DATENSCHUTZAKTUELL

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

MAI 2026

Schweiz

THEMENHEFT:
Neue Mitarbeiter – Datenschutz von Anfang an

NEUE MITARBEITER: BETEILIGEN SIE SICH AM WILLKOMMENSTAG

Onlinebereich:
https://kurzlink.ch/onlinebereich

PRIVACYXPERTS

Sorgen Sie für Know-how

Liebe Leserin, lieber Leser,

der Mai steht vor der Tür. Und das ist ein klassischer Einstellungsmonat für neue Mitarbeiter. Ein solcher Start in die neue Tätigkeit oder ins Arbeitsleben ist mit viel Neuem und Unbekanntem verbunden.

Weil es jedoch dauert, bis man sich im neuen Unternehmen zurechtfindet und über alles Relevante Bescheid weiss, kann in der Zwischenzeit manches schiefgehen. Das gilt gerade für den Umgang mit Personendaten. Ihr Ziel sollte es also sein, die neuen Mitarbeiter schnellstens mit Know-how zu versorgen. Das hilft nicht nur dem Datenschutz. Es erspart Ihnen Arbeit und schont Ihre Nerven.

Viele Grüsse

Andreas Würtz,
Rechtsanwalt und Chefredakteur

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

Inhalt

Expertensprechstunde:
https://kurzlink.ch/kontakt-wuertz

Bildnachweise:
Titel: Adobe Stock | sirichai
Seite 1: Adobe Stock | fizkes

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

Redaktionelles Ausgabenmanagement:
Nicole Brockmann, Madrid

Satz: Deinzer Grafik, Gartow

Druck: Warlich Druck Meckenheim GmbH, Meckenheim

Erscheinungsweise: 16-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Dieses monothematische Supplement „Neue Mitarbeiter – Datenschutz von Anfang an" liegt der Ausgabe Mai 2026 von „Datenschutz aktuell Schweiz" bei.

Stellen Sie sich den Neuen gleich am ersten Tag vor.

Neue Mitarbeiter: Beteiligen Sie sich am Willkommenstag

Bestimmt setzt Ihr Unternehmen darauf, neuen Mitarbeitern einen guten und möglichst entspannten Start zu ermöglichen. Schliesslich ist niemandem gedient, wenn neue Mitarbeiter ratlos sind und mehr falsch als richtig machen. Vielleicht gibt es daher auch Willkommenstage für neue Mitarbeiter, um diesen alles Wichtige zu vermitteln. Das ist auch eine Chance für Sie und den Datenschutz.

Nutzen Sie die Gelegenheit

Das „Anbordnehmen" neuer Mitarbeiter, das sogenannte Onboarding, ist wichtig, damit sich neue Mitarbeiter schnell zurechtfinden und auch die wichtigsten Regeln kennen. Gibt es eine solche Veranstaltung in Ihrem Unternehmen und sind Sie bislang nicht vertreten, sollten Sie nicht lange überlegen, warum Sie das nicht sind. Viel schlauer ist es, dass Sie alles daransetzen, zukünftig mit von der Partie zu sein.

Dazu sollten Sie schnellstens mit der Personalabteilung sprechen. Machen Sie deutlich, dass gerade neue Mitarbeiter eine „Grundimpfung" im Datenschutz brauchen. Schliesslich kann man mit Personendaten viel falsch machen. Und das kann ziemlich viel Ärger verursachen und für das Unternehmen richtig teuer werden. Schlagen Sie den Kollegen vor, dass Sie in 30 bis 60 Minuten Grundlegendes vermitteln und so manchem Fehlverhalten vorbeugen können.

Gibt es für Sie keinen Platz mehr in der Agenda, sollten Sie nicht einfach unverrichteter Dinge von dannen ziehen. Bitten Sie darum, dass Ihre Informationen oder eine Präsentation in eine Willkommensmappe aufgenommen werden und dass am Willkommenstag auch kurz auf diesen Inhalt hingewiesen wird.

Gestalten Sie Ihre Information kurzweilig

Bedenken Sie stets: Halten Sie es kurz und knapp und beschränken Sie sich auf das Wesentliche. Insofern sollten Sie die Ihnen zur Verfügung stehende Redezeit geschickt verwenden, um erforderliches Wissen zu vermitteln. Nutzen Sie also keinen umfangreichen Foliensatz, bei dem Sie sich in datenschutzrechtlichen Details verlieren. Gerade neue Mitarbeiter werden hier schnell überfordert sein.

Daher: Schaffen Sie etwas Neues, etwa eine Präsentation im Frage-Antwort-Stil, eben eine etwas anders dargestellte Liste mit (von neuen Mitarbeitern) häufig gestellten Fragen. Dazu können Sie sich an der folgenden Checkliste orientieren. Dabei ist wichtig: Die neuen Mitarbeiter werden an diesem Tag mit Informationen überhäuft. Vermitteln Sie die Informationen also nicht nur auf der Tonspur. Geben Sie den Teilnehmern unbedingt etwas an die Hand, beispielsweise einen Ausdruck.

CHECKLISTE: Wichtige Themen für neue Mitarbeiter

Ihr Schwerpunkt	Das können Ihre Erläuterungen sein	Enthalten?
Was hat es mit dem Thema Datenschutz auf sich?	› Erklären Sie, dass Datenschutz grundrechtlichen Schutz geniesst. Jeder hat ein Recht auf Achtung seines Persönlichkeitsrechts und Schutz seiner Daten. › Zeigen Sie auf, was personenbezogene Daten sind. Hier kann es schnell Missverständnisse geben, die grosse Tragweite haben. So wird beispielsweise die persönliche E-Mail-Adresse oder die User-ID im Unternehmen gerne als „nicht personenbezogen" gesehen. › Erklären Sie allenfalls kurz, worum es im Bundesgesetz über den Datenschutz (DSG) geht. Im Bedarfsfall können Sie beispielsweise auf die Grundsätze der Bearbeitung in Art. 6 DSG eingehen.	☐ Ja ☐ Nein

