



Datenschutz trifft Arbeitssicherheit

Wichtige Informationen und Tipps für Ihren Arbeitsalltag

Wissen kompakt



powered by



SAFETYXPERTS

Ihre Spezialisten für Arbeitssicherheit

Die Autoren



[AH] Andreas Hessel ist als Chief Information Security Officer langjähriger Leiter des Bereichs Informationssicherheit und Risikomanagement einer Landesbank. Daneben arbeitet er als externer Datenschutzbeauftragter und Berater im Bereich Cybersecurity.



[AW] Andreas Würtz, ist Rechtsanwalt und Chefredakteur von „Datenschutz aktuell“. Er verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.



[RW] Ricarda Waldon ist selbstständige Beraterin und Auditorin sowie im Qualitätsmanagement und Arbeitsschutz tätig. Sie ist zudem Teil des Redaktionsteams von „Arbeitssicherheit und Hygiene im Gesundheitswesen“.

Unterweisungen im Arbeitsschutz – welche Formen sinnvoll sind	5
Mitarbeitersensibilisierung: Datenschutz als Bestandteil der Unterweisung	6
Homeoffice und mobiles Arbeiten – was Arbeitgeber beachten müssen	7
Datenschutz im Arbeitsschutzalltag	9
Die 9 effektivsten Tipps für Video-Meetings	10
Datenverarbeitung: Was müssen Sie dabei beachten?	11
Sicherheitslösungen datenschutzkonform gestalten	12
Digitaler Arbeitsschutz: Datenschutz bei Wearables und Sensorik	13
Checkliste: DSGVO & Arbeitsschutz im Einklang	14
Informationssicherheit im Arbeitsalltag – ein Handout für Mitarbeiter	15
Clean Desk: Was heißt das im Home-Office?	16
Handout: Informationssicherheit im Arbeitsalltag	17
Fazit: Arbeitsschutz und Datenschutz gehören zusammen	18



Axel Hessel
Chief Information
Security Officer

Warum der Datenschutz den Arbeitsschutz berührt

Liebe Leserinnen, liebe Leser

Arbeitsschutz bedeutet längst nicht mehr nur Helm auf, Warnweste an und die Leiter richtig aufstellen. Der moderne Arbeitsschutz findet auch auf dem Bildschirm, im E-Mail-Postfach und in den Serverräumen statt. Denn überall dort, wo Daten über Mitarbeiter verarbeitet werden, spielt der Datenschutz eine zentrale Rolle.

Denken Sie an Unfallberichte, Gefährdungsbeurteilungen oder die digitale Zutrittskontrolle. Hier geht es nicht nur darum, die Gesundheit und Sicherheit der Beschäftigten zu gewährleisten, sondern auch ihre persönlichen Informationen zu schützen. Arbeitsschutz und Datenschutz greifen ineinander wie Zahnräder – und nur wenn beide rund laufen, funktioniert das ganze System.

Vielleicht haben Sie schon einmal erlebt, wie schnell Datenschutz im Alltag übersehen wird. Ein Attest liegt offen auf dem Schreibtisch, eine Zutrittsliste hängt im Pausenraum, oder die Unterweisung wird per Rundmail verschickt – mit allen Teilnehmern im offenen Verteiler. Genau hier liegt Ihre Chance: Sie können Datenschutz nicht nur als Pflicht begreifen, sondern als Teil einer Sicherheitskultur, die Vertrauen schafft.

Unsere Broschüre zeigt Ihnen, wie Sie Datenschutz und Arbeitsschutz zusammendenken und in der Praxis umsetzen können. Von der richtigen Handhabung von Mitarbeiterdaten über den Einsatz moderner Sicherheitslösungen bis hin zu sensiblen Themen wie Wearables oder Videoüberwachung.

Sie werden sehen: Datenschutz ist kein Stolperstein, sondern ein Sicherheitsnetz. Und wer dieses Netz sorgfältig knüpft, sorgt dafür, dass Mitarbeiter geschützt sind – nicht nur vor physischen Gefahren, sondern auch vor digitalen Risiken.

Wir zeigen Ihnen, wie moderner Arbeitsschutz funktioniert: sicher, datenschutzkonform und praxisnah.

A handwritten signature in black ink, appearing to read 'Andreas Hessel'. The signature is stylized with long, sweeping strokes.

Andreas Hessel

Unterweisungen im Arbeitsschutz – welche Formen sinnvoll sind

Präsenzunterweisungen am Arbeitsplatz

Die klassische Form bleibt die persönliche Unterweisung direkt am Arbeitsplatz. Hier können Gefahrenquellen unmittelbar gezeigt und der richtige Umgang mit Arbeitsmitteln praktisch vermittelt werden. Besonders in Bereichen mit hohen Risiken oder speziellen Gefährdungen ist eine Präsenzs Schulung unverzichtbar.

Digitale Unterweisungen

E-Learnings haben sich als flexible Ergänzung etabliert. Inhalte lassen sich zeit- und ortsunabhängig abrufen, was besonders für mobile Mitarbeiter oder große Belegschaften von Vorteil ist. Digitale Unterweisungen eignen sich gut für theoretische Grundlagen, rechtliche Vorgaben oder wiederkehrende Standardthemen.

Live-Online-Schulungen

Per Videokonferenz lassen sich ganze Unterweisungen auch live durchführen. Teilnehmer können Fragen stellen und der Referent kann flexibel reagieren. Solche Schulungen sind vor allem dann geeignet, wenn räumlich verteilte Teams gleichzeitig geschult werden sollen.

