Personaldaten im Fokus: Zeiterfassung

Datenschutzkonforme Verarbeitung von Arbeitszeitdaten

Oktober | 2026



Wichtige Datenschutzinformationen für Ihr Unternehmen

NBW BERATUNG
DATENSCHUTZ-EXPERTEN

Inhalte | Datenschutzinformationen

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort _____ 3

Zeiterfassung – Rechtliche Grundlagen und aktuelle Entwicklungen _____ 4

- EuGH- und BAG-Rechtsprechung zur Arbeitszeiterfassung
- Gesetzliche Anforderungen in Deutschland und der EU
- Abgrenzung zum Arbeitszeitgesetz und zur DSGVO

Arbeitszeitdaten und ihre rechtliche Einordnung _____ 6

- Arten und Kategorien von Arbeitszeitdaten
- Personenbezug und Sensibilität der Daten
- Rechtsgrundlagen nach DSGVO und § 26 BDSG

Systeme zur Zeiterfassung im Überblick _____ 8

- Manuelle, digitale und mobile Zeiterfassungssysteme
- Cloudlösungen vs. On-Premises
- Schnittstellen zu HR- und Payroll-Systemen

Datenschutzrisiken und typische Fehlerquellen _____ 10

- Unzulässige Leistungs- und Verhaltenskontrolle
- Übermäßige Datenerhebung und Dauerüberwachung
- Fehlende Transparenz gegenüber Beschäftigten

Technische und organisatorische Maßnahmen (TOM) _____ 12

- Zugriffskontrollen und Berechtigungskonzepte
- Protokollierung und Integrität der Daten
- Verschlüsselung und sichere Speicherung

Mitbestimmung und Beteiligung des Betriebsrats _____ 14

- Rechte des Betriebsrats nach § 87 BetrVG
- Gestaltung von Betriebsvereinbarungen
- Praxisbeispiele für datenschutzkonforme Regelungen

Informationspflichten und Transparenz _____ 16

- Umsetzung von Art. 13 DSGVO bei Zeiterfassungssystemen
- Verständliche Mitarbeiterinformationen
- Dokumentation und Nachweisführung

Speicherfristen und Löschkonzepte_____ 18

- Gesetzliche Aufbewahrungspflichten
- Löschfristen für Arbeitszeitdaten
- Umsetzung in der Praxis

Kontrolle, Audit und kontinuierliche Verbesserung _____ 20

- Interne Kontrollen und regelmäßige Überprüfung
- Auditierbarkeit von Zeiterfassungssystemen
- Kennzahlen und Compliance-Nachweise

Ausblick und Handlungsempfehlungen _____ 22

- Entwicklungen bei digitaler Zeiterfassung
- Handlungsempfehlungen für KMU
- Checkliste zur datenschutzkonformen Umsetzung der Zeiterfassung

Impressum _____ 24

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserinnen und Leser,

die Einführung und Umsetzung von Systemen zur Arbeitszeiterfassung ist für Unternehmen aktueller denn je. Spätestens seit den richtungsweisenden Entscheidungen des Europäischen Gerichtshofs und des Bundesarbeitsgerichts ist klar: Arbeitgeber sind verpflichtet, die Arbeitszeiten ihrer Beschäftigten systematisch zu erfassen. Doch mit der Erhebung dieser Daten gehen zugleich umfangreiche datenschutzrechtliche Anforderungen einher, denn Arbeitszeitdaten sind stets auch Personaldaten.

In dieser Ausgabe unserer Datenschutzzeitung beleuchten wir die Zeiterfassung aus Sicht des Datenschutzes und zeigen Ihnen, wie sich gesetzliche Vorgaben praxisnah und rechtssicher umsetzen lassen. Welche Daten dürfen im Rahmen der Zeiterfassung erhoben werden? Auf welcher Rechtsgrundlage erfolgt die Verarbeitung? Und wie lassen sich Transparenz, Datensparsamkeit und Zweckbindung im Arbeitsalltag gewährleisten?

Ein besonderer Fokus liegt auf der praktischen Umsetzung in Ihrem Unternehmen: Von der Auswahl geeigneter Zeiterfassungssysteme über die Berücksichtigung von Mitbestimmungsrechten bis hin zur Einführung technischer und organisatorischer Maßnahmen. Zudem zeigen wir typische Fehlerquellen auf und geben Ihnen konkrete Handlungsempfehlungen sowie Best Practices an die Hand, um Risiken zu minimieren und gleichzeitig effiziente Prozesse zu etablieren.

Wenn Sie Fragen haben, eine vertiefende Beratung wünschen oder Unterstützung bei der Umsetzung benötigen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter:
der Telefonnummer 0208
oder per E-Mail an
Kontakt@NBW-Beratung.com.

Mit besten Grüßen

NBW-Beratung

Bereich: Datenschutz

Zeiterfassung – Rechtliche Grundlagen und aktuelle Entwicklungen



Zeiterfassung im Spannungsfeld von Arbeitsrecht und Datenschutz

Die systematische Erfassung von Arbeitszeiten hat sich in den letzten Jahren von einer organisatorischen Option zu einer klaren rechtlichen Verpflichtung entwickelt. Ausgangspunkt hierfür sind insbesondere europäische und nationale Gerichtsentscheidungen, die den Handlungsdruck auf Unternehmen deutlich erhöht haben. Gleichzeitig betrifft die Zeiterfassung nicht nur arbeitsrechtliche Fragestellungen, sondern auch den Umgang mit personenbezogenen Daten – und damit unmittelbar die Anforderungen der DSGVO.

Für Unternehmen bedeutet das: Zeiterfassungssysteme müssen nicht nur vollständig und korrekt sein, sondern auch datenschutzkonform gestaltet und betrieben werden. Die Herausforderung liegt darin, beide Perspektiven – Arbeitsrecht und Datenschutz – in Einklang zu bringen.

EuGH- und BAG-Rechtsprechung zur Arbeitszeiterfassung

Mit dem Urteil des Europäischen Gerichtshofs (EuGH) aus dem Jahr 2019 wurde erstmals klargestellt, dass Arbeitgeber verpflichtet sind, ein objektives, verlässliches und zugängliches System zur Erfassung der täglichen Arbeitszeit einzuführen. Ziel ist es, die Einhaltung von Höchstarbeitszeiten und Ruhezeiten sicherzustellen und Arbeitnehmerrechte effektiv zu schützen.