CHECKLISTE: Wichtige Themen für neue Mitarbeiter

Ihr Schwerpunkt	Das können Ihre Erläuterungen sein	Enthalten?
Warum ist Datenschutz für unser Unternehmen wichtig?	› Vermitteln Sie, dass es nicht nur um die Einhaltung gesetzlicher Pflichten geht, sondern vielmehr darum, beispielsweise Kundeninteressen ernst zu nehmen. Diesen liegt viel daran, dass ihre Daten bei Ihrem Unternehmen in guten Händen sind. › Erwähnen Sie, dass Patzer beim Datenschutz zu einem grösseren Geschäftsrisiko werden können. Neben Imageschäden drohen Umsatzrückgang und Bussgelder.	☐ Ja ☐ Nein
Welche Vorteile bringt es, wenn jeder auf Datenschutz achtet?	› Jeder Mitarbeiter trägt dazu bei, dass Datenschutz insgesamt funktioniert. › In seinem Zuständigkeitsbereich kann jeder Mitarbeiter relevante Entscheidungen treffen oder vorbereiten, die gut für den Datenschutz sind.	☐ Ja ☐ Nein
Welche Datenschutzmassnahmen gibt es im Unternehmen?	› Erläutern Sie grob, was Ihr Unternehmen macht. Dazu zählen beispielsweise die Datenschutzstrategie, die Regelwerke und natürlich Sie als Berater und Kontrollinstanz. › Sie können auch auf verschiedene technische und organisatorische Massnahmen eingehen, die für neue Mitarbeiter von Relevanz sein können, etwa die Massnahmen zur Abwehr von Cyberkriminellen.	☐ Ja ☐ Nein
Welche Pflichten hat man als Mitarbeiter?	› Jeder Mitarbeiter muss darauf achten, dass er bei seiner Arbeit die Vorgaben zum Datenschutz einhält. › Machen Sie deutlich: Jeden Mitarbeiter trifft eine Schadensabwendungspflicht als Nebenpflicht aus dem Arbeitsvertrag. Insofern muss er auch drohende Gefahren melden und Schaden abwenden helfen. Das gilt auch für den Datenschutz.	☐ Ja ☐ Nein
Welche Regelwerke sind für Mitarbeiter besonders wichtig?	› Geben Sie einen Überblick über die internen Vorschriften. So z. B. Richtlinien und Arbeitsanweisungen mit Datenschutzbezug. › Gehen Sie auch auf datenschutzrelevante Prozesse ein, die für die Mitarbeiter von Relevanz sind. So z. B. zur Bearbeitung von Betroffenenanfragen. › Gibt es eine schriftliche Verpflichtung zum Datenschutz der neuen Mitarbeiter, können Sie hier die Aspekte praxisnah erläutern.	☐ Ja ☐ Nein
Welche Folgen können Datenschutzverstösse haben?	› Suchen Sie in Medien nach einigen aktuellen Schlagzeilen zu Datenschutzverstössen und deren finanziellen Folgen. Das macht klar, dass Sie in Sachen Bussgeld niemandem „etwas vom Pferd erzählen". › Verdeutlichen Sie, dass Datenschutzverstösse ernste Konsequenzen für das Unternehmen haben können. Vor allem kann es zu Bussgeldern kommen. Weisen Sie auf Art. 60 und Art. 61 DSG hin. Auch wenn es nicht so teuer wie in der EU wird: Geld ist Geld. › Erklären Sie, dass auch Pannen anderswo zum Datenschutzproblem werden und erhebliche Konsequenzen nach sich ziehen können. Etwa Fehler bei der IT-Sicherheit können zum unbefugten Zugriff auf personenbezogene Daten führen. Das wäre nicht nur dem EDÖB zu melden, eventuell wären auch die Betroffenen zu informieren. Das kann auch zu einem Bussgeld führen. › Natürlich sind Verstösse schlecht für das Image und den Umsatz, wenn etwa Medien darüber berichten.	☐ Ja ☐ Nein
Was kann einem als Mitarbeiter passieren?	› Generell kann es arbeitsrechtliche Konsequenzen haben. Neben Abmahnungen droht gerade in schlimmen Fällen die Kündigung. › Daneben gilt: Entsteht dem Unternehmen ein Schaden, der auf ein Fehlverhalten des Mitarbeiters zurückgeht, kann der Mitarbeiter unter Umständen den Schaden ersetzen müssen.	☐ Ja ☐ Nein
Worauf sollte man als Mitarbeiter ganz besonders achten?	› Geben Sie einen Überblick über besonders relevante Herausforderungen und Szenarien, denen sich gerade neue Mitarbeiter stellen müssen. › Nehmen Sie auch aktuelle oder besonders risikoträchtige Themen auf. So z. B. wie man Phishing-E-Mails erkennt und was man in einem solchen Fall macht.	☐ Ja ☐ Nein
Wie geht man richtig mit Vorfällen um?	› Machen Sie klar: Wo Menschen arbeiten, können auch Fehler passieren. Allerdings müssen zügig die nötigen Schritte eingeleitet werden, damit kein grösserer Schaden entsteht. › Zeigen Sie das richtige Vorgehen an typischen Alltagssituationen auf. Das erleichtert es den Mitarbeitern, in einer entsprechenden Situation sich an das Gesagte zu erinnern.	☐ Ja ☐ Nein
An wen kann man sich mit Fragen wenden?	› Erklären Sie deutlich: Peinliche oder blöde Fragen gibt es nicht. Gerade für neue Mitarbeiter ist vieles zum richtigen Verhalten unklar. › Erläutern Sie, dass man sich bei Fragen zum Datenschutz zunächst an den Vorgesetzten oder eine zuständige Fachabteilung wenden kann. Aber auch der Datenschutzberater ist gern Ansprechpartner.	☐ Ja ☐ Nein
Wo findet man was?	› Das kann eine Liste mit Links zu wichtigen Themen sein. Bauen Sie diese als Schlagwortregister von A bis Z auf und erklären Sie, wo man was finden kann. › Probieren Sie alle aufgenommenen Links aus. Tote Links sorgen nicht nur für Frust. Sie können auch falsches Verhalten oder falsche Entscheidungen fördern.	☐ Ja ☐ Nein

Neue Mitarbeiter als Phishing-Opfer? Beugen Sie ruckzuck vor

Phishing ist das beliebteste Einfallstor für Cyberkriminelle und das diesbezügliche Risiko Nummer eins für Unternehmen. Gerade bei neuen Mitarbeitern ist die Gefahr besonders gross, dass sie den Kriminellen auf den Leim gehen und das Geforderte machen, sensible Daten preisgeben oder gar Ransomware installieren. Passiert das, ist die Datenschutzpanne nicht weit. Grund genug für Sie, frühestmöglich zu sensibilisieren.