Blended Learning als Kombination

Die Mischung aus Präsenz- und Online-Unterweisung hat sich als besonders wirksam erwiesen. Während Grundlagen digital vermittelt werden können, bieten Präsenzphasen Raum für praktische Übungen, Diskussionen und Erfahrungsaustausch. Diese Kombina-

tion nutzt die Vorteile beider Welten und erhöht die Nachhaltigkeit des Gelernten.

Interaktive Elemente und Wissenstests

Unterweisungen sind nur dann erfolgreich, wenn Inhalte auch wirklich verstanden werden. Digitale Tests, kleine Praxisübungen oder Gruppendiskussionen helfen, das Gelernte zu vertiefen. So wird aus einer Pflichtveranstaltung ein interaktives Training mit Mehrwert.

Fazit: Unterweisungen lassen sich heute flexibel gestalten – von Präsenz über digital bis hin zu Blended Learning. Entscheidend ist, die richtige Form für den jeweiligen Inhalt und die Zielgruppe zu wählen. Theorie kann online vermittelt werden, praktische Fertigkeiten brauchen Präsenz. Wer diese Balance findet, sorgt nicht nur für rechtliche Sicherheit, sondern auch für motivierte und gut informierte Mitarbeiter.



© Maryna - stock.adobe.com

Interaktive Schulungen sorgen für mehr Verständnis und nachhaltiges Lernen im Arbeitsschutz.

Mitarbeitersensibilisierung: Datenschutz als Bestandteil der Unterweisung

Datenschutz gehört in jede Schulung

Unterweisungen zum Arbeitsschutz sind Pflicht. Warum also nicht gleich den Datenschutz mit aufnehmen? Schließlich geht es bei beiden Themen um eines: den Schutz der Mitarbeiter. Wenn Beschäftigte lernen, wie sie mit Maschinen sicher umgehen, sollten sie auch verstehen, wie sie vertrauliche Informationen vor neugierigen Blicken schützen.

Praxis statt Paragraphen

Trockene Gesetzestexte sind kein Motivationsbooster. Vermitteln Sie Datenschutz so, dass er greifbar wird. Erzählen Sie Geschichten aus dem Alltag: Das Attest, das offen auf dem Kopierer liegt. Die Unfallmeldung, die versehentlich an den falschen Verteiler geht. Solche Beispiele sind einprägsam und zeigen, dass Datenschutz nicht abstrakt, sondern praktisch relevant ist.



© stockpics - stock.adobe.com

Schulungen zum Datenschutz machen abstrakte Regeln greifbar und stärken das Verantwortungsbewusstsein.

Kleine Übungen mit großer Wirkung

Lassen Sie Ihre Mitarbeiter aktiv werden. Ein kurzer Rollentausch – „Was wäre, wenn Ihre eigenen Daten auf dem Schwarzen Brett hängen würden?“ – wirkt oft stärker als jede Präsentation. Auch kleine Quizfragen oder Fallbeispiele halten die Aufmerksamkeit hoch. Ziel ist nicht, Paragraphen auswendig zu lernen, sondern ein Bewusstsein für Risiken und Verantwortung zu schaffen.

Kontinuität ist entscheidend

Einmal sensibilisiert heißt nicht für immer sensibilisiert. Genau wie bei Sicherheitsschulungen braucht es Regelmäßigkeit. Bauen Sie Datenschutz als festen Bestandteil jeder Arbeitsschutzunterweisung ein und ergänzen Sie bei Bedarf aktuelle Themen, zum Beispiel den Umgang mit mobilen Geräten oder neuen Tools.

Vertrauen entsteht durch Vorleben

Mitarbeiter nehmen Sensibilisierung nur dann ernst, wenn sie sehen, dass auch Führungskräfte und Vorgesetzte nach den Regeln handeln. Wer selbst darauf achtet, dass vertrauliche Unterlagen sicher verwahrt sind und dass E-Mails verschlüsselt werden, setzt ein starkes Signal. Vorbilder wirken besser als Vorschriften.

Fazit: Datenschutz ist kein Fremdkörper im Arbeitsschutz, sondern Teil desselben Schutzgedankens. Wer ihn praxisnah vermittelt, regelmäßig wiederholt und selbst vorlebt, sorgt nicht nur für rechtliche Sicherheit, sondern stärkt auch das Vertrauen der Belegschaft.

Homeoffice und mobiles Arbeiten – was Arbeitgeber beachten müssen

Homeoffice bedeutet, dass Ihr Mitarbeiter einen festen Arbeitsplatz außerhalb der Betriebsstätte nutzt, in der Regel in den eigenen vier Wänden. Dieser Arbeitsplatz muss den Vorgaben der Arbeitsstättenverordnung entsprechen. Dazu gehören ergonomische Möbel, ein geeigneter Bildschirm und eine sichere Arbeitsumgebung. Das Arbeiten am Küchentisch ist also keine Dauerlösung, auch wenn es praktisch erscheinen mag. Sie als Arbeitgeber tragen die Verantwortung, dass die grundlegenden Anforderungen erfüllt sind.

Zwei Arbeitsformen mit klaren Unterschieden

Mobiles Arbeiten ist flexibler. Ihre Mitarbeiter greifen über Laptop, Tablet oder Smartphone von unterschiedlichen Orten auf Unternehmensressourcen zu – sei es im Zug, im Hotel oder im Café. Hier greift die Arbeitsstättenverordnung nicht, dennoch müssen Sie Gefährdungen in der Gefährdungsbeurteilung berücksichtigen. Dazu gehören etwa die sichere Nutzung öffentlicher WLANs, der Schutz vor neugierigen Blicken oder klare Vorgaben zur Datensicherung.