Das Bundesarbeitsgericht (BAG) hat diese Vorgaben im Jahr 2022 aufgegriffen und konkretisiert: Bereits nach geltendem Recht sind Arbeitgeber in Deutschland verpflichtet, die Arbeitszeiten ihrer Beschäftigten vollständig zu erfassen. Eine explizite gesetzliche Neuregelung im Arbeitszeitgesetz wird zwar weiterhin diskutiert, an der grundsätzlichen Pflicht zur Zeiterfassung besteht jedoch kein Zweifel mehr.

Für die Praxis heißt das: Unternehmen müssen unabhängig von ihrer Größe geeignete Systeme zur Arbeitszeiterfassung einführen und betreiben.

Gesetzliche Anforderungen in Deutschland und der EU

Die rechtlichen Anforderungen ergeben sich aus einem Zusammenspiel verschiedener Regelwerke. Auf europäischer Ebene bildet die Arbeitszeitrichtlinie die Grundlage, die Mindeststandards für Arbeits- und Ruhezeiten vorgibt. Diese wird in Deutschland insbesondere durch das Arbeitszeitgesetz (ArbZG) umgesetzt.

Ergänzend dazu konkretisiert die Rechtsprechung die Pflichten zur Arbeitszeiterfassung, während die DSGVO die Verarbeitung der dabei entstehenden personenbezogenen Daten regelt.

Unternehmen müssen daher sicherstellen, dass ihre Zeiterfassungssysteme:

- Arbeitszeiten vollständig und nachvollziehbar dokumentieren,
- eine verlässliche und manipulationssichere Erfassung ermöglichen,
- die gesetzlichen Aufbewahrungs- und Nachweispflichten erfüllen.

Besonders für kleine und mittelständische Unternehmen stellt sich dabei die Frage, wie sich diese Anforderungen pragmatisch und wirtschaftlich umsetzen lassen.

Abgrenzung zum Arbeitszeitgesetz und zur DSGVO

Das Arbeitszeitgesetz regelt primär den Schutz der Beschäftigten durch Vorgaben zu Höchstarbeitszeiten, Ruhepausen und Ruhezeiten. Die Pflicht zur Zeiterfassung dient hier als Kontrollinstrument, um die Einhaltung dieser Vorgaben nachweisen zu können.

Die DSGVO hingegen setzt an einem anderen Punkt an: Sie regelt, wie personenbezogene Daten – und damit auch Arbeitszeitdaten – erhoben, verarbeitet, gespeichert und gelöscht werden dürfen. Dabei stehen insbesondere Prinzipien wie Zweckbindung, Datenminimierung und Transparenz im Vordergrund.

In der Praxis greifen beide Regelungsbereiche ineinander: Während das Arbeitszeitrecht vorgibt, dass Arbeitszeiten erfasst werden müssen, bestimmt das Datenschutzrecht, wie diese Erfassung konkret ausgestaltet sein darf.

Für Unternehmen bedeutet das, dass eine rechtskonforme Zeiterfassung nur dann gegeben ist, wenn beide Perspektiven berücksichtigt werden – etwa durch klare Zugriffsregelungen, transparente Informationen für Beschäftigte und eine datensparsame Systemgestaltung.

Aktuelle Entwicklungen und Handlungsbedarf

Die konkrete gesetzliche Ausgestaltung der Arbeitszeiterfassung in Deutschland ist weiterhin in Bewegung. Es ist davon auszugehen, dass der Gesetzgeber die bestehenden Vorgaben künftig weiter präzisieren wird, insbesondere im Hinblick auf digitale und mobile Arbeitsformen.

Unabhängig davon besteht bereits jetzt Handlungsbedarf: Unternehmen sollten ihre bestehenden Prozesse und Systeme überprüfen und sicherstellen, dass diese sowohl den arbeitsrechtlichen Anforderungen als auch den datenschutzrechtlichen Vorgaben entsprechen.

Führungskräfte und Verantwortliche sind gut beraten, die Zeiterfassung nicht isoliert zu betrachten, sondern als Teil eines ganzheitlichen Compliance-Ansatzes – der Arbeitsrecht, Datenschutz und technische Umsetzung miteinander verbindet.

Arbeitszeitdaten und ihre rechtliche Einordnung

Arbeitszeitdaten als Teil des Beschäftigtenkontextes

Arbeitszeitdaten entstehen in nahezu jedem Unternehmen, in dem Arbeitszeiten, Pausen, Überstunden oder Abwesenheiten erfasst werden. Sobald diese Informationen einer bestimmten Person zugeordnet werden können, handelt es sich um personenbezogene Daten im Sinne der DSGVO. Das gilt unabhängig davon, ob die Erfassung manuell, per Terminal, per App oder über eine Cloudlösung erfolgt. Arbeitszeitdaten sind deshalb nicht nur ein organisatorisches Hilfsmittel, sondern zugleich ein datenschutzrechtlich relevantes Datenobjekt.

Für Unternehmen ist wichtig, die verschiedenen Datenarten sauber zu unterscheiden: Denn nicht jede Information, die im Zusammenhang mit Zeiterfassung anfällt, ist gleich sensibel. Je genauer die Datenerfassung ausgestaltet ist, desto eher lassen sich Datenschutzanforderungen wie Zweckbindung und Datenminimierung einhalten.

Arten und Kategorien von Arbeitszeitdaten

Zur Zeiterfassung gehören typischerweise Arbeitsbeginn, Arbeitsende, Pausenzeiten, Überstunden, Rufbereitschaften, Schichtzuordnungen und Abwesenheiten wie Urlaub oder Krankheit. Hinzu kommen je nach System weitere Metadaten, etwa Nutzerkennungen, Standortinformationen oder technische Protokolle zur Nachvollziehbarkeit der Erfassung. Auch Projektzeiten oder Tätigkeitszuordnungen können Teil des Systems sein, wenn sie für die Organisation oder Abrechnung benötigt werden.

Je nach Ausgestaltung kann die Datenbasis also relativ schlicht oder sehr umfangreich sein. Für die datenschutzrechtliche Bewertung ist entscheidend, ob das System nur die notwendige Arbeitszeit dokumentiert oder darüber hinaus Verhaltens- und Leistungsdaten erzeugt. Gerade bei Standort-, GPS- oder biometriebasierten Lösungen steigt die Eingriffsintensität deutlich an.