Wie wäre es mit einem Merkblatt?

Um gut zu sensibilisieren, können Sie auf Schulungen setzen. Doch manchmal ist das einfach nicht drin, etwa weil Sie nicht für jeden neuen Mitarbeiter eine Schulung durchführen können. Doch warten und darauf vertrauen, dass vielleicht Vorgesetzte die nötigen Tipps und Hinweise geben, kann auch schiefgehen. Weil jeder potenzielles Opfer sein kann, sollten Sie etwa mit einem Merkblatt für das nötige Wissen bei neuen Mitarbeitern sorgen. Das macht sich gut in einer Willkommensmappe oder als Ausdruck am Arbeitsplatz des neuen Mitarbeiters.

MUSTER: Merkblatt zu technisch-organisatorischen Schutzmassnahmen

Merkblatt Phishing

Machen Sie Cyberkriminellen das Leben schwer
Unser Unternehmen sitzt auf einem Schatz, und zwar auf seinen Daten. Dabei handelt es sich um geschäftliche Informationen wie auch personenbezogene Daten, etwa von Kunden und Beschäftigten. Auf diese Daten haben es Cyberkriminelle abgesehen. Schliesslich lassen sich Daten schnell zu Geld machen, etwa im Darknet. Auch Lösegelderpressungen sind an der Tagesordnung. Damit Cyberkriminelle kein leichtes Spiel haben, sind auch Sie gefragt! Lesen Sie dieses Merkblatt aufmerksam durch und handeln Sie entsprechend. Damit leisten Sie einen wichtigen Beitrag, damit unser Unternehmen und seine Daten sicher sind.

Was ist Phishing?
Cyberkriminelle geben sich beispielsweise als Vertrauenspersonen, Vorgesetzte oder vertrauenswürdige Unternehmen aus. Sie verschicken gefälschte E-Mails, die zunehmend täuschend echt wirken. Neben E-Mails werden auch andere Kommunikationsmittel genutzt, etwa SMS, Messengerdienste oder auch soziale Netzwerke.

Worauf zielen Cyberkriminelle ab?
Cyberkriminelle wollen an sensible Daten, beispielsweise Passwörter, Bankdaten, schützenswerte Informationen. Daneben wird auch versucht, das Opfer zu Zahlungen zu veranlassen, etwa mit gefälschten Rechnungen oder ausgetauschten Bankinformationen. Zudem wird versucht, Schadprogramme einzuschleusen, z. B. Ransomware. Damit werden Datenbestände verschlüsselt, um Lösegeld für das Entschlüsseln der Daten zu erpressen. Manchmal geht es auch um den Diebstahl der digitalen Identität des Opfers, um dieses zu erpressen oder mit der gestohlenen Identität Straftaten begehen zu können.

Wie kann man Phishing erkennen?
Sie sollten besonders misstrauisch sein und alle Alarmglocken müssen schrillen, wenn

- Sie jemand Unbekanntes von ausserhalb des Unternehmens anschreibt und das, obwohl Sie mit dem betreffenden Unternehmen eigentlich nichts zu tun haben,
- die E-Mail-Adresse etwa bei der Domain Fehler aufweist und nicht dem Original entspricht (z. B. mueller@f1rma.xyz anstatt mueller@firma.xyz),
- die Anrede unpassend oder unpersönlich ist,
- der Inhalt nicht zum Anlass passt,
- es Unstimmigkeiten oder Fehler bei Schriftart, Aufbau, Satzbau und Rechtschreibung gibt,
- Zeitdruck aufgebaut wird (z. B., dass ein Account gesperrt wird, wenn nicht sofort reagiert wird),
- mit Ärger oder Problemen gedroht wird (z. B. Anzeige bei der Staatsanwaltschaft, Strafzahlung),
- Sie die Sache absolut geheim halten sollen (Sie sollen niemandem im Unternehmen davon erzählen dürfen),
- sensible Informationen erfragt werden (z. B. die Aufforderung, das Passwort zu aktualisieren).

Wie verhalte ich mich richtig?
Ist eine E-Mail, SMS oder Messengernachricht verdächtig, müssen Sie Folgendes tun:

- Lassen Sie sich nicht verunsichern und überstürzen Sie nichts.
- Klicken Sie nicht auf enthaltene Links. Schauen Sie sich unbedingt die Adresse an, die hinter dem Link steckt. Ist das nicht möglich, ist Klicken verboten!
- Öffnen Sie keine enthaltenen Anhänge (z. B. Rechnungen, Programme, Office-Dokumente). Diese können Schadprogramme enthalten.
- Installieren Sie nichts, auch wenn Sie dazu aufgefordert werden. Brechen Sie eine Installation ab. Geht das nicht, kontaktieren Sie sofort das Cybersecurity-Team.
- Fragen Sie Kollegen, Ihren Vorgesetzten oder den Datenschutzberater, bevor Sie das Geforderte umsetzen.
- Leiten Sie die E-Mail nicht an Kollegen weiter. Das schafft unnötig zusätzliche Risiken.
- Melden Sie Ihren Verdacht unverzüglich den Kollegen vom Cybersecurity-Team. Diese sagen Ihnen, wie es weitergeht.

Was mache ich, wenn es dann doch passiert ist?
Haben Sie eine Nachricht falsch eingeschätzt oder auf einen Anhang geklickt? Dann heisst es: Nicht warten! Melden Sie die Sache sofort dem Cybersecurity-Team und dem Datenschutzberater. Diese entscheiden über die nächsten Schritte. Ihr schnelles Handeln ist entscheidend, damit kein grösserer Schaden entsteht.

Wie kann ich wen erreichen?

- Cybersecurity-Team:
  cyber@musterfirma.xyz, +41 1234 5678999 (rund um die Uhr)
- Datenschutzberater:
  Ben Zinka-Nister, **dsb@musterfirma.xyz,** +41 1234 5678900

Informieren Sie schnell, aber umfassend, damit sich die Neuen richtig verhalten

Neue Mitarbeiter im Unternehmen sind ein Risiko. Auch wenn sie sich bemühen, wissen sie unter Umständen nur wenig, worauf es im Datenschutz ankommt. Beugen Sie Patzern und Pannen vor, indem Sie die neuen Mitarbeiter mit dem nötigen Grundlagenwissen versorgen.