Arbeitsschutz auch außerhalb des Büros

Ob Homeoffice oder mobil – die Verantwortung des Arbeitgebers endet nicht an der Bürotür. Klare Regeln sind nötig: zur sicheren Aufbewahrung von Dokumenten, zur Nutzung von Unternehmensgeräten und zu Notfallwegen, falls etwas passiert. Auch die Ergonomie darf nicht fehlen, denn Rückenschmerzen oder Augenbelastung entstehen im Wohnzimmer genauso schnell wie im Büro.



©merla - stock.adobe.com

Auch Mobiles Arbeiten muss in der Gefährdungsbeurteilung berücksichtigt werden.

Arbeitszeiterfassung ist Pflicht

Ein Punkt, den Sie nicht unterschätzen dürfen, ist die Arbeitszeit. Das Bundesarbeitsgericht hat 2022 entschieden, dass in Deutschland eine Pflicht zur vollständigen Arbeitszeiterfassung besteht. Die Politik hat diese Entscheidung inzwischen aufgegriffen und das Arbeitszeitgesetz angepasst. Arbeitgeber müssen ein System einführen, mit dem Beginn, Ende und Dauer der täglichen Arbeitszeit objektiv, verlässlich und zugänglich erfasst werden.

Papierlisten oder „Selbstaufschreibungen“ reichen nicht mehr aus. Ob Ihre Mitarbeiter im Büro, im Homeoffice oder unterwegs arbeiten, spielt dabei keine Rolle.

Vorteile und Nachteile im Überblick

Die Arbeit von zu Hause oder unterwegs bringt viele Vorteile: Motivation und Attraktivität für Bewerber, Zeit- und Kostenersparnis, Ruhe und weniger Ablenkung durch Bürotübel. Gleichzeitig gibt es Risiken, die Führungskräfte aktiv managen müssen. Vereinsamung, Informationsverluste, mangelndes Selbstmanagement oder Ablenkungen im privaten Umfeld können die Produktivität belasten. Halten Sie deshalb den Kontakt, sorgen Sie für regelmäßige Kommunikation und bieten Sie Unterstützung, wenn es Schwierigkeiten gibt.

Digitale Lösungen für die Praxis

Für die Umsetzung bieten sich moderne digitale Zeiterfassungstools an. Sie lassen sich in bestehende Systeme integrieren und ermöglichen es den Beschäftigten, ihre Zeiten unkompliziert einzutragen – egal von welchem Ort aus. Wichtig ist, dass die Erfassung transparent ist und alle Mitarbeiter nachvollziehen können, welche Daten gespeichert werden. Damit erfüllen Sie nicht nur gesetzliche Vorgaben, sondern schaffen auch Vertrauen in Ihre Organisation.

Fazit: Homeoffice und mobiles Arbeiten sind Chancen, die Attraktivität Ihres Unternehmens zu steigern. Wenn Sie dabei Arbeitsschutz, Datenschutz und Arbeitszeitregelungen zusammendenken, haben Sie ein starkes Fundament, auf dem modernes Arbeiten sicher gelingen kann.



Das Home-Office kann die Arbeitgeberattraktivität fördern.

© JenkoAltman - stock.adobe.com

Datenschutz im Arbeitsschutzalltag

Sensible Daten gehören zum Alltag

Im Arbeitsschutz fällt eine Vielzahl an Daten an, die nicht auf den ersten Blick als sensibel erscheinen, bei genauerem Hinsehen aber höchst schutzbedürftig sind. Unfallberichte, Gefährdungsbeurteilungen, medizinische Atteste oder auch Protokolle von Beinaheunfällen enthalten regelmäßig personenbezogene Informationen. Werden diese unbedacht gespeichert oder weitergegeben, ist nicht nur der Datenschutz verletzt, sondern auch das Vertrauen der Beschäftigten erschüttert.

Weniger ist oft mehr

Das wichtigste Prinzip lautet Datensparsamkeit. Fragen Sie sich bei jeder Erhebung: Brauchen wir den Namen des Betroffenen wirklich oder reicht es, die Gefährdung anonymisiert zu dokumentieren? In vielen Fällen ist die Ursache für einen Unfall oder eine gesundheitliche Belastung wichtiger als die Person, die betroffen war. Wer hier konsequent reduziert, minimiert nicht nur Risiken, sondern zeigt auch Verantwortungsbewusstsein gegenüber seinen Mitarbeitern.

Klare Rechtsgrundlagen schaffen

Die Datenschutz-Grundverordnung liefert die Basis, doch sie bleibt abstrakt, wenn sie nicht in klare Prozesse übersetzt wird. Dokumentieren Sie deshalb nachvollziehbar, auf welcher Rechtsgrundlage Sie Daten erheben und speichern. Bei Gesundheitsdaten kommt Art. 9 DSGVO ins Spiel, kombiniert mit den Pflichten aus dem Arbeitsschutzgesetz. Entscheidend ist, dass Sie jederzeit belegen können, warum eine Verarbeitung erforderlich ist und wie lange sie notwendig bleibt.

