



## AUSBILDUNGSSTART: HEISSEN SIE DIE NEUEN AZUBIS WILLKOMMEN

### KNOW-HOW

Damit Audits gut gelingen:  
Machen Sie den Selbstcheck

1-2

### DATENSCHUTZ- ORGANISATION

Datenabfluss: Setzen Sie jetzt  
auf diese 10 Tipps

3



Onlinebereich:  
<https://www.privacyxperts.de>



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



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



**PRIVACYXPERTS**



## Üben Sie konstruktive Kritik

Liebe Leserin, lieber Leser,

wenn es im Datenschutz nicht rundläuft oder mancher anscheinend macht, was er will, kann das bei Ihnen für viel Frust und Ärger sorgen. Nun könnten Sie aus allen Wolken fallen und Ihrem Ärger Luft machen. Doch auch wenn Standpauken oft Eindruck machen, heißt das nicht, dass sie das Mittel der Wahl sind. Denn schnell können Sie über das Ziel hinausschießen.

Viel besser ist es, wenn Sie zwar kurz Ihre Enttäuschung oder Verärgerung zum Ausdruck bringen. Gehen Sie dann jedoch direkt in konstruktive Kritik über. Erklären Sie, was falsch lief, worauf es ankommt und wie es richtig geht.

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

### Know-how

Damit Audits gut gelingen:  
Machen Sie den Selbstcheck  
[Seiten 1–2](#)

### Datenschutzorganisation

Datenabfluss: Setzen Sie jetzt  
auf diese 10 Tipps  
[Seite 3](#)

### Awareness

Ausbildungsstart: Heißen Sie die  
neuen Azubis willkommen  
[Seiten 4–5](#)

### Datenschutzbeauftragter

Kennen Sie sich mit Ihrer  
Loyalitätspflicht aus?  
[Seite 6](#)

### Fragen an die Redaktion

Dürfen wir Jubiläen & Co. im  
Intranet veröffentlichen?  
[Seite 7](#)

Muss ich Dienstleister regelmäßig  
kontrollieren?  
[Seite 7](#)

### Recht

Arbeitgeber muss Gehaltsdaten  
an Headhunter geben  
[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



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 | Lifeisbeautiful; Seite 1: Adobe  
Stock | Yusri Adi  
Erscheinungsweise: 36-mal pro Jahr  
E-Mail: [kundendienst@privacyxperts.de](mailto:kundendienst@privacyxperts.de)  
Internet: [www.privacyxperts.de](http://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



Sie sollen auch die Einhaltung der Regelungen zum Datenschutz kontrollieren.

# Damit Audits gut gelingen: Machen Sie den Selbstcheck

Zu Ihren Aufgaben als Datenschutzbeauftragter nach Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO) zählt nicht nur das Beraten in allen Fragen des Datenschutzes. Sie sollen auch die Einhaltung der Regelungen zum Datenschutz beim Verantwortlichen kontrollieren, etwa im Unternehmen. Prüfen klingt erst einmal nach einer einfachen Sache. Doch Sie können viel falsch machen.

## Auditieren Sie nicht jeden und alles

Klar ist: Sie sollen die Einhaltung des Datenschutzes kontrollieren. Doch das darf nicht dazu führen, dass Sie Ihr Unternehmen lahmlegen. Sie müssen die richtigen Schwerpunkte setzen. Das sieht sogar der Gesetzgeber vor. Denn der macht Ihnen zur Auflage, dass Sie bei Ihren Aufgaben risikoorientiert vorgehen (Art. 39 Abs. 2 DSGVO). Insofern sollten Sie zunächst dort hinschauen, wo die größten Risiken für die Betroffenen liegen. Prio A muss auch haben, wo es in Ihrem Unternehmen unter Datenschutzaspekten eher zu Verstößen, Pannen oder Patzern kommen kann. Denn dann leisten Sie nicht nur dem Datenschutz einen guten Dienst. Sie betreiben auch Risikovorsorge für Ihr Unternehmen.

## Auf das richtige Mindset kommt es an

Audits sind prinzipiell immer ein Frage-Antwort-Gespräch. Sie fragen nach etwas, Sie bekommen eine Antwort und wollen ggf.

Belege sehen. Dann prüfen Sie, ob das Ist zum Soll passt, etwa zur DSGVO oder zu internen Vorschriften. Damit Audits viel bringen, kommt es jedoch auf Ihr Mindset an, sprich Ihre grundlegende Einstellung. Ihnen muss es darum gehen, dass der Datenschutz bestmöglich umgesetzt wird. Insofern sollte Ihnen nicht daran gelegen sein, die Geprüften abzustrafen. Besser ist es, wenn Sie auch beim Audit den Fokus auf das Beraten legen. Denn die Erfahrung zeigt, dass Beratungsaudits auch bei erheblichen Defiziten von den Geprüften leichter akzeptiert werden. Man ist eher bereit, die Defizite zügig anzugehen.

## Arbeiten Sie an Ihren Soft Skills

Für ein gutes Audit brauchen Sie viel fachliches Wissen. Doch daneben müssen Sie auch die weichen Faktoren berücksichtigen, etwa rund um Gesprächsführung oder geschicktes Vorgehen. Damit Ihnen das gelingt, sollten Sie bei jedem Audit die Punkte der folgenden Checkliste umsetzen. Machen Sie den Selbstcheck.

## Selbstcheck: Schlaues Vorgehen bei Audits



| Aspekte                                                     | Darauf sollten Sie achten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Umgesetzt?                                          |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>Vorbereitung</b>                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                     |
| Bereits bei der Auditplanung gehe ich risikoorientiert vor? | <ul style="list-style-type: none"> <li>› Setzen Sie konsequent auf Risikoorientierung. Gibt es Bereiche oder Verarbeitungen mit geringem Risiko, müssen Sie Audits nicht komplett entfallen lassen. Sie können etwa auf Kurzaudits oder die Beantwortung eines kurzen Fragenkatalogs setzen.</li> <li>› Idealerweise haben Sie eine detaillierte Auditplanung, aus der Risiken und abgeleitete Schwerpunkte für Audits hervorgehen. Als lebendes Dokument können Sie auch unterjährig die Prioritäten verschieben. Halten Sie die Gründe für eine Änderung der Prioritäten oder Bewertungen fest.</li> </ul> | <input type="radio"/> Ja <input type="radio"/> Nein |