Personenbezug und Sensibilität der Daten

Arbeitszeitdaten sind in der Regel eindeutig einer beschäftigten Person zuzuordnen und damit personenbezogene Daten. Sie können Rückschlüsse auf Anwesenheit, Arbeitsverhalten, Einsatzorte oder sogar gesundheitliche Ausfallzeiten zulassen. Deshalb sind sie zwar nicht automatisch besondere Kategorien personenbezogener Daten, aber oft dennoch sensibel, weil sie ein detailliertes Bild vom Beschäftigtenverhältnis vermitteln.

Besonders aufmerksam sollten Unternehmen bei zusätzlichen Informationen sein. Krankheitstage, Standortdaten, biometrische Merkmale oder Leistungsprofile können je nach Ausgestaltung deutlich höhere Datenschutzrisiken auslösen. Spätestens dann reicht ein rein organisatorischer Blick auf die Zeiterfassung nicht mehr aus, sondern es müssen auch technische und rechtliche Schutzmaßnahmen sauber mitgedacht werden.

Rechtsgrundlagen nach DSGVO und § 26 BDSG

Die Verarbeitung von Arbeitszeitdaten kann im Beschäftigungskontext auf mehreren Rechtsgrundlagen beruhen. Zentral ist regelmäßig Art. 6 Abs. 1 lit. c DSGVO, wenn die Erfassung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Ergänzend kommt § 26 Abs. 1 BDSG in Betracht, wenn die Verarbeitung für Zwecke des Beschäftigungsverhältnisses erforderlich ist, etwa zur Durchführung, Abrechnung oder Organisation der Arbeitsleistung.

Eine Einwilligung ist im Arbeitsverhältnis dagegen nur ausnahmsweise eine tragfähige Grundlage, weil sie wegen des bestehenden Abhängigkeitsverhältnisses oft nicht wirklich freiwillig ist. Für Unternehmen ist deshalb wichtig, die Zeiterfassung nicht auf „Gefälligkeit“ oder pauschale Zustimmung zu stützen, sondern auf eine belastbare Rechtsgrundlage und ein nachvollziehbares Verarbeitungskonzept.

In der Praxis sollte außerdem immer geprüft werden, ob die konkret erfassten Daten wirklich erforderlich sind. Je weniger Zusatzdaten verarbeitet werden, desto leichter lässt sich die Zeiterfassung rechtssicher und transparent ausgestalten.

Praktische Einordnung für Unternehmen

Für die tägliche Praxis bedeutet das: Arbeitszeitdaten sollten klar beschrieben, auf das notwendige Maß begrenzt und mit sauberen Zugriffs- und Löschkonzepten versehen werden. Unternehmen sollten außerdem dokumentieren, welche Daten zu welchem Zweck verarbeitet werden und wer darauf zugreifen darf. Das schafft nicht nur Transparenz gegenüber Beschäftigten, sondern erleichtert auch die interne Kontrolle und spätere Nachweise.

Wer Zeiterfassungssysteme einführt oder anpasst, sollte deshalb nicht nur die technische Lösung betrachten, sondern auch die datenschutzrechtliche Einordnung der einzelnen Datenkategorien. Genau an dieser Stelle entscheidet sich, ob aus einer nützlichen Arbeitszeiterfassung ein unnötig riskantes Datensystem wird.



Systeme zur Zeiterfassung im Überblick

Für die datenschutzkonforme Zeiterfassung kommt es nicht nur darauf an, dass Arbeitszeiten erfasst werden, sondern auch wie dies technisch erfolgt. Die Wahl des Systems hat direkte Auswirkungen auf Datensicherheit, Transparenz, Bedienbarkeit und den Umfang der verarbeiteten Daten. Unternehmen sollten daher bereits bei der Auswahl prüfen, ob das Modell zur eigenen Organisation, zur betrieblichen Praxis und zu den datenschutzrechtlichen Anforderungen passt.

Manuelle, digitale und mobile Zeiterfassungssysteme

Klassische manuelle Verfahren, etwa Stundenzettel oder Excel-Listen, sind zwar einfach einzuführen, bringen aber häufig Schwächen bei Nachvollziehbarkeit, Aktualität und Manipulationsschutz mit sich. Digitale Lösungen, etwa Terminals, Webportale oder Apps, bieten in der Regel mehr Automatisierung, eine bessere Auswertbarkeit und klarere Kontrollmöglichkeiten. Mobile Systeme ermöglichen zusätzlich die Erfassung unterwegs oder im Homeoffice, erhöhen aber zugleich die Anforderungen an Zugriffssteuerung, Authentifizierung und Transparenz.

Für Unternehmen stellt sich deshalb die Frage, ob eine einfache Lösung ausreicht oder ob ein System mit höherem Funktionsumfang langfristig die bessere Wahl ist. Entscheidend ist, dass die Lösung nicht mehr Daten verarbeitet als erforderlich und die Beschäftigten sie im Alltag zuverlässig nutzen können.

Cloudlösungen vs. On-Premises

Cloudbasierte Zeiterfassungssysteme sind oft flexibel, skalierbar und schnell verfügbar. Sie eignen sich besonders für Unternehmen, die mehrere Standorte haben, hybride Arbeitsmodelle unterstützen oder administrative Aufwände reduzieren wollen. Gleichzeitig müssen bei Cloudlösungen Fragen zur Auftragsverarbeitung, zum Speicherort der Daten und zu den Zugriffsmöglichkeiten des Anbieters sorgfältig geprüft werden.

On-Premises-Lösungen bieten dem Unternehmen hingegen mehr direkte Kontrolle über Infrastruktur, Datenhaltung und technische Einstellungen. Sie können datenschutzrechtlich und sicherheitstechnisch vorteilhaft sein, erfordern jedoch meist mehr internes Know-how, Wartung und Verantwortung für Betrieb und Schutzmaßnahmen.

Die Entscheidung zwischen Cloud und On-Premises ist daher nicht nur eine IT-Frage, sondern immer auch eine Frage von Governance, Risikobewertung und Compliance.

Schnittstellen zu HR- und Payroll-Systemen

In der Praxis entfalten Zeiterfassungssysteme ihren eigentlichen Nutzen häufig erst durch die Anbindung an HR-, Personal- oder Payroll-Systeme. Über Schnittstellen lassen sich Abwesenheiten, Zuschläge, Überstunden und abrechnungsrelevante Daten effizient weiterverarbeiten. Das reduziert manuelle Übertragungsfehler und verbessert die Prozesse zwischen Fachabteilungen.