Zusammenarbeit statt Silos

Arbeitsschutz- und Datenschutzbeauftragte verfolgen das gleiche Ziel: die Sicherheit der Beschäftigten. Dennoch arbeiten sie in vielen Unternehmen zu selten Hand in Hand. Sorgen Sie für regelmäßige Abstimmungen, zum Beispiel bei der Einführung neuer Systeme oder bei der Auswertung von Gefährdungsbeurteilungen. Wer beide Perspektiven früh einbindet, vermeidet Konflikte und beschleunigt Entscheidungen.

Transparenz stärkt das Vertrauen

Mitarbeiter wollen wissen, was mit ihren Daten geschieht. Erklären Sie offen, welche Informationen Sie erheben, wie lange diese gespeichert werden und wer Zugriff hat. Diese Transparenz ist keine zusätzliche Bürde, sondern ein Gewinn. Denn je klarer die Regeln, desto stärker das Vertrauen in die Organisation – und desto eher unterstützen die Beschäftigten die Maßnahmen, die zu ihrer eigenen Sicherheit dienen.

Fazit: Datenschutz im Arbeitsschutzalltag ist kein Selbstzweck. Er zeigt, dass Unternehmen nicht nur ihre Pflichten erfüllen, sondern die Interessen der Mitarbeiter ernst nehmen. Wer Unfallberichte sorgfältig behandelt, Zugriffsrechte klar regelt und Prozesse transparent gestaltet, schafft ein Arbeitsumfeld, in dem Sicherheit und Vertrauen zusammengehören.



Sensible Daten im Arbeitsschutz erfordern besonderen Schutz.

Die 9 effektivsten Tipps für Video-Meetings

Mit diesen 9 Tipps verlaufen virtuelle Meetings optimal

1. Technisches Equipment

Auch wenn Sie oder Ihre Mitarbeiter keine technischen Genies sind: Alle Teilnehmer müssen die Technik beherrschen. Zusammen und allein. Rückfragen wie „Wie geht es?“ und „Wo finde ich es?“ stören das Meeting. Versenden Sie im Zweifelsfall vorher ein „How to“-Video oder eine Anleitung.

2. Zeitzonen und Feiertage

Bei der Planung virtueller Meetings müssen neben den unterschiedlichen Zeitzonen auch die internationalen Feiertage berücksichtigt werden.

3. Maximale Teilnehmerzahl

Virtuelle Meetings mit mehr als max. 12 Teilnehmern werden unproduktiv, vor allem, wenn sie länger als 60 Minuten dauern.

4. Geeignete Räumlichkeiten

Webkonferenzen sollten an einem ruhigen und ungestörten Ort stattfinden. Öffentliche Cafés, das Wohnzimmer, in dem die Kinder spielen, oder andere belebte Orte wirken störend, weil sie alle Teilnehmer durch Geräusche oder Hintergrundbewegungen ablenken.

5. Eine Agenda ist obligatorisch

Ob Sie der Moderator sind oder ein Teilnehmer: Jedes Meeting sollte eine Agenda haben, die eingehalten wird.

6. Sichtbarkeit

Die Teilnehmer sollten alle sichtbar sein. Zumindest der Name und ein Foto sollten auf dem Bildschirm gut erkennbar sein. Rätselraten, wer gerade spricht, nervt alle.

7. Fokus!

Eine Regel, die für alle gilt: keine Parallelbeschäftigung, auch wenn es langweilig ist. Es ist verlockend, doch trotzdem: Nein!

8. Keine Monologe

Für virtuelle Meetings gilt das Gleiche wie für persönliche Besprechungen: Bringen Sie die Nachricht auf den Punkt. Am Bildschirm ist es noch schwieriger, konzentriert zu bleiben, wenn ein Redner einfach den Schlusspunkt nicht findet.

9. Präsentationsgrundlagen

Wenig Text, klarer Schrifttyp, Schriftgröße mind. 16. Keine nervigen Animationen. Und keine virtuellen Hintergründe, die für Verwirrung sorgen, wenn der Sprecher ständig verschwindet.



Datenverarbeitung: Was müssen Sie dabei beachten?

Alle Datenschutzerfordernungen sind selbstverständlich auch in der Krise im Unternehmen umzusetzen. Für Führungskräfte ergeben sich hierbei 2 wesentliche Herausforderungen: Zum einen werden kurzfristig Verfahren geändert bzw. neue technische Verfahren eingeführt und zum anderen werden auch neue sensible personenbezogene Daten im Unternehmen erhoben. Hier gilt es zunächst zu prüfen, welche dieser Daten das Unternehmen überhaupt erheben darf. Mit diesem Hintergrundwissen fällt es Ihnen als Arbeitsschützer und natürlich auch Ihren Betriebsärzten leichter, Entscheidungen zu treffen.

Der einzelne Betroffene bleibt natürlich „Herr seiner Daten“, gerade auch seiner besonders sensiblen Gesundheitsdaten. Dabei kann aber eine arbeitsvertragliche Pflicht bestehen, durch Angaben über Aufenthaltsorte oder Kontaktpersonen dem Arbeitgeber eine Einschätzung zu ermöglichen, ob Gesundheitsrisiken für den Betroffenen oder andere Beschäftigte bestehen. Bei den Daten, die das Unternehmen während der Pandemie verarbeiten darf, kann es sich insbesondere um folgende Informationen handeln:

- Informationen über Personen, bei denen eine Infektion festgestellt wurde oder die Kontakt mit einer nachweislich infizierten Person hatten
- Informationen über Personen, die sich im relevanten Zeitraum in einem vom Robert Koch-Institut (RKI) als Risikogebiet eingestuften Gebiet aufgehalten haben

Erlaubt sind die Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern, insbesondere um festzustellen, ob diese

- selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen,
- sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben.