|                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                     |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Bereite ich Audits frühzeitig und umfassend vor?                                       | <ul style="list-style-type: none"> <li>› Audits wollen gut durchdacht und entsprechend geplant werden.</li> <li>› Kündigen Sie Audits rechtzeitig an und stellen Sie sicher, dass erforderliche Gesprächspartner auch tatsächlich verfügbar sind.</li> <li>› Machen Sie sich Gedanken zum Auditumfang und zur -tiefe. Legen Sie konkret den Fokus fest.</li> </ul>                                                                                                                                                           | <input type="radio"/> Ja <input type="radio"/> Nein |
| Informationen zur auditierten Einheit bzw. zum auditierten Thema fordere ich vorab an? | <ul style="list-style-type: none"> <li>› Verschaffen Sie sich einen Überblick über die Situation im zu prüfenden Bereich. Sie sollten wissen, was man dort macht.</li> <li>› Prüfen Sie das Verzeichnis von Verarbeitungstätigkeiten. Damit haben Sie einen Überblick über die bekannten bzw. dokumentierten Verarbeitungstätigkeiten.</li> <li>› Holen Sie vorab Informationen im Bereich ein, etwa zur Datenschutzsituation vor Ort.</li> </ul>                                                                            | <input type="radio"/> Ja <input type="radio"/> Nein |
| Bei den relevanten Vorschriften und Regelwerken bin ich sattelfest?                    | <ul style="list-style-type: none"> <li>› Bei den Themen, die Sie prüfen, müssen Sie sich auskennen. Das umfasst vor allem die datenschutzrechtlichen Rahmenbedingungen.</li> <li>› Prüfen Sie vorab auch die internen Vorschriften und Prozesse. Diese beschreiben das Soll, gegen das Sie prüfen können.</li> </ul>                                                                                                                                                                                                         | <input type="radio"/> Ja <input type="radio"/> Nein |
| Mit den Auditierten führe ich rechtzeitig ein Vorgespräch?                             | <ul style="list-style-type: none"> <li>› Klären Sie in einem Gespräch darüber auf, worauf Sie es abgesehen haben, was Sie prüfen wollen und wie man sich vorbereiten sollte. Das vermeidet Stress und Frust beim Audit.</li> <li>› Nehmen Sie Bedenken oder Wünsche ernst. Passt Ihr Audit gerade überhaupt nicht in den Terminplan, sollten Sie darüber nachdenken, es ausnahmsweise zu verschieben.</li> </ul>                                                                                                             | <input type="radio"/> Ja <input type="radio"/> Nein |
| Stimme ich mit der Unternehmensleitung meine Prüfung ab?                               | <ul style="list-style-type: none"> <li>› Erläutern Sie, was Sie prüfen wollen. Ggf. können Sie Hinweise, Wünsche oder Empfehlungen in Ihr Audit einfließen lassen.</li> <li>› Die Abstimmung mit der Unternehmensleitung kann auch ein „Türöffner“ sein, wenn man in einem Bereich ein Audit generell ablehnt.</li> </ul>                                                                                                                                                                                                    | <input type="radio"/> Ja <input type="radio"/> Nein |
| Es ist festgelegt, was ich anhand welcher Belege wie prüfen will?                      | <ul style="list-style-type: none"> <li>› Denken Sie immer daran, dass Datenschutzrelevantes aufgrund der Rechenschaftspflicht nachweisbar sein muss.</li> <li>› Setzen Sie auch hier auf Risikoorientierung. Nicht alles muss immer schriftlich nachweisbar sein. Auch „gelebte Praxis“ kann im Einzelfall ausreichen.</li> </ul>                                                                                                                                                                                            | <input type="radio"/> Ja <input type="radio"/> Nein |
| Ich plane ausreichend Zeit für die Durchführung des Audits ein?                        | <ul style="list-style-type: none"> <li>› Nicht nur das Antworten auf Ihre Fragen braucht Zeit. Das gilt auch für die Sichtung von Nachweisen oder die Durchführung von Begehungen.</li> <li>› Planen Sie großzügig und mit Puffer. Niemand ist Ihnen böse, wenn ein Audit früher beendet ist.</li> </ul>                                                                                                                                                                                                                     | <input type="radio"/> Ja <input type="radio"/> Nein |
| <b>Prüfung</b>                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                     |
| Ich habe jederzeit meinen gesetzlichen Auftrag vor Augen?                              | <ul style="list-style-type: none"> <li>› Sie sollen die Umsetzung der Anforderungen zum Datenschutz kontrollieren. Sie sind dabei nicht die Datenschutzpolizei, die jeden Verstoß ahnden muss.</li> <li>› Beherzigen Sie stets, dass Sie risikoorientiert arbeiten sollen. Das gilt auch für Prüfungen.</li> </ul>                                                                                                                                                                                                           | <input type="radio"/> Ja <input type="radio"/> Nein |
| Ich arbeite meinen festgelegten Fragenkatalog konsequent ab?                           | <ul style="list-style-type: none"> <li>› Fragen, die Sie vorab festgelegt haben, sollten Sie auch tatsächlich stellen.</li> <li>› Wollen Sie Fragen übergehen, notieren Sie den entsprechenden Grund.</li> </ul>                                                                                                                                                                                                                                                                                                             | <input type="radio"/> Ja <input type="radio"/> Nein |
| Ich gestalte die Befragung so, dass die Auditierten umfassend antworten können?        | <ul style="list-style-type: none"> <li>› Lassen Sie die Geprüften reden und nehmen Sie sich zurück.</li> <li>› Geben Sie die nötige Zeit, um Antworten zu durchdenken.</li> </ul>                                                                                                                                                                                                                                                                                                                                            | <input type="radio"/> Ja <input type="radio"/> Nein |
| Bei Aspekten, die ich nicht beurteilen kann, hole ich Expertenwissen ein?              | <ul style="list-style-type: none"> <li>› Sie können sich nicht bei allem auskennen. Sind Sie sich unsicher, fragen Sie die zuständigen Spezialisten.</li> <li>› Dokumentieren Sie, wen Sie einbezogen haben und was man Ihnen geraten hat.</li> </ul>                                                                                                                                                                                                                                                                        | <input type="radio"/> Ja <input type="radio"/> Nein |
| Erkenntnisse und Feststellungen halte ich sofort fest?                                 | <ul style="list-style-type: none"> <li>› Verschieben Sie das nicht auf später. Denn was nicht gleich notiert wird, wird ggf. vergessen oder bleibt in falscher Erinnerung.</li> <li>› Haben Sie immer etwas parat, um Notizen oder Fotos zu machen. Auch Sprachnotizen sind hilfreich.</li> </ul>                                                                                                                                                                                                                            | <input type="radio"/> Ja <input type="radio"/> Nein |
| <b>Abschlussbesprechung</b>                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                     |
| Direkt nach dem Audit bespreche ich mit den Auditierten das Ergebnis?                  | <ul style="list-style-type: none"> <li>› Lassen Sie die Geprüften nicht im Ungewissen. Nehmen Sie sich die Zeit für ein kurzes Abschlussgespräch.</li> <li>› Idealerweise können Sie bereits einen vorläufigen Bericht zur Verfügung stellen.</li> </ul>                                                                                                                                                                                                                                                                     | <input type="radio"/> Ja <input type="radio"/> Nein |
| Ich lasse andere Auffassungen zu?                                                      | <ul style="list-style-type: none"> <li>› Viele Dinge kann man unterschiedlich sehen. Geben Sie Gelegenheit zur Stellungnahme.</li> <li>› Notieren Sie andere Sichtweisen. Lassen Sie diese im Bericht nicht unerwähnt.</li> </ul>                                                                                                                                                                                                                                                                                            | <input type="radio"/> Ja <input type="radio"/> Nein |
| Es werden erste Maßnahmen festgelegt?                                                  | <ul style="list-style-type: none"> <li>› Bereits in der Abschlussbesprechung können erste Maßnahmen vereinbart werden.</li> <li>› Denken Sie daran, Verantwortlichkeiten und Termine festzulegen.</li> </ul>                                                                                                                                                                                                                                                                                                                 | <input type="radio"/> Ja <input type="radio"/> Nein |
| <b>Bericht</b>                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                     |
| Ich halte alle wesentlichen Berichtsaspekte direkt nach dem Audit fest?                | <ul style="list-style-type: none"> <li>› Beschreiben Sie objektiv, was geprüft wurde, welche Nachweise es gibt und worin Defizite bestehen.</li> <li>› Lassen Sie nichts unter den Tisch fallen. Beschreiben Sie alles so, dass es auch später noch eindeutig nachvollzogen werden kann.</li> <li>› Erwähnen Sie auch Positives. Das motiviert für die Zukunft und trägt zur Datenschutzakzeptanz bei.</li> <li>› Achten Sie generell auf einen positiven Grundton. Vermeiden Sie Vorwürfe. Bleiben Sie sachlich.</li> </ul> | <input type="radio"/> Ja <input type="radio"/> Nein |
| Defizite und Mängel habe ich nach ihrem Schweregrad bewertet?                          | <ul style="list-style-type: none"> <li>› Machen Sie eine Einschätzung, ob Defizite gering, mittel oder gravierend sind. Das unterstreicht den Handlungsbedarf.</li> <li>› Orientieren Sie sich hier an den Maßstäben der internen Revision.</li> </ul>                                                                                                                                                                                                                                                                       | <input type="radio"/> Ja <input type="radio"/> Nein |
| Empfehlungen zur Behebung der Defizite oder Mängel spreche ich im Bericht aus?         | <ul style="list-style-type: none"> <li>› Geben Sie Hinweise, wie aus Ihrer Sicht Defizite behoben werden können. Allerdings sollten Sie auch andere Wege zum Ziel zulassen.</li> <li>› Achten Sie hier auf Realitätsbezug. Die Umsetzung muss möglich und machbar sein.</li> </ul>                                                                                                                                                                                                                                           | <input type="radio"/> Ja <input type="radio"/> Nein |