Es muss nicht immer gleich eine Schulung sein

Gerade wenn neue Mitarbeiter vereinzelt ihre Arbeit in Ihrem Unternehmen aufnehmen, ist klar: Sie können nicht für jeden eine Einzelschulung durchführen. Doch gar nicht sensibilisieren ist auch keine Option. Wie wäre es also mit einem Willkommensschreiben?

MUSTER: Willkommensschreiben für neue Mitarbeiter

Machen Sie mit beim Datenschutz

Liebe Mitarbeiterin, lieber Mitarbeiter,

auch ich als Datenschutzberater möchte Sie ganz herzlich in unserem Unternehmen willkommen heissen. Es ist schön, Sie mit an Bord zu haben. Als Ihr Datenschutzberater möchte ich Ihnen schon jetzt zeigen, dass der richtige Umgang mit Personendaten nicht nur eine gesetzliche Pflicht ist. Für uns alle im Unternehmen ist Datenschutz eine wahre Herzensangelegenheit.

Warum ist Datenschutz bei uns so wichtig?
Einerseits bringt es unsere Geschäftstätigkeit mit sich, dass wir viel mit persönlichen Informationen unserer Kunden zu tun haben. Neben Kunden vertrauen uns auch Geschäftspartner und Mitarbeiter, dass sorgsam mit ihren Personendaten umgegangen wird. Dieses Vertrauen dürfen wir nicht enttäuschen. Schliesslich ist Vertrauen die Basis für gute Geschäfte und langfristigen Erfolg. Andererseits sind in der heutigen Zeit Daten ein Schatz, den wir schützen und verteidigen müssen. Wir können nie sicher sein, dass nicht auch Cyberkriminelle es auf uns und unseren Datenschatz abgesehen haben. Umso wichtiger ist, dass wir alles unternehmen, um jedem das Leben schwer zu machen, der unser Unternehmen schädigen will.

Sie sind wichtig!
Eins leuchtet schnell ein: Datenschutz kann nur funktionieren, wenn alle mitmachen und an einem Strang ziehen. Jeder, auch Sie, trägt dazu bei, dass wir mit den uns anvertrauten Daten sicher und verantwortungsvoll umgehen. Insofern sind auch Sie als Mitarbeiter Datenschützer für Ihren Verantwortungsbereich. Deshalb ist wichtig: Gehen Sie sorgsam mit Personendaten um. Beachten Sie gesetzliche wie interne Vorgaben. Beherzigen Sie die in der folgenden Übersicht zusammengestellten Punkte. Diese helfen Ihnen, die wichtigsten Datenschutzaspekte am Arbeitsplatz im Blick zu behalten. Machen Sie regelmässig auch den Check. Prüfen Sie ab und an, ob Sie alles Relevante umsetzen.

Übrigens: Ich bin für Sie da
Gerade weil für Sie vieles noch neu ist, liegt es auf der Hand, dass hier und da Fragen aufkommen. Haben Sie Fragen zum Datenschutz oder sind Sie sich unsicher, wie Sie mit einer Situation umgehen sollen oder wie Sie sich richtig verhalten sollen? Dann warten Sie nicht lange. Rufen Sie mich an oder schicken Sie mir eine E-Mail.

Ihr Franz Ose,
Datenschutzberater

Bitte halten Sie sich an Folgendes	Das sollten Sie dazu noch wissen	Setzen Sie das um?
Beachten Sie die geltenden Regeln	› Wie mit Personendaten umgegangen werden darf, ergibt sich einerseits aus Gesetzen, beispielsweise dem Bundesgesetz über den Datenschutz (DSG). Andererseits gibt es bei uns zahlreiche interne Richtlinien, Arbeitsanweisungen und Prozesse, die Sie einhalten müssen. › Alle internen Vorschriften finden Sie im Intranet im Vorschriftenverzeichnis. Geben Sie dort „Datenschutz“ ein und Sie finden die Arbeitsanweisungen zur Datenschutzorganisation und zum Datenschutz.	☐ Ja ☐ Nein
Handeln Sie nie unüberlegt	› Wenn Sie Entscheidungen im Zusammenhang mit Personendaten treffen müssen, sollten Sie sich nie unter Druck setzen lassen oder unüberlegt vorgehen. Das kann zu Fehlern führen, die besonders im Datenschutz zu grossen Problemen führen können. › Gerade bei Unsicherheiten treffen Sie lieber zunächst keine Entscheidung und klären alles Relevante mit Kollegen, Vorgesetzten oder anderen zuständigen Stellen. Bei Personendaten ist auch der Datenschutzberater eine gute Anlaufstelle.	☐ Ja ☐ Nein