Die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von Kontaktpersonen ist dagegen nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen ausnahmsweise erforderlich ist.

HINWEIS

Wenn Sie wissen wollen, ob Ihre E-Mails mit sensiblen Daten, die Sie an Externe versenden, verschlüsselt werden, können Sie unter: <https://de.ssltools.net> nachschauen. Geben Sie dazu einfach die Domäne des E-Mail-Empfängers in das entsprechende Feld auf der Internetseite ein. Sie erhalten dann umgehend Informationen darüber, ob die Kommunikation mit diesem Partner sicher ist.



© sabelskaya - AdobeStock.com

Gehen Sie sicher, dass Ihre E-Mails an Externe verschlüsselt werden.

Sicherheitslösungen datenschutzkonform gestalten

Sicherheit ja – Überwachung nein

Elektronische Zutrittskontrollen, digitale Schließsysteme oder Videoüberwachung sind aus modernen Betrieben kaum noch wegzudenken. Sie schützen Gebäude, Maschinen und nicht zuletzt die Menschen, die dort arbeiten. Doch schnell entsteht der Eindruck, dass Mitarbeiter überwacht werden. Genau hier liegt die Kunst: Systeme so einzusetzen, dass sie Sicherheit erhöhen, ohne Persönlichkeitsrechte zu verletzen.

Zutrittskontrolle mit Augenmaß

Digitale Schließsysteme sind praktisch und effizient, dürfen aber nicht zur Erstellung von Bewegungsprofilen missbraucht werden. Es reicht, Zutritte freizugeben oder zu verweigern. Wer wann genau den Pausenraum betritt oder wie lange er dort verweilt, gehört nicht in die Auswertung. Achten Sie bei der Auswahl der Systeme darauf, dass nur die unbedingt erforderlichen Daten gespeichert werden – und legen Sie Speicherfristen fest.

Videoüberwachung nur im Ausnahmefall

Kameras am Arbeitsplatz sind ein sensibles Thema. Dauerhafte Überwachung ist unzulässig, weil sie das Vertrauen der Mitarbeiter zerstört. Zulässig ist Videoüberwachung nur dort, wo sie für den Schutz vor Gefahren oder Straftaten erforderlich ist – etwa in Hochsicherheitsbereichen, an Zugängen oder in Bereichen mit besonderen Unfallrisiken. Auch hier gilt: so viel wie nötig, so wenig wie möglich. Beschäftigte müssen zudem informiert werden, wo Kameras hängen und warum sie dort angebracht sind.

Pflicht zur Datenschutz-Folgenabschätzung

Besonders eingriffsintensive Systeme wie biometrische Zutrittskontrollen oder umfassende Videoüberwachung lösen eine gesetzliche Pflicht zur Datenschutz-Folgenabschätzung aus. Diese ist mehr als nur ein Formular für die Schublade. Sie zwingt dazu, Risiken für die Rechte der Beschäftigten zu identifizieren und Gegenmaßnahmen zu entwickeln. Dokumentieren Sie genau, warum Sie das System brauchen, welche Schutzmechanismen Sie einsetzen und wie Sie Missbrauch verhindern. Damit schaffen Sie Transparenz – auch gegenüber Mitarbeitern und Aufsichtsbehörden.

Zusammenarbeit schafft Akzeptanz

Technik allein reicht nicht. Suchen Sie das Gespräch mit Betriebsrat, Datenschutzbeauftragtem und den betroffenen Mitarbeitern, bevor Sie ein neues System einführen.

Wer seine Belegschaft informiert und einbindet, erhöht die Akzeptanz erheblich. Transparenz ist hier der Schlüssel: erklären Sie nicht nur, dass Sie ein System einführen, sondern auch, warum und mit welchen Schutzvorkehrungen.

Fazit: Sicherheitslösungen dürfen kein Überwachungsinstrument sein, sondern müssen die Balance halten zwischen Schutz und Vertrauen. Wenn Sie Zutrittskontrollen und Videoüberwachung datenschutzkonform gestalten und eine Folgenabschätzung durchführen, schaffen Sie nicht nur Rechtssicherheit, sondern auch ein Arbeitsumfeld, in dem sich Ihre Mitarbeiter geschützt – und nicht beobachtet – fühlen.

Digitaler Arbeitsschutz: Datenschutz bei Wearables und Sensorik

Technik als Helfer im Arbeitsalltag

Exoskelette entlasten die Wirbelsäule, smarte Helme melden Stürze und Armbänder überwachen Puls oder Körpertemperatur. Solche digitalen Helfer können Arbeitsplätze sicherer machen und die Gesundheit der Mitarbeiter schützen. Sie eröffnen neue Chancen im Arbeitsschutz, bringen jedoch auch datenschutzrechtliche Herausforderungen mit sich.

Gesundheitsdaten sind besonders sensibel

Viele Wearables erfassen Informationen, die direkt in die Kategorie der Gesundheitsdaten fallen – und damit besonders schutzbedürftig sind. Das bedeutet: Unternehmen dürfen sie nicht einfach so verarbeiten, sondern brauchen eine klare Rechtsgrundlage und technische Schutzmaßnahmen. Wer diese Daten erhebt, muss genau wissen, warum und wie lange sie gespeichert werden und wer darauf zugreifen darf.