# Datenabfluss: Setzen Sie jetzt auf diese 10 Tipps

**Die Beschäftigten Ihres Unternehmens wissen: Geht es um Fragen mit Datenschutzrelevanz, dann sind sie bei Ihnen an der richtigen Adresse. Das gilt umso mehr, wenn Beschäftigte vermuten, dass Daten in falsche Hände geraten sind. In diesem Fall muss schnell gehandelt werden.**

Gründe für einen Datenabfluss kann es viele geben. Es muss nicht ein Angriff von Cyberkriminellen sein. Auch ein falsch konfigurierter Onlineshop oder ein Server können Informationen für Unbefugte offenlegen oder abrufbar machen. Meldet sich ein Beschäftigter bei Ihnen, können Sie viel dazu beitragen, dass sich ein möglicher Schaden in Grenzen hält. Beherzigen Sie dazu diese Tipps:

## **Tipp Nr. 1: Hören Sie zu und strahlen Sie Ruhe aus**

Weil die Sache eilt, wird man Sie wahrscheinlich per Telefon kontaktieren. Nehmen Sie die Sache und den Anrufer ernst. Beruhigen Sie ihn. Drücken Sie das auch so aus. Auch bestätigende oder positive Formulierungen helfen dabei, den „erhöhten Blutdruck“ aus der Sache zu nehmen. Wichtig ist zudem: Hören Sie zu. Wimmeln Sie auf keinen Fall den Anrufer ab. Das kann nach hinten losgehen und unter Umständen sind dann gerade Sie die Ursache dafür, dass nicht schnell gehandelt wird.

## **Tipp Nr. 2: Klären Sie die Situation**

Lassen Sie sich konkret schildern, was passiert ist bzw. worauf die Wahrnehmung des Anrufers beruht. Um möglichst viele Informationen zu erhalten, sollten Sie W-Fragen nutzen, und zwar so wie auch eine Rettungsleitstelle sich einen Überblick über eine Situation verschaffen würde. Fragen Sie etwa: Was ist passiert? Wer hat was und wie bemerkt? Welche und wessen Daten sind betroffen? Wer ist für die betroffene Verarbeitung verantwortlich?

## **Tipp Nr. 3: Stoßen Sie die sofortige Eindämmung an**

Gibt es spezifische Notfall- oder Incident-Response-Pläne, sollten Sie die dort vorgegebenen Prozesse starten. Weichen Sie nach Möglichkeit nicht davon ab. Hakt es jedoch irgendwo, etwa weil ein Ansprechpartner nicht verfügbar ist, sollten Sie die Sache pragmatisch handhaben.

Fehlen entsprechende Pläne, gilt: Veranlassen Sie unverzüglich, dass der Datenabfluss gestoppt wird. Ihr erster Ansprechpartner wird hier die IT-Abteilung oder eine Fachabteilung sein. Diese müssen sofort das Nötige veranlassen und beispielsweise IT-Systeme vom Internet trennen oder Zugriffsrechte einschränken. Die betroffenen Systeme oder Verarbeitungen dürfen erst wieder online gehen, wenn ein erneuter Datenabfluss ausgeschlossen ist.

## **Tipp Nr. 4: Berufen Sie ein Reaktionsteam ein**

Gerade wenn die Sache größer ist, kommen Sie nicht drum herum, alles Relevante im Team abzustimmen und die nächsten Maßnahmen festzulegen. Neben IT- und Fachabteilung können auch die Unternehmenskommunikation oder die Rechtsabteilung relevante

Teilnehmer sein. Auch einen Vertreter der Unternehmensleitung sollten Sie nicht vergessen.