Bitte halten Sie sich an Folgendes	Das sollten Sie dazu noch wissen	Setzen Sie das um?
Achten Sie auf Clean Desk an Ihrem Arbeitsplatz	› Lassen Sie keine Personendaten oder vertraulichen Dokumente offen herumliegen, sodass Unbefugte Kenntnis nehmen können. Das gilt gerade dann, wenn Sie abwesend sind. › Packen Sie alles Schützenswerte bei Abwesenheit in verschliessbare Schränke oder Schubladen. Zum Schützenswerten gehört auch alles, was Daten speichern kann. So z. B. Ihr Smartphone oder ein USB-Stick. › Erschweren Sie die zufällige Kenntnisnahme durch Unbefugte, etwa durch vorbeilaufende Besucher. Decken Sie Unterlagen ab, wenn Sie nicht damit arbeiten.	☐ Ja ☐ Nein
Sperren Sie Ihren Computer bei jeder Abwesenheit	› Verlassen Sie Ihren Arbeitsplatz – auch nur vorübergehend für den Gang zur Toilette –, dann sperren Sie den Computer. Das geht ganz einfach: Drücken Sie die Windows-Taste und L. › Achten Sie auch darauf, dass Sie Smartphone & Co. sperren, wenn Sie abwesend sind. So vermeiden Sie eine unbefugte Nutzung.	☐ Ja ☐ Nein
Wahren Sie die Vertraulichkeit bei Gesprächen	› Unter Umständen tauschen Sie in Gesprächen oder virtuellen Konferenzen Schützenswertes aus, das nicht für jedermanns Ohren bestimmt ist. Suchen Sie sich für solche Gespräche einen Ort, an dem Sie die Vertraulichkeit leicht gewährleisten können. › Ist kein entsprechender Ort verfügbar, achten Sie darauf, dass Sie anstatt einer Freisprecheinrichtung ein Headset nutzen und personenbezogene Informationen vermeiden.	☐ Ja ☐ Nein
Setzen Sie auf das Minimalprinzip	› Machen Sie dieses Grundprinzip zum Standard im Zusammenhang mit personenbezogenen Daten. Egal, ob es um den Umfang der Bearbeitung, Berechtigungen oder Auswertungsmöglichkeiten geht. Es gilt: so wenig wie möglich und so viel wie für den Zweck oder die Aufgabe erforderlich. › Sind Sie sich unschlüssig, ob Sie bei der Umsetzung des Minimalprinzips richtigliegen, sprechen Sie mit Kollegen und Vorgesetzten.	☐ Ja ☐ Nein
Nutzen Sie nur die Technik, die Ihnen vom Unternehmen bereitgestellt wurde	› Beim Bearbeiten von Personendaten hat Sicherheit höchste Priorität. Daher dürfen Sie nur diejenigen Geräte für das Bearbeiten von Personendaten nutzen, die Ihnen hierfür zur Verfügung gestellt worden sind. › Nichts anderes gilt für Software. Benötigen Sie etwas ausserhalb der üblichen Standardsoftware, sprechen Sie hierzu mit Ihrem Vorgesetzten. Ist etwas anderes erforderlich, übernimmt alles Weitere die IT-Abteilung.	☐ Ja ☐ Nein
Achten Sie auf eine sichere Entsorgung	› Legen Sie grössten Wert darauf, jegliche Datenträger (z. B. auch Dokumente, Briefe, Ausdrucke) richtig zu entsorgen. Nur so ist sichergestellt, dass auch hierbei der Datenschutz gewährleistet ist. Informationen zum richtigen Entsorgen finden Sie an jedem Drucker. Dort erfahren Sie auch, wo Sie die nächstgelegene Entsorgungsstation finden. › Sind Sie sich unsicher, wie Sie etwas richtig entsorgen können, sprechen Sie mit Ihren Kollegen und Vorgesetzten. Verbleiben Zweifel, können Sie auch den Datenschutzberater ansprechen.	☐ Ja ☐ Nein
Sorgen Sie für Datenschutz beim mobilen Arbeiten	› Arbeiten Sie unterwegs, etwa auf einer Tagung oder im Hotel, gelten die gleichen Rahmenbedingungen wie im Unternehmen. Achten Sie bei vertraulichen Telefonaten insbesondere darauf, dass niemand mithört. › Verlieren Sie beim Arbeiten unterwegs, etwa auch im Zug, Ihre Geräte und Unterlagen nie aus den Augen. Lassen Sie diese nicht zurück, auch wenn Sie nur kurz Ihren Platz verlassen. Nutzen Sie beim Arbeiten mit dem Notebook unterwegs eine Sichtschutzfilterfolie für den Bildschirm. › Auch im Homeoffice müssen Sie sicherstellen, dass der Datenschutz passt. Das gilt insbesondere für die Umsetzung von Clean Desk sowie das vertrauliche Führen von Gesprächen. Bedenken Sie auch: Das datenschutzkonforme Entsorgen ist auch hier unerlässlich.	☐ Ja ☐ Nein
Lassen Sie beim E-Mail-Versand Vorsicht walten	› Vor dem Versand von E-Mails sollten die Empfänger genau geprüft werden. Auch versehentlich ausgewählte Empfänger führen zu einem Datenschutzproblem. › Wenn Sie Vertrauliches oder Sensibles verschicken wollen, achten Sie auf die korrekte Wahl des Verteilers und das richtige Platzieren der Empfänger. Ist es nicht in Ordnung, wenn die Empfänger voneinander erfahren, sollten Sie unbedingt das Bcc-Adressfeld nutzen.	☐ Ja ☐ Nein
Setzen Sie auf sichere Passwörter	› Setzen Sie auf starke Passwörter, die möglichst komplex und nur schwer zu erraten oder zu erschliessen sind. Am besten nutzen Sie hierfür den im Passwortmanager enthaltenen Generator. › Jedes Passwort sollte ein Unikat sein. Das heisst, Sie verwenden kein Passwort zweimal. › Für das sichere Aufbewahren nutzen Sie ausschliesslich den Passwortmanager.	☐ Ja ☐ Nein
Fragen Sie in Zweifelsfällen nach	› Es kann immer zu Situationen kommen, in denen Sie sich unsicher sind, wie Sie sich richtig verhalten sollen. Treffen Sie hier keine Entscheidung nach dem Bauchgefühl. › Holen Sie sich Hilfe und Unterstützung bei der Entscheidungsfindung. Ihre ersten Anlaufpunkte sind Kollegen und Ihr Vorgesetzter.	☐ Ja ☐ Nein
Melden Sie Ungereimtheiten und Vorfälle	› Haben Sie den Verdacht, dass etwas im Zusammenhang mit Personendaten falschläuft oder dass es zu einer Panne gekommen ist, dürfen Sie nicht zögern. Melden Sie die Sache den zuständigen Kollegen bzw. Ihrem Vorgesetzten. › Auch wenn Sie etwas falsch gemacht haben, wird Ihnen niemand den Kopf abreissen. Fehler können passieren, sie verschweigen ist jedoch ein Problem.	☐ Ja ☐ Nein

Datenschutz von Anfang an: Holen Sie die Vorgesetzten mit ins Boot

Starten in Ihrem Unternehmen neue Mitarbeiter, geht das regelmässig damit einher, dass sie Vorgesetzte haben. Diese geben vor, welche Aufgaben der neue Mitarbeiter übernimmt und wie er diese zu erledigen hat. Hat der neue Mitarbeiter mit Personendaten zu tun, spielt auch der Datenschutz eine wichtige Rolle. Also muss das auch Thema für den Vorgesetzten sein.