Gleichzeitig steigen mit jeder Schnittstelle die datenschutzrechtlichen Anforderungen. Unternehmen müssen genau festlegen, welche Daten wohin übertragen werden, wer Zugriff erhält und wie sich Missbrauch oder Fehlkonfigurationen verhindern lassen. Schnittstellen sollten deshalb nach dem Prinzip der Datenminimierung gestaltet und technisch abgesichert werden.

Besonders wichtig ist außerdem eine saubere Rollen- und Rechteverteilung: Nicht jede Abteilung benötigt denselben Zugriff auf Zeiterfassungsdaten. Eine klare Begrenzung sorgt hier für Transparenz und reduziert unnötige Risiken.

Auswahl mit Augenmaß

Bei der Auswahl eines Zeiterfassungssystems sollten Unternehmen nicht nur auf Funktionsumfang und Preis achten, sondern auch auf Datenschutz, Informationssicherheit und Integrationsfähigkeit. Ein gutes System ist nicht das mit den meisten Funktionen, sondern dasjenige, dass die betrieblichen Anforderungen effizient erfüllt und zugleich datenschutzkonform betrieben werden kann.

Gerade für kleine und mittelständische Unternehmen empfiehlt sich eine Lösung, die praktikabel, verständlich und wartungsarm ist. So lassen sich Arbeitszeiterfassung und Datenschutz in einem System verbinden, ohne den betrieblichen Alltag unnötig zu belasten.



Datenschutzrisiken und typische Fehlerquellen

Zeiterfassungssysteme sind im Unternehmen ein wichtiges Steuerungsinstrument – sie können aber schnell zum datenschutzrechtlichen Risikofaktor werden, wenn sie zu weit in das Verhalten der Beschäftigten hineinwirken. Besonders kritisch ist, dass aus einer reinen Arbeitszeiterfassung ungewollt ein Kontrollsystem wird, das mehr über Anwesenheit, Leistung oder Bewegung verrät als eigentlich erforderlich. Genau hier entstehen in der Praxis die häufigsten Fehler.

Unzulässige Leistungs- und Verhaltenskontrolle

Ein Zeiterfassungssystem darf in erster Linie dazu dienen, Arbeitszeiten korrekt zu dokumentieren und gesetzliche Vorgaben einzuhalten. Es ist jedoch unzulässig, daraus ein Instrument zur permanenten Leistungs- oder Verhaltenskontrolle zu machen. Problematisch wird es etwa dann, wenn Vorgesetzte minutengenau nachvollziehen können, wann Beschäftigte welche Tätigkeit ausgeführt haben oder wenn aus Bewegungs- und Buchungsdaten Rückschlüsse auf Arbeitsverhalten gezogen werden.

Für Unternehmen bedeutet das: Je detaillierter die Auswertung, desto größer das Risiko eines unzulässigen Eingriffs in die Persönlichkeitsrechte der Beschäftigten. Deshalb sollte bereits bei der Systemauswahl klar festgelegt werden, welche Auswertungen zulässig sind und welche bewusst unterbleiben müssen.

Übermäßige Datenerhebung und Dauerüberwachung

Nicht jede technisch mögliche Funktion ist auch datenschutzrechtlich zulässig oder betrieblich sinnvoll. Gerade moderne Zeiterfassungslösungen bieten häufig Zusatzfunktionen wie GPS-Ortung, Standortprotokolle, biometrische Verfahren oder detaillierte Aktivitätslogs. Solche Funktionen können in bestimmten Fällen zwar nützlich sein, führen aber schnell zu einer übermäßigen Datenerhebung und damit zu einem unverhältnismäßigen Eingriff.

Auch eine dauerhafte Überwachung des Aufenthaltsorts oder des Arbeitsverhaltens ist regelmäßig nicht erforderlich, um Arbeitszeiten zu erfassen. Unternehmen sollten daher konsequent prüfen, welche Daten wirklich gebraucht werden und welche Informationen besser gar nicht erst erhoben werden. Das Prinzip der Datenminimierung ist hier nicht nur ein Datenschutzgrundsatz, sondern ein praktischer Schutz vor unnötigen Konflikten.

Datenschutzrisiken und typische Fehlerquellen

Fehlende Transparenz gegenüber Beschäftigten

Ein weiterer häufiger Fehler besteht darin, Zeiterfassungssysteme einzuführen, ohne die Beschäftigten ausreichend zu informieren. Wer nicht weiß, welche Daten erfasst werden, zu welchem Zweck dies geschieht und wer Zugriff darauf hat, empfindet das System schnell als intransparent oder sogar kontrollierend. Das kann zu Akzeptanzproblemen, Rückfragen und Konflikten im Betrieb führen.

Transparenz bedeutet deshalb mehr als nur eine kurze Information im Intranet. Beschäftigte sollten verständlich darüber informiert werden, welche Daten verarbeitet werden, wie lange diese gespeichert bleiben und welche Rechte sie haben. Je klarer die Regeln kommuniziert werden, desto eher wird Zeiterfassung als legitimer und fairer Bestandteil des Arbeitsalltags akzeptiert.

Typische Risiken in der Praxis

Besonders häufig entstehen Probleme durch unklare Berechtigungskonzepte, fehlende Löschregeln oder eine zu weitgehende Verknüpfung mit anderen Personalprozessen. Wenn Zeiterfassungsdaten etwa ohne klare Zweckbindung für Leistungsbewertungen, Disziplinarmaßnahmen oder Verhaltensanalysen genutzt werden, steigt das Risiko datenschutzrechtlicher Verstöße erheblich.

Unternehmen sollten deshalb nicht nur das System selbst prüfen, sondern auch die internen Prozesse rund um Erfassung, Auswertung und Zugriff. Eine datenschutzkonforme Zeiterfassung lebt nicht allein von der Technik, sondern vor allem von klaren Regeln, nachvollziehbaren Zuständigkeiten und einem bewussten Umgang mit den erhobenen Daten.

Technische und organisatorische Datensicherheitsmaßnahmen (TOM)



Technische und organisatorische Maßnahmen (TOM)

Technische und organisatorische Maßnahmen sind das Fundament einer datenschutzkonformen Zeiterfassung. Sie sorgen dafür, dass Arbeitszeitdaten nur von den Personen verarbeitet werden, die dies tatsächlich dürfen, und dass die Daten vor Verlust, Manipulation oder unbefugtem Zugriff geschützt bleiben. Gerade bei Zeiterfassungssystemen ist das besonders wichtig, weil hier regelmäßig personenbezogene Daten von Beschäftigten verarbeitet werden und die Systeme oft in größere Personal- oder IT-Umgebungen eingebunden sind.