## **Tipp Nr. 5: Ermitteln Sie Umfang und Schutzbedarf**

Einerseits sollten Sie das tatsächliche Vorliegen eines Vorfalls bewerten. Andererseits ist es unerlässlich, das Ausmaß des Vorfalls zu bewerten. Dabei spielt nicht nur die Zahl der Betroffenen eine Rolle. Prüfen Sie auch die Menge und Sensibilität der betroffenen Daten. Denn klar ist: Je sensibler und schadensträchtiger die Daten sind, desto entschlossener muss Ihr Unternehmen handeln.

## **Tipp Nr. 6: Bewerten Sie die Risiken**

Analysieren Sie, welche Gefahren für Betroffene bestehen. Bewerten Sie dann das Risiko auf Basis der Faustformel „Schadenshöhe x Eintrittswahrscheinlichkeit“. Hohe Risiken müssen schnellstens angegangen werden. Dokumentieren Sie die Risikoanalyse.

## **Tipp Nr. 7: Prüfen Sie die Melde- und Infopflichten**

Bewerten Sie gemeinsam, inwieweit eine Meldung nach Art. 33 Datenschutz-Grundverordnung (DSGVO) binnen 72 Stunden an die Aufsichtsbehörde erforderlich ist. Zudem ist zu entscheiden, inwieweit ein hohes Risiko für Betroffene besteht und eine Information nach Art. 34 DSGVO erfolgen muss.

## **Tipp Nr. 8: Bereiten Sie nötige Entscheidungen vor**

Als Datenschutzbeauftragter sind Sie nicht in der Entscheidungs- und Umsetzungsverantwortung. Belassen Sie diese beim Unternehmen bzw. dessen Vertretern. Sprechen Sie allerdings Empfehlungen aus, etwa gegenüber der Unternehmensleitung. Unterstützen Sie beratend bei der Entscheidungsfindung, etwa bezüglich einer Meldung oder Presseinformation.

## **Tipp Nr. 9: Begleiten Sie die Sache bis zum Abschluss**

Datenabflüsse haben wie alle Datenpannen höchste Priorität. Räumen Sie der Sache Vorrang vor anderen Themen und Terminen ein. Stehen Sie für kurzfristige Termine bereit und begleiten Sie die festgelegten Maßnahmen fortlaufend.

## **Tipp Nr. 10: Dokumentieren Sie alles Wichtige**

Alles Relevante sollte festgehalten werden, etwa Sachverhalt, Bewertungen, Begründungen, Entscheidungen und Maßnahmen. Dass das nötig ist, ergibt sich aus Art. 33 Abs. 5 DSGVO. Dokumentieren Sie auch Ihre Beratung.

# Ausbildungsstart: Heißen Sie die neuen Azubis willkommen

Bald geht es wieder los, der Ausbildungsstart 2026 steht vor der Tür, und zwar vielleicht auch in Ihrem Unternehmen. Mancher junge Mensch startet dann in sein Arbeitsleben, mit vielen neuen Herausforderungen. Eine davon ist, mit personenbezogenen Daten richtig und sorgsam umzugehen. Dass das gelingt, haben auch Sie in der Hand.

## Awareness können Sie im Handumdrehen steigern

Gerade bei neuen Auszubildenden ist das Risiko für Datenschutzverstöße groß. Zwar haben viele schon einmal vom Datenschutz gehört. Was es damit im Unternehmen auf sich hat und worauf man als Beschäftigter achten muss, dürfte vielen jedoch fremd sein. Umso wichtiger ist, dass Sie potenziellen Risiken den Kampf ansagen und Datenschutzverstößen oder Pannen vorbeugen. Vermitteln Sie also direkt am Anfang einige wichtige Regeln und geben Sie die passenden Tipps.

## Wählen Sie das passende Vorgehen

Um ein Grundverständnis zu schaffen, haben Sie verschiedene Möglichkeiten. Gibt es eine Willkommensveranstaltung für die Azubis, können Sie dort einen Vortrag halten. Doch häufig ist das Programm so gefüllt, dass Sie nicht ausreichend Zeit für Ihr Thema

bekommen. Dann brauchen Sie Alternativen für Ihren Kontakt zu den Azubis.

So haben Sie die Möglichkeit, eine eigene Veranstaltung anzubieten. Wichtig ist, dass Sie hier alle Azubis erreichen. Ist das nicht sichergestellt, besteht das Risiko, dass genau diejenigen Fehler im Umgang mit personenbezogenen Daten machen, die nicht teilnehmen konnten. Daher ist Folgendes sinnvoll: Sie können in einem Willkommensschreiben des Datenschutzbeauftragten einige wichtige Tipps geben. Dieses Schreiben können Sie der Personalabteilung geben. Und die versendet dieses Schreiben per Post bzw. per E-Mail in einem Informationspaket an die neuen Azubis. Dann können sich die Azubis schon vor dem ersten Arbeitstag mit den Tipps beschäftigen. Alternativ können Sie am ersten Tag eine E-Mail an die neuen Azubis schicken. Ihren Entwurf können Sie auf folgendem Muster aufbauen. Ergänzen Sie die Tipps um betriebliche Besonderheiten Ihres Unternehmens oder um eine Liste mit Links oder wichtigen Ansprechpartnern.



## Muster: Datenschutztipp für neue Azubis

Liebe Auszubildende,  
lieber Auszubildender,

herzlich willkommen in unserem Unternehmen! Ich bin Mira Belle, deine Datenschutzbeauftragte, und kümmere mich darum, dass alle in unserem Unternehmen – auch Du – richtig und sorgsam mit personenbezogenen Daten umgehen. Personenbezogene Daten (z. B. Name, Adresse, Telefonnummer, E-Mail-Adressen von Kunden oder Kollegen) gut zu schützen ist kein Hexenwerk. Damit Dir das leichtfällt und Du von Anfang an alles richtig machst, habe ich Dir einige wichtige Tipps zusammengestellt.

### Warum ist Datenschutz bei uns so wichtig?

Du kannst Dir die Daten in unserem Unternehmen wie einen Schatz vorstellen. Der besteht aus den Daten von Kunden, aber auch aus Geschäftsgeheimnissen, Entwicklungs- oder Vertriebsinformationen. Gerade Kunden, Geschäftspartner und Deine Kolleginnen und Kollegen vertrauen darauf, dass wir alle sorgsam mit ihren Informationen umgehen. Und dieses Vertrauen ist die Grundlage für gute Geschäfte und den langfristigen Erfolg unseres Unternehmens. Wir müssen alles daran setzen, dass wir dieses Vertrauen nicht enttäuschen. Denn Pannen oder vernachlässigter Datenschutz setzen nicht nur den Geschäftserfolg aufs Spiel. Es drohen auch erheblicher Ärger und hohe Bußgelder.