Anonymisierung statt Überwachung

Nicht jede Analyse braucht personenbezogene Daten. Häufig genügt es, anonyme Auswertungen zu erstellen, um Belastungen oder Gefahren zu erkennen. So lässt sich beispielsweise feststellen, dass eine bestimmte Ar-

beitsposition zu hoher Belastung führt – ohne, dass der Name des betroffenen Mitarbeiters bekannt wird. Sie sollten in Ihrem Unternehmen sollten prüfen, ob eine Anonymisierung möglich sein kann, bevor sie personenbezogene Daten erfassen.

Transparenz schafft Vertrauen

Mitarbeiter akzeptieren neue Technologien nur dann, wenn sie verstehen, wofür die Daten genutzt werden. Machen Sie deshalb von Anfang an klar, dass es nicht darum geht, die Leistungsfähigkeit einzelner Personen zu überwachen, sondern gesundheitliche Risiken zu reduzieren.

Offene Kommunikation ist hier entscheidend: erläutern Sie, welche Daten erhoben werden, wie sie verarbeitet werden und welche Schutzmaßnahmen bestehen.

Datenschutz-Folgenabschätzung bei neuen Systemen

Der Einsatz von Wearables und Sensorik kann eine Datenschutz-Folgenabschätzung notwendig machen. Insbesondere dann, wenn großflächig Gesundheitsdaten verarbeitet werden. Nutzen Sie diese Pflicht als Chance, um Risiken systematisch zu erkennen und Lösungen zu entwickeln, die Mitarbeiterrechte respektieren.

Fazit: Digitale Helfer können den Arbeitsschutz revolutionieren – wenn sie verantwortungsvoll eingesetzt werden. Wer Wearables und Sensorik nicht als Überwachungsinstrument, sondern als Unterstützung versteht, kombiniert Sicherheit mit Vertrauen. So wird der digitale Arbeitsschutz zu einem echten Gewinn für alle.



Datenschutz bleibt bei digitalen Arbeitsschutzhilfen unverzichtbar.

Checkliste: DSGVO & Arbeitsschutz im Einklang

Die wichtigsten Fragen für Ihre Praxis

Datenschutz und Arbeitsschutz lassen sich nur dann erfolgreich vereinen, wenn klare Regeln gelten. Nutzen Sie die folgende Checkliste, um Ihre Maßnahmen zu überprüfen und Stolperfallen frühzeitig zu vermeiden:

Erheben wir nur das Nötigste?

Prüfen Sie bei jeder Datenerfassung, ob sie wirklich erforderlich ist. Namen oder Gesundheitsdetails sind oft überflüssig, wenn das Risiko anonym beschrieben werden kann.

Gibt es eine klare Rechtsgrundlage?

Dokumentieren Sie, auf welchen Artikeln der DSGVO oder welchen Vorgaben aus dem Arbeitsschutzgesetz Ihre Datenverarbeitung beruht. So sind Sie auch bei Rückfragen der Aufsichtsbehörde auf der sicheren Seite.

Sind die Beschäftigten informiert?

Transparenz schafft Vertrauen. Machen Sie offen, welche Daten erhoben werden, wie lange sie gespeichert bleiben und wer Zugriff hat.

Haben wir Speicher- und Löschfristen festgelegt?

Daten, die einmal erhoben wurden, dürfen nicht endlos liegen bleiben. Legen Sie konkrete Fristen fest und dokumentieren Sie die Löschung.

Brauchen wir eine Datenschutz-Folgenabschätzung?

Bei besonders eingriffsintensiven Maßnahmen wie Videoüberwachung, biometrischen Systemen oder Wearables ist eine DSFA Pflicht. Sie



Klare Regeln schaffen Sicherheit.

schützt Mitarbeiterrechte und gibt Ihnen Planungssicherheit.

Werden sensible Daten technisch geschützt?

Gesundheitsdaten oder Zutrittsprotokolle gehören nicht unverschlüsselt auf einen Server oder in eine Excel-Datei. Sorgen Sie für Verschlüsselung, Zugriffsbeschränkungen und sichere Aufbewahrung.

Fazit: Mit dieser Checkliste behalten Sie den Überblick. Sie zeigt, dass Datenschutz und Arbeitsschutz keine Gegensätze sind, sondern sich gegenseitig ergänzen. Wer beide Aspekte von Anfang an zusammendenkt, sorgt für Sicherheit auf allen Ebenen – physisch und digital.

Tipp: Vertiefen Sie Ihr Wissen! In der Aufzeichnung des Webinars „DSGVO-Grundsätze – warum Art. 5 DSGVO die zentrale Datenschutz-Norm ist“ erfahren Sie praxisnah, warum gerade dieser Artikel die Basis für alle Datenschutzmaßnahmen bildet.

Unter folgendem Link gelangen Sie zur Aufzeichnung: <https://bit.ly/4mLNthi>

Informationssicherheit im Arbeitsalltag – ein Handout für Mitarbeiter

Warum Informationssicherheit zum Arbeitsschutz gehört

Arbeitsschutz bedeutet, dass Sie gesund und sicher durch den Arbeitsalltag kommen. Dazu gehört nicht nur die Vermeidung von Stolperfallen oder Lärmbelastungen, sondern auch der Schutz vor digitalen Gefahren.

Ein verlorenes Passwort oder eine unbedacht geöffnete Phishing-Mail kann nicht nur das Unternehmen lahmlegen, sondern auch Ihre tägliche Arbeit massiv beeinträchtigen. Informationssicherheit ist damit ein Teil des Arbeitsschutzes – sie schützt Sie, Ihre Kollegen und Ihre Arbeitsumgebung.