Sie beraten und unterstützen

Als Datenschutzberater sind Sie in erster Linie Berater in allen Datenschutzfragen. Zum Beraten gehört es auch, dass Sie mögliche Risiken ausmachen und darauf hinwirken, dass diese Risiken reduziert werden. Und gerade neue Mitarbeiter stellen nicht unbedingt ein kleines Risiko für den richtigen Umgang mit Personendaten dar. Schnell werden Personendaten falsch bearbeitet oder es geht sonst etwas schief. Dem können auch Sie als Datenschutzberater vorbauen, indem Sie den Vorgesetzten eine Checkliste mit besonders relevanten Aspekten zur Verfügung stellen. Wird vor dem und am ersten Arbeitstag alles Datenschutzrelevante erledigt, ist schon viel gewonnen.

Leisten Sie Hilfe zur Selbsthilfe

Sprechen Sie mit der Personalabteilung. Dort werden meist die Aktivitäten rund um Neueinstellungen gesteuert. Dort könnte man bei einer Neueinstellung in der Information an den zukünftigen Vorgesetzten auch eine Checkliste aufnehmen. Inhaltlich können Sie sich an folgendem Muster orientieren. Ergänzen Sie diese, um weitere Punkte, die für Ihr Unternehmen bzw. für den Datenschutz von besonderer Bedeutung sind.

CHECKLISTE: To-dos für Vorgesetzte bei neuen Mitarbeitern

Das sind die wichtigsten To-dos	Achten Sie hierauf	Erledigt?
Im Vorfeld zum ersten Arbeitstag des Mitarbeiters erledigen		
Gefahren und Risiken ausmachen	› Wichtig ist, dass zunächst überlegt wird, was schiefgehen bzw. wo es zu Fehlern oder Fehlverhalten kommen kann. Die nicht abwegigen Gefahren sollten im Hinblick auf den denkbaren Schaden und die Eintrittswahrscheinlichkeit bewertet werden. Das sind dann die Risiken. Alle Risiken, die nicht als niedrig eingestuft werden, sollten behandelt werden. Hier gibt es verschiedene Möglichkeiten. So können Risiken mit technischen wie organisatorischen Massnahmen reduziert werden. › Die Risiken einfach hinnehmen und hoffen, dass alles gut geht, wäre eine ziemlich schlechte Idee. Bedenken Sie, dass auch Sie als Vorgesetzter Verantwortung tragen, beispielsweise für den sorgsamen Umgang mit Personendaten, aber auch mit der Pflicht zur Risikominimierung an sich. Schadensrisiken sehenden Auges einzugehen, kann auch für Sie zum Problem werden.	☐ Ja ☐ Nein
Massnahmen zur Risikobehandlung einleiten	› Haben Sie Massnahmen zur Risikoreduzierung ausgewählt, müssen diese auch tatsächlich umgesetzt werden. › Übertragen Sie diese Aufgaben anderen Mitarbeitern, sollten Sie gerade bei wichtigen Massnahmen die Umsetzung nachverfolgen. Bitten Sie um eine Bestätigung der Erledigung.	☐ Ja ☐ Nein
Berechtigungen vergeben und Minimalprinzip beachten	› Neue Mitarbeiter brauchen Berechtigungen, um auf Daten zugreifen oder mit Systemen arbeiten zu können. Achten Sie bereits bei der Vergabe auf das Minimalprinzip. Hinterfragen Sie stets, ob eine bestimmte Berechtigung für die konkrete Aufgabe tatsächlich erforderlich ist. › Stufen Sie die Berechtigungen ab und beschränken Sie diese zunächst nur auf das unbedingt Erforderliche. Die Berechtigungen können nach und nach erweitert werden.	☐ Ja ☐ Nein
Mitarbeiterausweis und Zutrittsberechtigungen beantragen	› Bei uns ist ein Mitarbeiterausweis mit Foto Pflicht. Daneben benötigt der neue Mitarbeiter auch die erforderlichen Zutrittsberechtigungen, aber auch nicht mehr. › Vereinbaren Sie frühzeitig einen Termin mit den Kollegen der Ausweisstelle und merken Sie für den neuen Mitarbeiter den entsprechenden Termin vor.	☐ Ja ☐ Nein
Erfahrenen Mitarbeiter als Ansprechpartner festlegen	› Das kann entscheidend sein, damit sich ein neuer Mitarbeiter schnell zurechtfindet. Schliesslich ist alles neu und es stellen sich viele Fragen. Eine Anlaufstelle für alles Unklare zu haben, beugt Fehlverhalten vor und schafft Sicherheit. › Je nachdem, wie sehr die Bearbeitung von Personendaten in Ihrer Abteilung eine Rolle spielt, sollte sich der Ansprechpartner auch im Datenschutz gut auskennen.	☐ Ja ☐ Nein
Relevante Datenschutzthemen zusammenstellen	› Bestehen in Ihrer Abteilung Besonderheiten zum Umgang mit Personendaten, sollten Sie die entsprechenden Informationen zusammenstellen. Hier kann eine Linkliste gute Dienste leisten. Noch besser ist es, wenn Sie Regelwerke als PDF in einer E-Mail oder in ausgedruckter Form bereitstellen können. › Verweisen Sie auch auf die Intranetseiten des Datenschutzberaters. Dort gibt es viele Informationen, die für jeden im Unternehmen von Bedeutung sind. Gerade neue Mitarbeiter sollten sich hier informieren.	☐ Ja ☐ Nein