### Auf Dich kommt es an!

Mach Dir stets klar: Datenschutz funktioniert nur, wenn alle mitmachen – also auch Du! Jeder Beschäftigte in unserem Unternehmen trägt entsprechend Verantwortung für den sorgsamen und richtigen Umgang mit personenbezogenen Daten. Daher ist wichtig: Bitte gehe immer verantwortungsvoll mit personenbezogenen Daten um. Beachte unsere Regeln. Beherzige sie immer, wenn es um schützenswerte Daten geht.

### Diese wichtigen Tipps musst Du immer umsetzen:

#### Verarbeite personenbezogene Daten nur, wenn das erlaubt ist. Halte Dich an unsere Regeln und Prozesse

Personenbezogene Daten dürfen nicht nach Lust und Laune beschafft und verwendet werden. Hier gelten wichtige Rahmenbedingungen. Beispielsweise muss es dafür immer eine Erlaubnis geben, eine Rechtsgrundlage. Zudem müssen bestimmte Rahmenbedingungen eingehalten werden, etwa um die Sicherheit der verarbeiteten Daten zu gewährleisten.

Welche Daten für welche Zwecke verarbeitet werden dürfen, erfährst Du in den Arbeitsanweisungen und bei den entsprechenden Prozessbeschreibungen. Zudem kannst Du jederzeit mit Deinen Kollegen, Ausbildern oder Vorgesetzten sprechen. Das ist gerade dann wichtig, wenn Du Dir beim richtigen Vorgehen unsicher bist.

## Achte auf Clean Desk und sperre bei jeder Abwesenheit Deinen Computer

Was mit Clean Desk gemeint ist, ist schnell erklärt: Schützenswertes und Sensibles darfst Du nicht offen herumliegen lassen. Das gilt einerseits, wenn Unbefugte die Informationen zur Kenntnis nehmen können. Andererseits darf nichts Schützenswertes offen herumliegen, wenn Du Deinen Arbeitsplatz verlässt, auch wenn das nur für einen kurzen Moment ist.

Auch auf Deinen Computer musst Du ein Auge haben. Diesen musst Du sperren, wenn Du den Arbeitsplatz verlässt. Das geht ganz einfach: Drücke gleichzeitig auf der Tastatur „Windows“ und „L“.

## Gib Deine Anmeldedaten nie weiter und nutze für jedes Konto ein individuelles und sicheres Passwort

Deine Anmeldeinformationen gehen nur Dich etwas an. Behalte sie für Dich, egal, wer Dich danach fragt. Insbesondere darfst Du Dein Passwort niemandem verraten.

Nutze außerdem sichere Passwörter, und zwar für jedes Benutzerkonto individuell. Die bestehen aus mindestens zwölf Zeichen mit Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Damit Du Dir die komplexen Passwörter nicht merken musst, verwendest Du die Passwortdatenbank in dem auf Deinem Computer oder Smartphone bereitgestellten Passwortmanager. Den kannst Du auch für das Erzeugen sicherer Passwörter nutzen. Achte darauf, dass das Passwort für den Zugriff auf Deine Passwortdatenbank sicher ist.

## Verwende an Technik und Software nur das, was wir Dir gegeben haben

Unsere Computer, Smartphones und Software sind sicher. Diese werden zentral von der IT-Abteilung geprüft, gemanagt und bereitgestellt. Nutze daher nichts anderes. Denn das birgt zahlreiche Risiken, etwa für die Sicherheit von Daten oder Systemen. Brauchst Du für Deine Arbeit etwas anderes, besprich das mit Deinem Vorgesetzten oder Ausbilder. Handle nie eigenmächtig. Installiere keine Software, nutze keine Programme und Speicher im Internet und verändere keine Sicherheitseinstellungen bei Computer oder Smartphone.

## Gehe sorgsam mit KI um

Es gibt viele KI-Tools, mit denen man sich das Leben leichter machen kann. Allerdings bergen viele so einige Risiken, gerade für den Datenschutz. Daher gilt: Nutze nur die in unserem Unternehmen freigegebenen KI-Tools. Andere Tools, etwa kostenlose Chatbots im Internet, darfst Du bei uns nicht nutzen. Beachte zudem bei den internen KI-Tools die geltenden Regeln und Prozesse. Bei Fragen oder Unklarheiten kannst Du jederzeit Deinen Vorgesetzten oder Ausbilder ansprechen.

## Prüfe vor Versand von E-Mails genau die Empfänger

Willst Du eine E-Mail versenden, prüfe genau, an wen Du diese verschickst. Gerade wenn Du die Autovervollständigung bei der Adresseingabe nutzt, heißt es „zweimal hinschauen“. Schließlich musst Du vermeiden, dass E-Mails mit ggf. sensiblen Informationen an die falschen Empfänger gehen.

Nutzt Du E-Mail-Verteiler, heißt es ebenfalls Augen auf. Prüfe genau, ob Du den richtigen Verteiler gewählt hast. Bei mehreren externen Empfängern solltest Du das Bcc-Feld für die Adresseingabe nutzen. So erfahren die Empfänger nicht, wer sonst noch die E-Mail erhalten hat. Und auch hier gilt: Frage bei Unklarheiten oder Unsicherheiten bei Deinen Kollegen oder Deinem Vorgesetzten nach.

## Wahre immer die Vertraulichkeit

Schützenswerte Informationen und Interna gehen Unbefugte und Dritte außerhalb des Unternehmens nichts an. Achte bei Gesprächen mit sensiblen Inhalten darauf, dass Du diese so führst, dass niemand Unbefugtes mithören kann. Behalte jegliche Informationen aus dem Unternehmen für Dich. Diese sind auch für Familienmitglieder und Freunde tabu.

Arbeitest Du mit dem Computer unterwegs, platziere Dich so, dass niemand über die Schulter mitlesen kann. Nutze bei Bedarf eine Sichtschutzfolie für den Bildschirm. Denke auch daran, Computer und andere Geräte vor Diebstahl zu schützen. Nutze beispielsweise für das Notebook ein Kabelschloss.

## Falle nicht auf Cyberkriminelle rein

Kriminelle geben sich oft als Vorgesetzte, Kollegen oder Mitarbeiter vertrauenswürdiger Unternehmen aus. Sie verschicken täuschend echte E-Mails, SMS oder Messenger-Nachrichten. Mit solchem Phishing will man Dir sensible Informationen entlocken oder Dich zu unüberlegten Handlungen verleiten. Stutzig werden musst Du, wenn Du Nachrichten von unbekannten Absendern bekommst, Du unpersönlich angesprochen wirst, Rechtschreib- oder Grammatikfehler enthalten sind, Zeitdruck aufgebaut wird, man Dir droht oder von Dir absolute Geheimhaltung verlangt.

Kommt Dir etwas seltsam vor, dann gilt: Denke zweimal nach, bevor Du handelst. Lass Dir nicht drohen oder Dich unter Druck setzen. Setze das Geforderte nicht um. Sprich umgehend mit Kollegen, Deinem Vorgesetzten oder Ausbilder. Auch ich als Datenschutzbeauftragte habe ein offenes Ohr für Dich.