Vorsicht vor Phishing

Phishing-Mails sind Betrugsversuche, die oft täuschend echt aussehen. Sie geben sich zum Beispiel als Paketdienst aus („Ihr Paket konnte nicht zugestellt werden“), als vermeintlicher Chef („Bitte überweisen Sie sofort...“) oder sogar als Bank. Ein Klick genügt, und Schadsoftware gelangt ins System oder Zugangsdaten werden abgegriffen.

Beispiel: Ein Mitarbeiter erhält eine Mail angeblich von der Personalabteilung mit der Bitte, seine Kontodaten zu bestätigen. Ein Klick hätte die Daten direkt an Kriminelle weitergeleitet. Oder der Klick auf einen Anhang hätte Schadsoftware auf den PC geladen und das gesamte Netzwerk wäre verschlüsselt worden. Nur weil er misstrauisch war und die IT informierte, konnte ein Schaden verhindert werden.

Sichere Passwörter wählen

Passwörter sind wie Schlüssel. Wer denselben Schlüssel für Haustür, Auto und Schreibtisch nutzt, macht es Einbrechern leicht. Nutzen Sie daher für jedes System ein eigenes, starkes Passwort. Ein Passwortmanager hilft, den Überblick zu behalten.

Beispiel: Das Passwort „Sommer2024“ ist schnell erraten. „F!schKutter_98?“ hingegen ist sicherer und trotzdem merkbar. Noch besser: längere Passphrasen wie „MeinHundMag-KekseAmFreitag!“.

E-Mailsicherheit beachten

E-Mails sind praktisch, aber nicht immer sicher. Gehen Sie sparsam mit vertraulichen Daten um und prüfen Sie vor dem Versand, wer wirklich im Verteiler steht. Besonders sensible Informationen sollten verschlüsselt verschickt werden.

Beispiel: Ein Unfallbericht mit Namen von Mitarbeitern wird versehentlich an die gesamte Abteilung gesendet – statt nur an den Betriebsarzt. Ein klassischer Fall von „zu schnell auf Senden gedrückt“. Mit einer klaren Regel „Vertrauliches nur verschlüsselt“ lassen sich solche Fehler vermeiden.

Sicher surfen im Internet

Das Internet ist voller nützlicher Informationen, aber auch voller Fallen. Nutzen Sie nur vertrauenswürdige Seiten und laden Sie keine Programme von unbekannten Quellen herunter. Achten Sie auf „https://“ in der Adresszeile.

Beispiel: Eine Mitarbeiterin lädt eine „kostenlose PDF-Software“ aus einer dubiosen Quelle herunter. Statt eines Tools erhält sie Schadsoftware, die ihre Dateien verschlüsselt. Das hätte leicht vermieden werden können, wenn sie nur geprüfte Programme aus dem Unternehmensportal genutzt hätte.

Fazit: Informationssicherheit schützt nicht nur Daten, sondern auch Arbeitsprozesse

und damit die Gesundheit aller. Ein verschlüsselter E-Mail-Versand, ein sicheres Passwort oder ein wachsames Auge bei Phishing sind genauso Teil des Arbeitsschutzes wie ein sicherer Arbeitsplatzstuhl.

Gemeinsam sorgen wir dafür, dass Arbeitsschutz nicht an der Bürotür endet, sondern auch im digitalen Raum gelebt wird.

Clean Desk: Was heißt das im Home-Office?

Sie müssen wirksam verhindern, dass während Ihrer Abwesenheit Unbefugte Zugriff auf vertrauliche Informationen erhalten. Denken Sie z. B. an Auswertungen von Mitarbeiterbefragungen im Zusammenhang mit dem psychischen Arbeitsschutz, Unfallberichte, Statistiken etc. [AH]

Die nachfolgenden Punkte müssen Sie daher berücksichtigen

Büroraum im privaten Umfeld

- Ich bewahre (streng) vertrauliche Daten sicher auf (abschließbarer Schrank usw.). Ich schließe ggf. den Raum ab, wenn ich ihn verlasse.

IT-Systeme

- Ich sperre meine IT-Systeme und Dokumentationen zum Arbeitsschutz beim Verlassen des Raumes (WIN- und L-Tasten).
- Ich fahre meine IT-Systeme am Ende des Arbeitstages herunter.
- Ich verwende sichere Anmelde-Passwörter für meine Accounts.

Mobile Geräte

- Ich verwende starke Passwörter (PIN-Code mindestens 6 Zeichen).

- Ich aktiviere die Geräteverschlüsselung.
- Ich verschlüssele die Daten auf mobilen Datenträgern.
- Ich lasse die IT-Geräte nur bei vertrauenswürdigen Stellen reparieren.

Entsorgung von Daten/Informationen

- Ich schreddere vertrauliche Papiere.
- Ich vernichte nicht mehr benötigte Datenträger datenschutzkonform (Schredder, Entsorger).

Wichtig: Auch Reinigungskräfte, Besucher oder Familienmitglieder können Unbefugte sein. Wichtige Dokumente dürfen nicht verloren gehen, z. B. durch Kinder, die aufgrund von Homeschooling mit Ihnen in einem Raum sitzen oder spielen. Sie müssen also dafür sorgen, dass Unterlagen mit personenbezogenen Daten oder der PC auch bei kurzer Abwesenheit vor unbefugtem Zugang geschützt werden. Denn man kann nicht ausschließen, dass jemand Ihr privates Büro betritt.