Zugriffskontrollen und Berechtigungskonzepte

Ein zentrales Element der TOM sind klare Zugriffskontrollen. Nicht jeder Mitarbeitende und nicht jede Führungskraft benötigt Zugriff auf dieselben Daten oder dieselben Auswertungen. Deshalb sollte genau definiert werden, wer Arbeitszeiten erfassen, korrigieren, freigeben oder einsehen darf.

Ein gutes Berechtigungskonzept orientiert sich am Prinzip der Erforderlichkeit: Wer keine Aufgabe in Bezug auf die Zeiterfassung hat, erhält auch keinen Zugriff. So lassen sich unnötige Einsichten in Beschäftigtendaten vermeiden und interne Risiken deutlich reduzieren.

Zusätzlich sollten Rollen regelmäßig überprüft und bei Personalwechseln oder Funktionsänderungen zeitnah angepasst werden. Veraltete Berechtigungen gehören zu den häufigsten Schwachstellen in der Praxis.

Protokollierung und Integrität der Daten

Damit Zeiterfassungsdaten nachvollziehbar und belastbar bleiben, müssen Änderungen und Zugriffe in geeigneter Form protokolliert werden. Protokolle helfen dabei, nachzuvollziehen, wann Daten erfasst, geändert oder gelöscht wurden. Das ist nicht nur für interne Kontrollen wichtig, sondern auch für die Klärung von Abweichungen oder Streitfällen.

Ebenso relevant ist die Integrität der Daten. Arbeitszeitangaben dürfen nicht unbemerkt verändert werden können. Systeme sollten daher Manipulationen erkennen oder zumindest erschweren, etwa durch Änderungsprotokolle, Freigabeprozesse oder revisionssichere Ablagen.

Für Unternehmen bedeutet das: Nur wenn Zeiterfassungsdaten nachvollziehbar und verlässlich sind, können sie als Grundlage für Abrechnung, Nachweise und organisatorische Entscheidungen dienen.

Verschlüsselung und sichere Speicherung

Arbeitszeitdaten sollten sowohl bei der Übertragung als auch bei der Speicherung angemessen geschützt werden. Verschlüsselung ist dabei ein wesentlicher Baustein, um unbefugten Zugriff auf sensible Beschäftigtendaten zu verhindern. Das gilt insbesondere bei webbasierten oder mobilen Zeiterfassungslösungen sowie bei Cloudsystemen.

Ebenso wichtig ist eine sichere Speicherung mit regelmäßig überprüften Backups, einem kontrollierten Berechtigungskonzept und klaren Löschregeln. Daten, die nicht mehr benötigt werden, dürfen nicht unbegrenzt im System verbleiben.

Unternehmen sollten außerdem darauf achten, dass auch Schnittstellen zu anderen Systemen abgesichert sind. Denn jedes angebundene System kann eine zusätzliche Angriffsfläche darstellen, wenn Schutzmaßnahmen nicht konsequent umgesetzt werden.

TOM als laufende Aufgabe

Technische und organisatorische Maßnahmen sind kein einmaliges Projekt, sondern ein fortlaufender Prozess. Systeme, Berechtigungen und Sicherheitsanforderungen verändern sich mit der Zeit, weshalb regelmäßige Überprüfungen erforderlich sind.

Eine datenschutzkonforme Zeiterfassung funktioniert daher nur dann dauerhaft gut, wenn Technik, Organisation und Verantwortlichkeiten zusammen gedacht werden. Genau darin liegt der Unterschied zwischen einer formalen Lösung und einem wirklich belastbaren Datenschutzkonzept.

Mitbestimmung und Beteiligung des Betriebsrats

Die Einführung und Ausgestaltung von Zeiterfassungssystemen betreffen nicht nur den Datenschutz, sondern häufig auch die Mitbestimmungsrechte des Betriebsrats. Immer dann, wenn technische Einrichtungen dazu geeignet sind, das Verhalten oder die Leistung von Beschäftigten zu überwachen, ist eine enge Abstimmung mit der Arbeitnehmervertretung erforderlich. Für Unternehmen ist das wichtig, weil Zeiterfassungssysteme in der Praxis oft genau diese Möglichkeit mitbringen – selbst, wenn sie ursprünglich nur zur Arbeitszeitdokumentation eingeführt wurden.

Rechte des Betriebsrats nach § 87 BetrVG

Nach § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, Verhalten oder Leistung der Beschäftigten zu überwachen. Dieses Recht greift regelmäßig auch bei Zeiterfassungssystemen, wenn etwa Zeitbuchungen, Standortdaten oder Auswertungen Rückschlüsse auf das Arbeitsverhalten zulassen.

Daneben können je nach Ausgestaltung weitere Mitbestimmungstatbestände relevant sein, etwa bei Beginn und Ende der täglichen Arbeitszeit, bei Pausenregelungen oder bei der Verteilung von Arbeitszeit im Betrieb. Unternehmen sollten daher nicht nur die technische Lösung prüfen, sondern auch frühzeitig klären, welche mitbestimmungsrechtlichen Fragen damit verbunden sind.

In der Praxis bedeutet das: Eine Zeiterfassungslösung sollte möglichst nicht „fertig eingeführt“ werden, bevor die betriebliche Mitbestimmung sauber berücksichtigt wurde.

Gestaltung von Betriebsvereinbarungen

Eine Betriebsvereinbarung ist oft das passende Instrument, um die Nutzung eines Zeiterfassungssystems rechtssicher und praktikabel zu regeln. Sie schafft verbindliche Vorgaben für Erfassungsumfang, Zugriffsrechte, Auswertungen, Löschfristen und Kontrollmechanismen. Zugleich hilft sie dabei, die Interessen von Arbeitgeber und Beschäftigten in ein ausgewogenes Verhältnis zu bringen.

Wichtig ist, dass die Vereinbarung nicht zu allgemein formuliert wird. Sie sollte konkret regeln, welche Daten erfasst werden, wer darauf zugreifen darf, zu welchen Zwecken eine Auswertung erfolgt und welche Nutzungen ausdrücklich ausgeschlossen sind. Je klarer diese Punkte definiert sind, desto geringer ist das Risiko späterer Konflikte.

Auch datenschutzrechtlich ist eine saubere Betriebsvereinbarung hilfreich, weil sie Transparenz schafft und die interne Umsetzung verbindlich strukturiert.