## Und wenn doch einmal etwas passiert ...

... dann ist das kein Weltuntergang. Denn wo Menschen arbeiten, passieren Fehler. Wichtig ist allerdings: Wende Dich umgehend vertrauensvoll an Deinen Vorgesetzten. Du kannst Dich natürlich auch an mich wenden. Was nicht geht, ist abwarten und hoffen, dass alles gut geht. Denn das kann sich rächen. Schließlich kann im Datenschutz schnell viel Schaden entstehen, wenn nicht schnell gehandelt wird.

## Ich bin für Dich da!

Vieles ist für Dich neu. Da ist es kein Wunder, dass viele Fragen aufkommen. Bei allen Fragen rund um den Datenschutz kannst Du Dich gerne bei mir melden. Ich habe jederzeit ein offenes Ohr und behandle Dein Anliegen selbstverständlich vertraulich.

Ich wünsche Dir einen guten Start bei uns!

Deine Mira Belle

Datenschutzbeauftragte



# Kennen Sie sich mit Ihrer Loyalitätspflicht aus?

**Sind Sie interner Datenschutzbeauftragter, ist klar: Sie sind nicht nur Datenschutzbeauftragter. Egal, in welchem Umfang Sie diese Rolle ausüben, Sie sind zugleich auch Arbeitnehmer. Wie bei jedem Arbeitsverhältnis bestehen Haupt- und Nebenpflichten. Teil der Nebenpflichten ist die Loyalitätspflicht. Nehmen Sie diese nicht ernst oder verstoßen Sie dagegen, kann das massiven Ärger bedeuten.**

## Das steckt hinter der Loyalitätspflicht

Im Allgemeinen werden mit der Loyalitätspflicht verschiedene Nebenpflichten zusammengefasst. So z. B. die Pflicht zur Treue, zum Schutz und zur Rücksichtnahme. Auch die Schadensabwendungspflicht zählt dazu. Dabei richten sich diese arbeitsvertraglichen Nebenpflichten nicht nur an Sie als Arbeitnehmer. Auch das Unternehmen, Ihr Arbeitgeber, muss den Verpflichtungen gerecht werden. Gegenseitig muss auf die Rechte, Rechtsgüter und Interessen des anderen Rücksicht genommen werden.

## Auch als Datenschutzbeauftragter trifft Sie die Loyalitätspflicht

Unbestritten ist: Als Datenschutzbeauftragter nehmen Sie Ihre Aufgaben weisungsfrei wahr. Das ergibt sich aus Art. 38 Abs. 3 Satz 1 Datenschutz-Grundverordnung (DSGVO). Zudem trifft Sie als Datenschutzbeauftragten keine Umsetzungsverantwortung. Die liegt gerade nach Art. 24 Abs. 1 DSGVO beim Unternehmen bzw. der Unternehmensleitung. Und dennoch sind diese Aspekte kein Freifahrtschein. Achten Sie insbesondere auf Folgendes:

### Sie müssen Schaden vom Unternehmen abhalten

Droht ein Schaden für das Unternehmen, trifft Sie wie jeden Arbeitnehmer auch die Pflicht, den Schaden vom Unternehmen abzuwenden oder diesen abzumildern. Dabei müssen Sie sich natürlich nicht in Gefahr bringen oder selbst schaden. In der Praxis sollten Sie also Ihre Aufgaben ernsthaft wahrnehmen. Erkennen Sie Defizite oder Verstöße gegen den Datenschutz, dürfen Sie nicht einfach wegschauen. Sie müssen diese den Verantwortlichen bzw. der Unternehmensleitung melden. Übrigens: Nehmen Sie Ihre Aufgaben nicht wahr, kann auch eine Aufsichtsbehörde an Ihrer Eignung bzw. fachlichen Qualifikation zweifeln. Das kann sie berechtigen, vom Unternehmen Ihre Abberufung zu verlangen (§ 40 Abs. 6 Satz 2 Bundesdatenschutzgesetz).

### Informieren Sie immer die Verantwortlichen

Auf der sicheren Seite wären Sie, wenn Sie bei Defiziten immer zuerst den Verantwortlichen informieren, sprich die Unternehmensleitung. Doch das kann nach hinten losgehen, gerade wenn die Verfehlungen nicht so schlimm sind. Am besten gehen Sie gestuft vor: Stellen Sie ein Defizit, einen Verstoß oder Fehlverhalten fest, informieren Sie die jeweils verantwortliche Führungskraft, beispielsweise den Abteilungsleiter. Die Führungskraft trägt nämlich

für ihren Bereich die personelle bzw. unternehmerische Verantwortung. Dringen Sie dort mit Ihrem Hinweis nicht durch oder will man nicht aktiv werden, informieren Sie die Unternehmensleitung.

## Gehen Sie nie eigenmächtig zur Datenschutzaufsicht

Ob ein Datenschutzverstoß für die Aufsichtsbehörde relevant ist oder ob etwa eine Datenpanne gemeldet werden muss, entscheiden nicht Sie. Das ist Sache des Verantwortlichen. Handeln Sie hier nie eigenmächtig und machen Sie keine Meldung. Doch auch wenn es um datenschutzrechtliche Fragen geht, sollten Sie sich vorab das Okay der Unternehmensleitung einholen. Unter Umständen will man gerade nicht, dass Sie mit Ihrer Kontaktaufnahme schlafende Hunde wecken.

## Vermeiden Sie rufschädigende Äußerungen

Äußern Sie sich nie so über Ihr Unternehmen bzw. Ihren Arbeitgeber, dass man Ihnen das als Rufschädigung vorwerfen kann. Auch wenn Missstände noch so gravierend sein mögen, sollten Sie sich auf die Zunge beißen. Das geht Außenstehende nichts an. Adressieren Sie das beim Chef. Vermeiden Sie auch „anonyme“ Äußerungen in sozialen Netzwerken. Denn: Schädigen Sie den Ruf des Unternehmens, liefern Sie meist einen guten Grund für eine außerordentliche Kündigung.

## Seien Sie gegenüber dem Betriebsrat nicht zu redselig

Der Betriebsrat mag zwar Ihr Freund sein. Dennoch sollten Sie mit Informationen zu Defiziten oder Verstößen vorsichtig sein. Schließlich kann ein Betriebsrat diese Informationen auch nutzen, um eigene Interessen zu verfolgen und um in einer anderen Sache Druck auf den Arbeitgeber auszuüben. Sind Sie also zu redselig und offenbaren Sie Kritisches zum Datenschutz gegenüber dem Betriebsrat, kann Ihnen das als Illoyalität ausgelegt werden.