Handout: Informationssicherheit im Arbeitsalltag

Ihr Beitrag zum Arbeitsschutz im digitalen Raum	
Phishing – seien Sie misstrauisch	✓
• Prüfen Sie Absenderadressen und Links vor dem Klicken	☐
• Reagieren Sie nicht auf Mails mit Zeitdruck („sofort handeln!“)	☐
• Verdächtige Nachrichten sofort an die IT weiterleiten	☐
Passwörter – Ihr Schlüssel zur Sicherheit	
• Nutzen Sie lange und komplexe Passwörter oder Passphrasen	☐
• Für jedes System ein eigenes Passwort verwenden	☐
• Passwortmanager und Zwei-Faktor-Authentifizierung einsetzen	☐
E-Mailsicherheit – vorsichtig senden	
• Anhänge nur öffnen, wenn die Quelle vertrauenswürdig ist	☐
• Vertrauliche Informationen nur verschlüsselt versenden	☐
• Verteiler vor dem Senden prüfen – nicht jeder muss alles wissen	☐
Sicher surfen – Fallen vermeiden	
• Achten Sie auf „https://“ in der Adresszeile	☐
• Laden Sie Software nur aus vertrauenswürdigen Quellen	☐
• Keine persönlichen Daten in unsicheren Formularen eingeben	☐
Clean Desk – nicht nur fürs Büro	
• Rechner sperren, wenn Sie den Platz verlassen	☐
• Vertrauliche Unterlagen wegschließen	☐
• Keine sensiblen Daten offen herumliegen lassen	☐

Merken Sie sich:

Informationssicherheit ist Teil des Arbeitsschutzes. Jeder trägt dazu bei, dass Daten und Systeme sicher bleiben – so wie jeder

einen Helm aufsetzt oder einen Sicherheitsgurt anlegt.

Fazit: Arbeitsschutz und Datenschutz gehören zusammen

Arbeitsschutz schützt Körper und Gesundheit, Datenschutz schützt Privatsphäre und Vertrauen. Beides sind keine Gegensätze, sondern zwei Seiten derselben Medaille. Wer die Sicherheit seiner Mitarbeiter ernst nimmt, kann das eine nicht ohne das andere umsetzen.

Vielleicht haben Sie beim Lesen gemerkt, dass die Herausforderungen gar nicht so weit voneinander entfernt sind: Unfallberichte wollen genauso geschützt werden wie Zutrittsprotokolle. Unterweisungen sind nur dann vollständig, wenn sie auch den Datenschutz einbeziehen. Und moderne Technik wie Wearables oder Videoüberwachung entfaltet ihren Nutzen nur dann, wenn sie verantwortungsvoll eingesetzt wird

Sie als Arbeitsschutzverantwortlicher haben die Chance, hier Vorreiter zu sein. Indem Sie Datenschutz nicht als bürokratisches Hindernis sehen, sondern als Teil einer gelebten Sicherheitskultur, schaffen Sie Mehrwert für Ihr

Unternehmen. Ein Team, das sich sicher fühlt und Vertrauen in den Umgang mit seinen Daten hat, arbeitet motivierter und engagierter.

Nehmen Sie die Impulse dieser Broschüre mit in Ihren Alltag. Prüfen Sie Ihre Prozesse, sprechen Sie mit Ihrem Datenschutzbeauftragten und binden Sie die Mitarbeiter aktiv ein. Kleine Schritte reichen oft schon aus, um spürbare Verbesserungen zu erzielen.

Und behalten Sie dabei eines im Kopf: Sicherheit entsteht nicht durch einzelne Maßnahmen, sondern durch eine Kultur. Arbeitsschutz und Datenschutz gemeinsam zu denken, ist ein starkes Signal – an Ihre Belegschaft, an Kunden und an Partner.

Oder, um es mit einem bekannten Satz aus der Filmgeschichte zu sagen: „This is the beginning of a beautiful friendship.“ Lassen Sie Arbeitsschutz und Datenschutz nicht nebeneinanderlaufen, sondern Hand in Hand – für mehr Sicherheit, Vertrauen und Zukunftsfähigkeit in Ihrem Unternehmen.



Sicherheit braucht beides – Schutz für Menschen und Daten.

© Наталья Пилипенко - stock.adobe.com

Impressum

Safety Xperts
ein Unternehmensbereich der
VNR Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4 • 53095 Bonn
Telefon: 02 28 / 95 50 490 • Fax: 02 28 / 36 96 480
Vorstand: Richard Rentrop, Bonn
Internet: www.safetyxperts.de
E-Mail: info@safetyxperts.de
Herausgeber: Michael Jodda, Bonn
Produktmanager: Milena Eilers

Satz & Layout: OtterbachMedien, Freudenberg
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim

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. Vervielfältigungen jeder Art sind nur mit Genehmigung des Verlags gestattet.

© 2025 by Safety Xperts – ein Unternehmensbereich der Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

Zusätzlicher Hinweis

Diese Broschüre richtet sich gleichermaßen an männliche und weibliche Personen. Aus Gründen der Lesbarkeit wurde die männliche Schreibweise (z. B. Unternehmer, Mitarbeiter) gewählt. Diese beinhaltet stets auch alle anderen Geschlechterformen.

Datenschutz trifft Arbeitssicherheit

Wichtige Informationen und Tipps für Ihren Arbeitsalltag

Wissen kompakt