Praxisbeispiele für datenschutzkonforme Regelungen

Datenschutzkonforme Regelungen in einer Betriebsvereinbarung können etwa vorsehen, dass nur die tatsächlich erforderlichen Arbeitszeitdaten erfasst werden und keine dauerhafte Standortüberwachung stattfindet. Ebenso kann festgelegt werden, dass Führungskräfte nur auf die für ihre Aufgaben notwendigen Informationen zugreifen dürfen und keine individuellen Detailauswertungen zu Leistungszwecken erhalten.

Sinnvoll sind außerdem Regelungen zu Protokollierung, Korrekturen und Löschung. So kann beispielsweise bestimmt werden, dass Änderungen an Zeitbuchungen dokumentiert werden, dass Korrekturen nur durch berechtigte Personen erfolgen und dass Daten nach Ablauf der gesetzlichen oder betrieblich festgelegten Fristen gelöscht werden.

Ein weiterer praxisnaher Ansatz ist die Beschränkung von Reports und Auswertungen auf aggregierte oder anonymisierte Daten, sofern keine personenbezogene Detailansicht erforderlich ist. Dadurch lässt sich die Steuerungsfunktion der Zeiterfassung erhalten, ohne unnötig tief in die Privatsphäre der Beschäftigten einzugreifen.

Mitbestimmung als Erfolgsfaktor

Wenn Betriebsrat und Unternehmensleitung Zeiterfassung gemeinsam gestalten, steigt die Akzeptanz im Betrieb deutlich. Beschäftigte erleben das System dann eher als fair, nachvollziehbar und zweckgebunden. Für Unternehmen ist das nicht nur rechtlich sinnvoll, sondern auch organisatorisch vorteilhaft, weil so spätere Nachbesserungen und Konflikte vermieden werden können.

Eine frühzeitige Beteiligung des Betriebsrats ist deshalb kein Hemmnis, sondern ein wichtiger Baustein für eine belastbare und praxistaugliche Lösung.

Informationspflichten und Transparenz



Informationspflichten und Transparenz

Eine datenschutzkonforme Zeiterfassung setzt nicht nur eine zulässige Rechtsgrundlage und sichere Technik voraus, sondern auch eine verständliche Information der Beschäftigten. Gerade bei Arbeitszeitdaten ist Transparenz besonders wichtig, weil die Betroffenen unmittelbar nachvollziehen können müssen, welche Angaben erfasst werden und wofür sie verwendet werden. Die Informationspflichten nach Art. 13 DSGVO gehören deshalb zu den zentralen Voraussetzungen einer rechtssicheren Umsetzung.

Umsetzung von Art. 13 DSGVO bei Zeiterfassungssystemen

Bei der Einführung oder Änderung eines Zeiterfassungssystems müssen Beschäftigte darüber informiert werden, welche personenbezogenen Daten verarbeitet werden, zu welchem Zweck dies geschieht und auf welcher Rechtsgrundlage die Verarbeitung beruht. Dazu gehören in der Regel auch Angaben zu Empfängern, Speicherdauer, möglichen Auftragsverarbeitern und den Rechten der betroffenen Personen.

In der Praxis sollte die Information möglichst vor oder spätestens bei Beginn der Verarbeitung erfolgen. Das kann über eine Mitarbeiterinformation, eine Datenschutzrichtlinie, eine Betriebsvereinbarung oder eine Kombination dieser Dokumente umgesetzt werden. Wichtig ist, dass die Informationen vollständig, aktuell und gut auffindbar sind.

Verständliche Mitarbeiterinformationen

Eine gute Mitarbeiterinformation ist nicht nur formal korrekt, sondern auch sprachlich klar und alltagstauglich. Beschäftigte sollten auf einen Blick verstehen können, welche Daten erfasst werden, ob etwa Pausen, Überstunden oder Abwesenheiten dokumentiert werden und wer Zugriff auf die Daten hat.

Besonders hilfreich ist eine Struktur in kurzen Abschnitten mit klaren Überschriften. So lassen sich Zweck, Rechtsgrundlage, Speicherfristen und Ansprechpartner einfach erfassen. Wenn Unternehmen zusätzlich Beispiele oder kurze Erläuterungen verwenden, steigt die Akzeptanz des Systems meist deutlich.

Unklare oder zu technische Formulierungen führen dagegen schnell zu Rückfragen und Misstrauen. Transparenz bedeutet deshalb nicht nur rechtliche Korrektheit, sondern auch Verständlichkeit.

Informationspflichten und Transparenz

Dokumentation und Nachweisführung

Unternehmen sollten nicht nur informieren, sondern die Informationspflichten auch dokumentieren. Das ist wichtig, um gegenüber Aufsichtsbehörden, Betriebsrat oder im internen Audit nachweisen zu können, dass die Informationsanforderungen tatsächlich erfüllt wurden.

Sinnvoll ist es, die verwendeten Datenschutzhinweise, Versionsstände, Verteilwege und Freigaben nachvollziehbar zu archivieren. Auch Änderungen an Zeiterfassungssystemen sollten dokumentiert werden, damit klar bleibt, welche Informationen zu welchem Zeitpunkt galten.

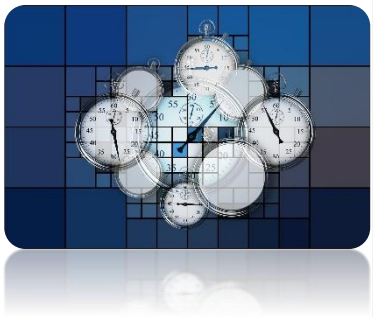
Ebenso wichtig ist eine saubere Ablage der Rechtsgrundlagen, etwa einer Betriebsvereinbarung oder der internen Verfahrensbeschreibung. So lässt sich später leicht belegen, dass Transparenz nicht nur behauptet, sondern auch organisatorisch umgesetzt wurde.

Transparenz als Vertrauensbasis

Gerade bei Zeiterfassungssystemen entscheidet Transparenz wesentlich über die Akzeptanz im Betrieb. Wer nachvollziehen kann, welche Daten verarbeitet werden und warum, empfindet die Lösung eher als fair und legitim. Für Unternehmen ist das ein klarer Vorteil, weil weniger Unsicherheit, weniger Konflikte und eine bessere Zusammenarbeit entstehen.

Transparenz ist damit nicht bloß eine DSGVO-Pflicht, sondern auch ein praktischer Erfolgsfaktor für die Einführung und den Betrieb von Zeiterfassungslösungen.