## Vertrauen Sie nicht unerschütterlich auf Ihren Kündigungsschutz

Der besondere Kündigungsschutz schützt Sie zwar und es bedarf eines wichtigen Grundes für den Ausspruch einer Kündigung. Den können Sie aber schnell liefern, wenn Sie schwerwiegend gegen Ihre Loyalitätspflicht verstoßen. So z. B., wenn Sie selbst den Datenschutz nicht beachten, gravierende Defizite im Unternehmen ignorieren oder sich abfällig über das Unternehmen äußern.



# Dürfen wir Jubiläen & Co. im Intranet veröffentlichen?

**FRAGE:** Wir überarbeiten gerade das Intranet des Unternehmens. Eine Idee ist, dass es dort auch eine Rubrik für Dienstjubiläen und runde Geburtstage geben soll. Überlegt wird auch, über Sterbefälle von Mitarbeitern bzw. ehemaligen Mitarbeitern zu informieren. Die Kollegen haben mich gefragt, inwieweit das machbar sei. Was meinen Sie? Dürfen wir die entsprechenden Daten veröffentlichen?

**ANTWORT:** Wichtig ist zunächst: Sie sollten zwischen lebenden und verstorbenen Beschäftigten unterscheiden. Diese Unterscheidung ist nämlich entscheidend für den Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO). Dieses Regelwerk gilt nämlich nur für lebende natürliche Personen und die sie betreffenden Daten. Mit dem Tod greift das Persönlichkeitsrecht nicht mehr. Insofern endet auch die Anwendbarkeit der DSGVO. Das ergibt sich so auch ausdrücklich aus Erwägungsgrund 27 Satz 1 zur DSGVO.

## Informationen Verstorbener unproblematisch

Will Ihr Unternehmen also darüber informieren, dass ein Beschäftigter oder ehemaliger Beschäftigter verstorben ist, dann braucht es hierfür keine Rechtsgrundlage. Insbesondere ist auch keine Einwilligung von Angehörigen, Vorsorgebevollmächtigten, Betreuern oder möglichen Erben erforderlich. Allerdings kann es dennoch im Einzelfall geboten sein, eine Veröffentlichung mit Hinterbliebenen abzustimmen.

## Ansonsten Rechtsgrundlage erforderlich

Bei lebenden natürlichen Personen ist die DSGVO voll anwendbar. Das bedeutet insbesondere, dass für das Verarbeiten personenbezogener

Informationen eine Rechtsgrundlage erforderlich ist. Hier könnte man zunächst an § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) denken. Allerdings wird diese deutsche Rechtsgrundlage als europarechtswidrig angesehen, sodass eher auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO gesetzt werden müsste. Doch egal, wie: Es fehlt jeweils an der Erforderlichkeit. Weder für die Durchführung eines Beschäftigungsverhältnisses noch für die Durchführung eines Vertrags ist die Bekanntgabe von Jahrestagen, Jubiläen oder Geburtstagen erforderlich.

## Setzen Sie auf die Einwilligung

Auch ein überwiegendes berechtigtes Interesse ist problematisch. Zwar können auch Wertschätzung oder eine Stärkung des Zusammenhalts als berechtigtes Interesse gelten. Die Interessen der Betroffenen dürften jedoch überwiegen. Denken Sie hier daran, dass Beschäftigte Jubiläen oder ihren Geburtstag bzw. ihr Alter für sich behalten wollen. Auch will nicht jeder Glückwünsche oder Geschenke erhalten oder zu einem Umtrunk einladen müssen. Das heißt in der Folge: Vor einer Veröffentlichung ist die Einwilligung des Beschäftigten erforderlich. Hier gelten für aktive wie ehemalige Beschäftigte dieselben Regeln. Neben Art. 7 und 4 Nr. 11 DSGVO ist auch § 26 Abs. 2 BDSG zu beachten. Hier ist wichtig: § 26 BDSG gilt auch für ehemalige Beschäftigte.

# Muss ich Dienstleister regelmäßig kontrollieren?

**FRAGE:** Bei uns gab es Probleme im Datenschutz mit einem IT-Dienstleister. Nun hat mir der IT-Leiter vorgeworfen, dass ich als Datenschutzbeauftragter hätte Kontrollen machen müssen. Dabei hätten mir Missstände auffallen müssen. Muss ich wirklich jeden Dienstleister regelmäßig prüfen?

**ANTWORT:** Die Umsetzungsverantwortung für die Pflichten aus der Datenschutz-Grundverordnung (DSGVO) liegen beim Unternehmen als Verantwortlichem. Das kann auch umfassen, dass man IT-Dienstleister im Rahmen einer Auftragsverarbeitung (Art. 28 DSGVO) sorgfältig auswählt und ggf. auch im Datenschutz kontrolliert.

Sie als Datenschutzbeauftragter trifft nur die Pflicht, Ihren Aufgaben nach Art. 39 Abs. 1 DSGVO ordnungsgemäß nachzukommen.

Dabei setzen Sie risikoorientiert die Schwerpunkte (Art. 39 Abs. 2 DSGVO), gerade im Bereich der Kontrolle des Verantwortlichen. Insofern können Sie den Verantwortlichen kontrollieren, ob dieser seinen Pflichten nachkommt, etwa auch im Hinblick auf eine Auftragsverarbeitung. Das heißt nicht, dass Sie selbst als Datenschutzbeauftragter die Auftragsverarbeiter Ihres Unternehmens kontrollieren müssen. Hierfür lässt sich aus der DSGVO keine Pflicht ableiten. Das gilt gerade auch für regelmäßig durchzuführende Kontrollen. Und das ist eher Sache der IT-Abteilung.

# Arbeitgeber muss Gehaltsdaten an Headhunter geben

**Personalvermittler und Headhunter kommen oft zum Einsatz, wenn es schwer ist, bestimmte Stellen in Unternehmen zu besetzen. Diese erhalten für Ihre Vermittlung ein Honorar, das sich am Gehalt des Vermittelten bemisst. Doch darf ein Arbeitgeber die Gehaltsinfos weitergeben, auch wenn der Mitarbeiter dagegen ist? Ja, meint das Landgericht Köln in einer Entscheidung vom 13.11.2025 (Az. 30 O 146/25).**

## Der Sachverhalt

Ein Personalvermittler, der spätere Kläger, wurde für ein Unternehmen tätig. Er sollte bei der Besetzung einer leitenden Position im Unternehmen unterstützen. Dazu wurde ein Vermittlungsvertrag geschlossen. Darin war ein Vermittlungshonorar von 25 % des Bruttojahreseinkommens eines erfolgreich vermittelten Bewerbers vereinbart. Dazu verpflichtete sich das Unternehmen auch, nach Einstellung eines vermittelten Bewerbers dem Personalvermittler die Höhe des gesamten Bruttogehalts mitzuteilen. Im Vertrag verpflichtete sich der Vermittler zudem, dass er sämtliche erhaltene Informationen absolut vertraulich behandeln würde, diese nur für Vermittlungszwecke zu verwenden und nicht an Dritte weiterzugeben.

