daten rechtswidrig verarbeitet. Für das Löschen der Daten gab es keine Rechtfertigung. Zudem würde das eigenmächtige Löschen das Recht des Betroffenen auf Auskunft beschneiden. Diese Verwarnung wollte die Agentur nicht auf sich sitzen lassen. Also zog sie vor das VG Düsseldorf, und zwar mit dem Ziel der Aufhebung des Behördenbescheids. Das VG lehnte das jedoch ab.

So entschied das Gericht

Die Klage der Agentur ist unbegründet. Der Bescheid der Aufsichtsbehörde ist rechtmäßig. Die Agentur wird nicht in ihren Rechten verletzt. Die Aufsichtsbehörde durfte den Bescheid nach Art. 58 Abs. 2 Buchst. d DSGVO erlassen. Ein Verwarnungsgrund lag vor. Die Agentur hat gegen die DSGVO verstoßen. Das Löschen der betreffenden Daten trotz der bestehenden Auskunftspflicht war rechtswidrig. Beim Löschen von Daten handelt es sich um eine Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO. Eine solche Verarbeitung muss nach Art. 5 Abs. 2 i. V. m. Abs. 1 Buchst. a DSGVO rechtmäßig erfolgen. Die Rechtmäßigkeit beurteilt sich nach Art. 6 DSGVO. Keine der Rechtsgrundlagen ist vorliegend erfüllt. Die Verarbeitung ist weder für eine Vertragserfüllung erforderlich, lässt sich nicht auf ein überwiegendes berechtigtes Interesse stützen, noch liegt die Einwilligung des Betroffenen vor.

Für Löschen gab es keinen Grund

Zudem bestand keine rechtliche Pflicht nach Art. 6 Abs. 1 Satz 1 Buchst. c DSGVO, die Daten zu löschen. So lagen die Voraussetzungen des Art. 17 DSGVO nicht vor. Die Daten waren vor dem Hintergrund des Art. 17 Abs. 1 DSGVO weiterhin für das E-Mail-Marketing sowie für die Erfüllung der Auskunftspflicht erforderlich. Ein Widerspruch gegen die Verarbeitung hatte der Mann nicht erklärt, genauso wenig eine erteilte Einwilligung widerrufen. Eine unrechtmäßige Verarbeitung fand aus Sicht der Klägerin nicht statt. Auch lässt sich die Löschung nicht auf eine angebliche sachliche Unrichtigkeit der Daten stützen.

Verwarnung war verhältnismäßig

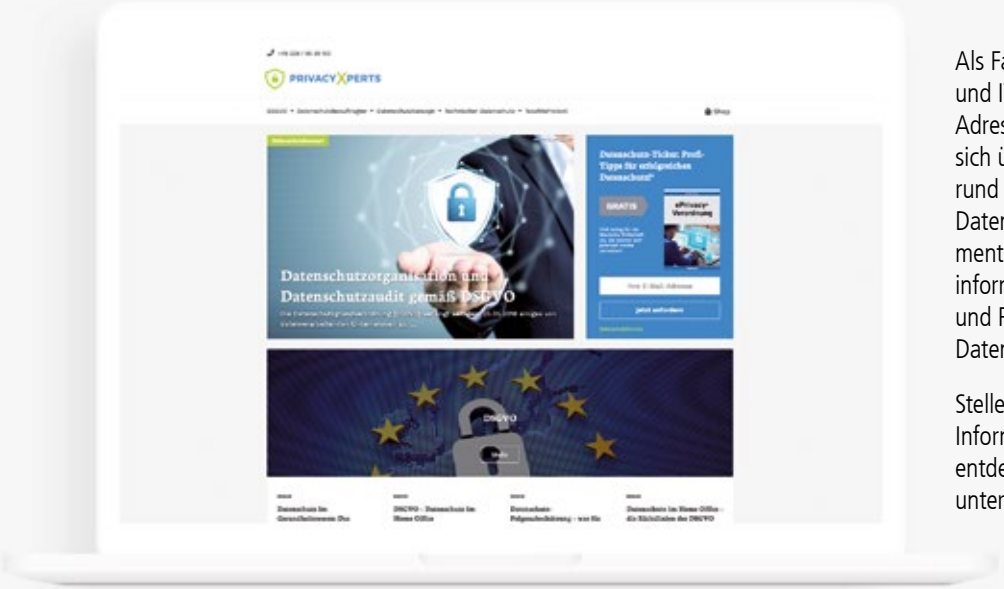
Nach Ansicht des Gerichts hat die Behörde ihr Ermessen fehlerfrei ausgeübt. Es liegt kein Verstoß gegen den Grundsatz der Verhältnismäßigkeit bezüglich der behördlichen Handlungsoptionen vor. Die Verwarnung ist das mildeste Mittel, weil kein Bußgeld damit verbunden ist. Letzteres wäre möglich gewesen, weil die Agentur aus ihrer Sicht rechtmäßig verarbeitete Daten löschte und so das Recht auf Auskunft des Betroffenen vereitelt hat.

§

Das können Sie folgern

Will ein Betroffener Auskunft von Ihrem Unternehmen, kann man sich die Sache nicht einfach machen und die personenbezogenen Daten löschen. Das erst recht nicht, wenn ein Betroffener gar keine Löschung fordert, sondern nur Auskunft. In einem solchen Fall geht die Auskunft einer Löschung vor. Greifen die Löschpflichten aus Art. 17 DSGVO nicht, gilt außerdem: Das Löschen kann eine Verarbeitung personenbezogener Daten darstellen, für die Ihr Unternehmen eine Rechtsgrundlage haben muss.

„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

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:

Urlaubszeit: Das sollten Sie vorbereiten

Messestand & Co.: Checken Sie diese Punkte