CHECKLISTE: To-dos für Vorgesetzte bei neuen Mitarbeitern

Das sind die wichtigsten To-dos	Achten Sie hierauf	Erledigt?
Ersten Arbeitstag mit Ansprechpartner vorbereiten	› Überlegen Sie, wie der erste Arbeitstag ablaufen soll. Machen Sie eine entsprechende Agenda für den Tag. › Achten Sie darauf, dass der Ansprechpartner für den neuen Mitarbeiter verfügbar ist. › Erstellen Sie eine Erledigungsliste mit Aktivitäten für den neuen Mitarbeiter. Diese sollte direkt am ersten Arbeitstag abgearbeitet werden.	☐ Ja ☐ Nein
Den Mitarbeiter bei wichtigen Ansprechpartnern bekannt machen	› Unter Umständen wird der neue Mitarbeiter viel mit anderen Kollegen im Unternehmen zu tun haben. Hier ist es hilfreich, wenn diese vom neuen Mitarbeiter erfahren. So lässt sich auch vermeiden, dass diese die Zusammenarbeit ablehnen, weil ihnen der neue Mitarbeiter noch nicht bekannt ist. › Informieren Sie vor dem ersten Arbeitstag und stellen Sie in den ersten Arbeitstagen am besten den neuen Mitarbeiter persönlich bei den Kollegen vor. Das persönliche Kennenlernen macht vieles einfacher.	☐ Ja ☐ Nein
Arbeitsmittel und Technik bereitstellen sowie zuordnen	› Sorgen Sie dafür, dass der neue Mitarbeiter möglichst vom ersten Tag an arbeitsfähig ist und dass die Geräte in den Inventarlisten dem neuen Mitarbeiter zugeordnet sind. › Achten Sie darauf, dass Computer, Smartphone und sonstige Datenträger verschlüsselt sind. › Installieren Sie bereitstehende Aktualisierungen und Sicherheitsupdates.	☐ Ja ☐ Nein
Organigramme anpassen	› Ist der neue Mitarbeiter ins Organigramm aufzunehmen, geben Sie den zuständigen Kollegen die entsprechende Information. › Achten Sie darauf, dass nur erforderliche Informationen aufgenommen werden. Ein Foto des Mitarbeiters ist nicht zwingend notwendig, kann jedoch auf freiwilliger Basis aufgenommen werden.	☐ Ja ☐ Nein
Datenschutzwissen organisieren	› Hat der neue Mitarbeiter viel mit Personendaten zu tun, sollten Sie frühzeitig klären, welches Know-how im Datenschutz erforderlich ist. › Melden Sie den Mitarbeiter zu unseren internen Datenschutzschulungen an, die einmal im Quartal stattfinden. › Ist aus Ihrer Sicht ein Kennenlernen des Datenschutzberaters wichtig, vereinbaren Sie frühzeitig einen Termin.	☐ Ja ☐ Nein
To-dos, wenn der Mitarbeiter die Arbeit aufgenommen hat		
Schriftliche Verpflichtung zum Datenschutz vornehmen	› Die Verpflichtung zum Datenschutz und zur Wahrung der Vertraulichkeit ist Pflicht in unserem Unternehmen. › Lassen Sie am ersten Arbeitstag die Erklärung als eine der ersten Aufgaben erledigen. Leiten Sie ein Original an die Personalabteilung zwecks Aufnahme in die Personalakte weiter.	☐ Ja ☐ Nein
Datenschutz-Basics vermitteln	› Erläutern Sie dem neuen Mitarbeiter Grundlegendes. So z. B., was Personendaten sind und dass ein Bearbeiten nur im Rahmen des gesetzlich Zulässigen erlaubt ist. Es braucht eine Rechtsgrundlage. Auch der Schutz personenbezogener Daten ist wichtig. › Nutzen Sie für Ihre Information die Kurzpräsentation „Datenschutz für neue Mitarbeiter“. Diese enthält alle wichtigen Basics. › Stellen Sie dem neuen Mitarbeiter die Unterlagen zur Verfügung. Teilen Sie auch mit, dass er sich bei Fragen zum Datenschutz und zum richtigen Umgang mit Personendaten jederzeit an den Datenschutzberater wenden kann.	☐ Ja ☐ Nein
Auf richtiges Verhalten am Arbeitsplatz hinweisen	› Vermitteln Sie unbedingt, worauf am Arbeitsplatz zu achten ist. Heben Sie die Bedeutung von Clean Desk und Clear Screen hervor: Bei Abwesenheit ist Schützenswertes sicher zu verstauen und der Computer zu sperren. › Weisen Sie auf Besonderheiten in Ihrer Abteilung hin, etwa worauf speziell zu achten ist.	☐ Ja ☐ Nein
Datenschutzkonformes Entsorgen erklären	› Auch in der heutigen Zeit gibt es noch fehlerhafte Ausdrucke, Briefe oder Schmierzettel. Diese können personenbezogene Daten und sensible (Geschäfts-)Informationen enthalten. Umso wichtiger ist, dass Sie für das richtige und sichere Entsorgen sensibilisieren. › Machen Sie bei einem Abteilungsrundgang auch einen Abstecher dorthin, wo man Sensibles entsorgen kann. Zeigen Sie, was wo wie zu entsorgen ist, bleibt kein Raum für Fehler.	☐ Ja ☐ Nein
Für Risiken durch Cyberkriminelle sensibilisieren	› Gehen Sie mit dem neuen Mitarbeiter die typischen Gefahren in Ihrem Bereich durch. Zeigen Sie auf, wie man etwa eine Phishing-E-Mail erkennt und wie man bei einer solchen richtig reagiert. › Machen Sie deutlich, dass entscheidend ist, dass der Mitarbeiter bei Unklarheiten und Unsicherheiten Sie oder seinen Ansprechpartner kontaktieren muss.	☐ Ja ☐ Nein
Notwendige Erledigungen für den Mitarbeiter zusammenstellen	› Stellen Sie zusammen, was der Mitarbeiter am ersten Arbeitstag noch zu erledigen hat. › Geben Sie dem Mitarbeiter am besten eine Checkliste an die Hand oder schicken Sie ihm eine Liste per E-Mail. Bitten Sie darum, die Erledigung zu bestätigen.	☐ Ja ☐ Nein
Eintrittscheckliste abarbeiten	› Arbeiten Sie die verschiedenen Punkte auf der Eintrittscheckliste der Personalabteilung ab. › Leiten Sie die bearbeitete Liste an die Personalabteilung weiter.	☐ Ja ☐ Nein

Verpflichtung zum Datenschutz: Das kann Ihre Vorlage sein

Nehmen neue Mitarbeiter ihre Tätigkeit in Ihrem Unternehmen auf, ist diesen unter Umständen noch nicht bekannt, worauf es beim Datenschutz ankommt. Um hier direkt am ersten Arbeitstag auf wichtige Regeln hinzuweisen, setzen viele Unternehmen auf eine schriftliche Verpflichtung der neuen Mitarbeiter.