Speicherfristen und Löschkonzepte



Speicherfristen und Löschkonzepte

Arbeitszeitdaten dürfen nicht unbegrenzt gespeichert werden. Für eine datenschutzkonforme Zeiterfassung ist deshalb von Anfang an festzulegen, wie lange welche Daten aufbewahrt werden und wann sie zu löschen sind. Maßgeblich sind dabei sowohl gesetzliche Aufbewahrungspflichten als auch das Datenschutzprinzip der Speicherbegrenzung, nach dem personenbezogene Daten nur so lange gespeichert werden dürfen, wie sie für den jeweiligen Zweck erforderlich sind.

Gesetzliche Aufbewahrungspflichten

Eine wichtige Grundlage ist § 16 Abs. 2 ArbZG. Danach sind Arbeitszeitnachweise grundsätzlich mindestens zwei Jahre aufzubewahren, soweit sie zur Dokumentation über die werktägliche Arbeitszeit hinaus erforderlich sind. Hinzu kommen weitere Aufbewahrungsfristen, wenn Arbeitszeitdaten zugleich für andere Zwecke genutzt werden, etwa für die Lohnabrechnung oder für Nachweise gegenüber Behörden.

Für Unternehmen bedeutet das: Nicht jede Zeiterfassung kann pauschal gleichbehandelt werden. Je nach Verwendungszweck können unterschiedliche Fristen gelten, die sauber voneinander getrennt und dokumentiert werden sollten.

Löschfristen für Arbeitszeitdaten

Aus datenschutzrechtlicher Sicht sollten Löschfristen nicht nur an gesetzlichen Mindestfristen orientiert sein, sondern auch an der praktischen Erforderlichkeit. Wenn Arbeitszeitdaten für die Abrechnung, für Nachweise oder zur Geltendmachung möglicher Ansprüche benötigt werden, kann eine längere Speicherung zulässig sein. Sobald der Zweck entfällt, müssen die Daten jedoch gelöscht oder zumindest sicher archiviert werden.

In der Praxis hat sich daher eine differenzierte Betrachtung bewährt: Reine Arbeitszeitnachweise werden getrennt von lohnrelevanten Unterlagen oder steuerlich relevanten Dokumenten behandelt. So lässt sich vermeiden, dass Daten länger vorgehalten werden als notwendig.

Umsetzung in der Praxis

Ein funktionierendes Löschkonzept beginnt mit einer klaren Kategorisierung der Daten. Unternehmen sollten unterscheiden zwischen reinen Arbeitszeitnachweisen, abrechnungsrelevanten Daten, Korrekturen, Protokollen und Archivdaten. Für jede Kategorie sollte eine konkrete Frist festgelegt werden, die sich aus Gesetz, Zweck und internen Prozessen ableiten lässt.

Wichtig ist außerdem, dass Löschungen tatsächlich technisch umgesetzt werden. Dazu gehören automatisierte Fristen im System, Löschroutinen für produktive Daten und eine Berücksichtigung von Backups und Archiven. Werden Daten nur „aus dem Sichtbereich“ entfernt, aber technisch weiter vorgehalten, ist das datenschutzrechtlich noch keine echte Löschung.

Sinnvoll ist zudem eine dokumentierte Löschroutine mit Verantwortlichkeiten, damit nachvollziehbar bleibt, wann welche Daten gelöscht wurden und wer die Freigabe erteilt hat. Gerade bei Beschäftigtendaten ist eine saubere Nachweisführung wichtig, um interne und externe Prüfungen bestehen zu können.

Praxisnahe Leitlinie

Für Unternehmen empfiehlt sich eine einfache Grundregel: so kurz wie möglich, so lang wie nötig. Arbeitszeitdaten sollten nur solange gespeichert werden, wie es für den gesetzlichen Nachweis, die Abrechnung oder die Verteidigung möglicher Ansprüche erforderlich ist. Danach gehören sie in ein geregeltes Lösch- oder Archivverfahren.

Ein klar dokumentiertes Löschkonzept reduziert nicht nur Datenschutzrisiken, sondern schafft auch Ordnung im Umgang mit Personaldaten und entlastet die Systeme dauerhaft.



Kontrolle, Audit und kontinuierliche Verbesserung

Eine datenschutzkonforme Zeiterfassung endet nicht mit der Einführung eines Systems. Erst durch regelmäßige Kontrollen, dokumentierte Prüfungen und eine laufende Anpassung an technische und rechtliche Entwicklungen wird aus der reinen Erfassung ein belastbarer Compliance-Prozess. Gerade bei Arbeitszeitdaten ist es wichtig, nicht nur die formale Erhebung sicherzustellen, sondern auch die tatsächliche Nutzung, den Zugriff und die Auswertung im Blick zu behalten. Unternehmen sollten Zeiterfassung deshalb als festen Bestandteil ihrer Datenschutz- und Organisationsprozesse verstehen.

Interne Kontrollen helfen dabei, Schwachstellen frühzeitig zu erkennen. Dazu gehört beispielsweise die regelmäßige Überprüfung, ob alle Arbeitszeiten vollständig erfasst werden, ob Korrekturen nachvollziehbar dokumentiert sind und ob nur berechtigte Personen Zugriff auf die Daten haben. Auch die Frage, ob Auswertungen ausschließlich für den vorgesehenen Zweck genutzt werden, sollte Teil der Kontrolle sein. So lassen sich Fehler, organisatorische Lücken und unzulässige Verarbeitungen rechtzeitig erkennen, bevor daraus größere Risiken entstehen.

Interne Überprüfung

In der Praxis sollte Zeiterfassung nicht nur technisch, sondern auch organisatorisch überprüft werden. Sinnvoll sind feste Verantwortlichkeiten, regelmäßige Stichproben und ein klarer Prüfplan, der etwa quartalsweise oder halbjährlich angewendet wird. So lässt sich feststellen, ob das System korrekt genutzt wird, ob neue Arbeitszeitmodelle berücksichtigt sind und ob Änderungen im Unternehmen Auswirkungen auf die Verarbeitung haben. Auch bei Systemwechseln oder Anpassungen der Arbeitsabläufe sollte eine erneute Prüfung erfolgen.