Der Personalvermittler schaltete für die zu besetzende Stelle eine Anzeige. Darauf meldete sich ein Bewerber, der im Gerichtsverfahren später als Zeuge gehört wurde. Der Bewerber bekundete sein Interesse an der Stelle und nannte eine Gehaltsvorstellung von 110.000 € zuzüglich eines Firmenwagens. Es kam zu einem Vorstellungsgespräch beim Unternehmen. Allerdings kam es nicht zur Einstellung, weil man sich über das Gehalt nicht einigen konnte.

## Bewerber wird doch eingestellt

Rund ein Jahr nach dem Vorstellungsgespräch wurde der Bewerber dann doch beim Unternehmen eingestellt. Das bekam auch der Personalvermittler mit. Also forderte er vom Unternehmen die Mitteilung des Gehalts, um seine Honorarforderung für die Vermittlungstätigkeit geltend machen zu können. Dem wollte das Unternehmen jedoch nicht nachkommen. Als Grund gab das Unternehmen an, dass der neue Mitarbeiter noch in der Probezeit sei und diese erst in einigen Monaten ablaufe. Ferner wolle der neue Mitarbeiter nicht, dass seine Gehaltsinformationen an den Personalvermittler weitergegeben würden. Dieser Weitergabe hätte der Mitarbeiter zwecks Schutzes seiner informationellen Selbstbestimmung ausdrücklich widersprochen.

Der Personalvermittler sah die Sache ganz anders. Schon durch die Zusammenarbeit des Bewerbers mit dem Personalvermittler hätte der Bewerber sein Einverständnis in die Weitergabe der Gehaltsdaten an den Vermittler erteilt. Zudem bestehe nach Art. 6 Abs. 1 Satz 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) ein überwiegendes berechtigtes Interesse am Erhalt der Auskunft. Also strengte der Vermittler eine Stufenklage an, zunächst auf Auskunft über das Gehalt des eingestellten Bewerbers und darauf basierend auf Zahlung des vereinbarten Honorars. Das Gericht bestätigte in einem Teilurteil den Auskunftsanspruch des Vermittlers.

## So urteilte das Gericht

Es wurde zwischen den Parteien ein wirksamer Vermittlungsvertrag geschlossen. Die dort enthaltene Auskunftspflicht ist nicht gesetzes- oder sittenwidrig. Auch ist es branchenüblich, dass sich ein Honorar am Bruttojahresgehalt eines vermittelten Arbeitnehmers orientiert.

## Keine Unmöglichkeit der Auskunft

Die Erteilung der Auskunft ist dem beklagten Unternehmen auch nicht aus rechtlichen Gründen nach § 275 Abs. 1 Bürgerliches Gesetzbuch unmöglich. Denn eine solche Unmöglichkeit ergibt sich gerade nicht aus dem Widerspruch des Arbeitnehmers im Hinblick auf § 26 Bundesdatenschutzgesetz. In diesem Zusammenhang sind auch die Erlaubnistatbestände der DSGVO zu berücksichtigen.

## Vermittlerinteresse überwiegt

Das Recht auf Erteilung der Auskunft lässt sich auf Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO stützen. Das Interesse des Vermittlers überwiegt das Geheimhaltungsinteresse des eingestellten Bewerbers. Hierbei sind insbesondere der verfolgte Zweck, Art und Aussagekraft der Daten sowie die Folgen der Verarbeitung zu betrachten. Ferner kommt es auf die Erwartungshaltung der Betroffenen sowie die Absehbarkeit der Verarbeitung, sprich die Branchenüblichkeit, an.

Das vom eingestellten Bewerber geäußerte grundsätzliche Geheimhaltungsinteresse muss bei der Abwägung zurücktreten. So hatte der Bewerber bereits selbst Gehaltsvorstellungen mitgeteilt. Ihm musste bewusst sein, dass die Mitteilung von Gehaltsdaten zur Honorarberechnung branchenüblich ist. Zudem geht es nicht um aktuelle Gehaltsdaten, sondern diejenigen zum Zeitpunkt der Einstellung. Auch ist der Vermittler vertraglich zur Verschwiegenheit verpflichtet.

## §

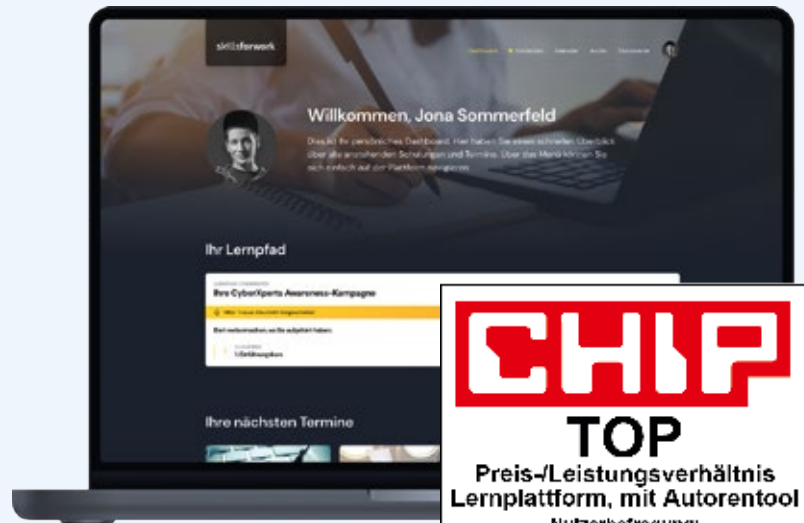
## Das können Sie aus dem Urteil folgern

**Auch Interessen eines Dritten können überwiegen und eine Übermittlung von personenbezogenen Daten rechtfertigen. Zudem führt ein Widerspruch eines Betroffenen nach Art. 21 DSGVO nicht automatisch dazu, dass Daten nicht übermittelt werden dürfen. Allerdings sind hier eine genaue Prüfung und Interessenabwägung erforderlich. Beides sollten Sie dokumentieren.**

# 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



Telefon: 02 28 95 50 150

Fax: 02 28 36 96 480

E-Mail: [kundendienst@privacyxperts.de](mailto:kundendienst@privacyxperts.de)

Internet: [www.privacyxperts.de](http://www.privacyxperts.de)

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

## Vorschau:

Neue Mitarbeiter: Ihre Tipps für Vorgesetzte

Urteil: Verschlüsselte E-Mails sind keine Pflicht