Stellen Sie die Grundprinzipien in den Fokus

Die Verpflichtung soll den neuen Mitarbeitern die Regeln im Datenschutz klarmachen. Zugleich ist eine schriftliche Verpflichtung ein Nachweis für eine organisatorische Massnahme zur Umsetzung des Bundesgesetzes über den Datenschutz (DSG). Inhaltlich ist es am besten, wenn Sie auf die Grundsätze aus Art. 6 DSG abstellen. Dabei ist wichtig: Halten Sie die Inhalte möglichst allgemein, vermeiden Sie etwa Ausführungen zu speziellen Bearbeitungen oder zur künstlichen Intelligenz. Schliesslich soll die Verpflichtungserklärung inhaltlich auch in vielen Jahren noch passen.

MUSTER: Schriftliche Verpflichtung zum Datenschutz

Verpflichtung zum Datenschutz und zur Wahrung von Geschäftsgeheimnissen

Datenschutz ist bei der Musterfirma XYZ GmbH nicht nur ein rechtliches Muss. Vielmehr ist der sorgsame Umgang mit personenbezogenen Daten Teil unserer Unternehmenskultur. Als Mitarbeiter tragen auch Sie dazu bei, dass alle Daten geschützt sind, egal, ob sie Kunden, Mitarbeiter oder unsere Geschäftstätigkeit an sich betreffen. Wir gehen bei der Musterfirma XYZ GmbH verantwortungsvoll mit den uns anvertrauten Daten um. Jeder hat die Aufgabe, dieses Vertrauen gegenüber allen Betroffenen zu rechtfertigen, und zwar jeden Tag bei allem, was wir tun. Bitte halten Sie sich daher an Folgendes:

Bearbeitung nur mit Erlaubnis
Es ist Ihnen ausnahmslos untersagt, Personendaten ohne eine entsprechende Rechtsgrundlage zu bearbeiten. Dabei gelten als personenbezogene Daten alle Informationen, die sich einer Person zuordnen lassen, also beispielsweise Name, Adresse, E-Mail-Adresse, User-ID, Kundeninformationen oder Beschäftigtendaten. Unter Bearbeiten fallen alle Aktivitäten im Zusammenhang mit Personendaten. Das heisst insbesondere: das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Bereitstellen, Abgleichen, Verknüpfen, Einschränken, Löschen oder Vernichten.

Sie sind zu Folgendem verpflichtet:

1. Wahrung fundamentaler Datenschutzgrundsätze

› Rechtmässigkeit, Bearbeitung nach Treu und Glauben, Transparenz
Für jede Bearbeitung von Personendaten bedarf es einer Erlaubnis oder Rechtfertigung, der sogenannten Rechtsgrundlage. Diese kann sich aus dem Bundesgesetz über den Datenschutz und der dazugehörigen Verordnung, anderen Gesetzen oder betreiblichen Reglements ergeben. Dabei muss die Bearbeitung fair und transparent erfolgen. Es müssen die Interessen Betroffener berücksichtigt werden und sie müssen wissen, was mit ihren Daten geschieht.

› Zweckbindung
Personendaten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Diese Zwecke müssen schon bei der Erhebung klar definiert sein. Eine Weiterbearbeitung für andere, nicht vereinbarte Zwecke ist grundsätzlich unzulässig.

› Datenminimierung
Halten Sie sich an das Prinzip: so wenig wie möglich, so viel wie nötig. Die bearbeiteten Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zweckerreichung notwendige Mass beschränkt sein.

› Richtigkeit
Personendatenn müssen sachlich richtig und aktuell sein. Unrichtige Daten müssen unverzüglich berichtigt oder gelöscht werden. Auch Sie tragen Mitverantwortung dafür, dass offensichtliche Fehler korrigiert und Personendaten auf dem neuesten Stand gehalten werden.

› Speicherbegrenzung
Personendaten dürfen nur so lange gespeichert werden, wie es für den ursprünglichen Zweck erforderlich ist. Ist der Zweck erreicht oder nicht mehr relevant, müssen die Daten gelöscht werden, wenn nicht andere Pflichten (z. B. gesetzliche Aufbewahrungspflichten) dem entgegenstehen.

› Integrität und Vertraulichkeit
Personendaten müssen durch angemessene technische und organisatorische Massnahmen vor unbefugtem Zugriff, Verlust, Zerstörung oder Beschädigung geschützt werden. Sie sind verpflichtet, alle verfügbaren Schutzmassnahmen zu nutzen, auf verdächtige Aktivitäten zu achten und diese zu melden.

2. Schutz von Geschäftsgeheimnissen
Alle Informationen über unsere Geschäftstätigkeit, Organisationsstrukturen, Produktionsverfahren, wirtschaftliche Kennzahlen, Kundendaten oder interne Abläufe sind als Geschäftsgeheimnisse zu behandeln. Solche Informationen dürfen Sie nicht an unbefugte Personen weitergeben – auch nicht im privaten Umfeld oder in sozialen Netzwerken.

Ihre Bestätigung
Mit Ihrer Unterschrift bestätigen Sie, dass Sie die oben dargestellten Pflichten verstanden haben und einhalten werden. Sie sind sich bewusst, dass Ihre Pflicht zur Wahrung des Datenschutzes und zum Schutz von Geschäftsgeheimnissen auch über das Ende Ihrer Tätigkeit fortbesteht.

_____
(Ort, Datum, Unterschrift)

IHR NEUER ONLINEBEREICH IST DA!

JEDERZEIT VON ALLEN GERÄTEN AUF ARBEITSHILFEN ZUGREIFEN. **JETZT ANMELDEN!**

Videos: Monatliche Live-Webinare

Hier finden Sie alle Aufzeichnungen der bereits erschienenen Webinare und und erhalten ebenfalls Ihre Teilnahmeurkunde.

Arbeitshilfen: Muster, Vorlagen, Checklisten

In jeder Ausgabe weisen wir auf Arbeitshilfen zum Download hin. Diese finden Sie hier bequem per Schlagwortsuche. Mit diesen praktischen Lösungen arbeiten Sie schneller und fehlerfrei.

Archiv: Ihre Ausgaben

Digital und auf allen Geräten können Sie auf die bisher erschienenen Ausgaben bequem zugreifen – nichts geht verloren!

Newsfeed: Aktuelle Beiträge

Bleiben Sie stets über aktuelle Themen und wichtige Änderungen im Arbeitsschutz informiert.

Jetzt über 500 Vorlagen und Checklisten nutzen:

www.privacyxperts.de

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 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
Deutschland