Besonders wichtig ist dabei die Kontrolle von Berechtigungen. Wer Arbeitszeiten erfassen, korrigieren, auswerten oder exportieren darf, sollte eindeutig geregelt und dokumentiert sein. Änderungen an Rollen oder Zugriffsrechten müssen nachvollziehbar bleiben, damit später erkennbar ist, wer wann welche Daten bearbeitet hat. Auch die Überprüfung der Datenqualität gehört dazu, etwa bei vergessenen Buchungen, Doppelbuchungen oder fehlerhaften Korrekturen. Je klarer diese Prozesse geregelt sind, desto geringer ist das Risiko von Fehlern und Missbrauch.

Kontrolle, Audit und kontinuierliche Verbesserung

Auditierbarkeit des Systems

Ein Zeiterfassungssystem sollte so aufgebaut sein, dass es interne und externe Prüfungen unterstützt. Dafür braucht es nachvollziehbare Protokolle, eine transparente Datenhistorie und eine klare Trennung zwischen Erfassung, Korrektur und Auswertung. Besonders hilfreich sind Systeme, die Änderungen mit Zeitstempel, Benutzerkennung und Änderungsgrund dokumentieren. Nur so lässt sich im Nachhinein nachvollziehen, wie Daten entstanden sind und wer sie verändert hat.

Für ein Audit ist außerdem wichtig, dass die Aufbewahrung und Löschung geregelt sind. Unternehmen sollten nachweisen können, wie lange welche Arbeitszeitdaten gespeichert werden, aus welchem Grund dies geschieht und wann die Löschung erfolgt. Eine saubere Dokumentation erleichtert nicht nur interne Kontrollen, sondern auch die Zusammenarbeit mit Datenschutzbeauftragten, Betriebsrat oder Aufsichtsbehörden. So wird aus der Zeiterfassung ein nachvollziehbarer und belastbarer Bestandteil der Unternehmenscompliance.

Kennzahlen und Nachweise

Zur kontinuierlichen Verbesserung gehört auch die Auswertung geeigneter Kennzahlen. Dazu können etwa der Anteil vollständig erfasster Arbeitszeiten, die Anzahl manueller Korrekturen, die Häufigkeit verspäteter Nachträge oder die Zahl unberechtigter Zugriffsversuche gehören. Solche Kennzahlen machen sichtbar, ob das System im Alltag zuverlässig funktioniert und wo organisatorische Maßnahmen nötig sind. Sie können auch dabei helfen, Trends frühzeitig zu erkennen und Abläufe gezielt zu verbessern.

Für die Praxis empfiehlt sich eine kurze Compliance-Dokumentation, die die wichtigsten Punkte zusammenführt: Rechtsgrundlage, Zweck, Zugriffsberechtigungen, Aufbewahrungsfristen, Löschkonzept, Informationspflichten und technische Schutzmaßnahmen.

So entsteht ein belastbarer Nachweis, dass Zeiterfassung nicht nur eingeführt, sondern auch kontrolliert und weiterentwickelt wird. Wer diese Nachweise regelmäßig pflegt, schafft Transparenz und kann im Fall einer Prüfung deutlich besser reagieren.

Ausblick und Handlungsempfehlungen

Ausblick auf die digitale Zeiterfassung

Die Zeiterfassung entwickelt sich zunehmend in Richtung digitaler, mobiler und stärker integrierter Systeme. Für Unternehmen bedeutet das mehr Komfort und bessere Auswertungsmöglichkeiten, aber auch höhere Anforderungen an Datenschutz, Transparenz und technische Sicherheit. Gerade kleine und mittelständische Unternehmen müssen darauf achten, nur die wirklich erforderlichen Daten zu verarbeiten.

Immer häufiger werden Zeiterfassungssysteme mit HR- oder Payroll-Lösungen verbunden. Das erleichtert Abläufe, schafft aber auch zusätzliche Datenflüsse, die sauber geregelt und geschützt werden müssen. Je stärker ein System vernetzt ist, desto wichtiger sind klare Berechtigungen und eine saubere Trennung zwischen Zeiterfassung und Leistungsbewertung.

Mobiles Erfassen per App oder Weboberfläche wird ebenfalls wichtiger. Das ist flexibel, verlangt aber besondere Aufmerksamkeit bei Übertragung, Speicherung und Zugriffsschutz. Entscheidend ist, dass die Lösung nicht nur praktisch, sondern auch datensparsam und rechtssicher ist.

Handlungsempfehlungen für kleine und mittelständische Unternehmen

KMU sollten Zeiterfassung nicht nur technisch, sondern auch organisatorisch betrachten. Vor der Einführung oder Anpassung eines Systems sollte geprüft werden, welche Arbeitszeitmodelle tatsächlich abgebildet werden müssen und welche Daten dafür wirklich nötig sind. So lässt sich vermeiden, dass unnötig komplexe oder datenschutzkritische Lösungen eingesetzt werden.

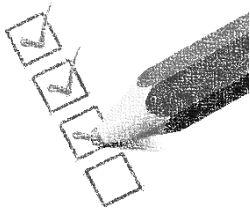
Ebenso wichtig ist die klare Verteilung von Verantwortlichkeiten. Wer pflegt Stammdaten, wer prüft Zeitkorrekturen, wer gibt Auswertungen frei und wer ist für Datenschutzfragen zuständig?

Ohne eindeutige Zuständigkeiten entstehen schnell Fehler oder unzulässige Zugriffe. Eine kurze schriftliche Regelung schafft hier oft mehr Sicherheit als eine technisch gute, aber organisatorisch unklare Lösung.

Auch die Kommunikation mit den Beschäftigten sollte nicht zu kurz kommen. Wenn Mitarbeitende verstehen, welche Daten erfasst werden, warum dies geschieht und wer Zugriff darauf hat, steigt die Akzeptanz deutlich. Transparenz ist daher nicht nur eine Pflicht, sondern ein wichtiger Erfolgsfaktor für eine professionelle und rechtssichere Umsetzung.

Ausblick und Handlungsempfehlungen

Checkliste zur datenschutzkonformen Umsetzung der Zeiterfassung



- **Zweck festlegen:** Definieren Sie klar, warum die Zeiterfassung erfolgt.
- **Datenumfang prüfen**: Erfassen Sie nur die Daten, die für den Zweck wirklich erforderlich sind.
- **Rechtsgrundlage dokumentieren**: Halten Sie nachvollziehbar fest, auf welcher Rechtsgrundlage die Verarbeitung erfolgt.
- **Informationspflichten erfüllen**: Beschäftigte müssen verständlich darüber informiert werden, welche Daten verarbeitet werden, zu welchen Zwecken dies geschieht, wie lange die Daten gespeichert werden und wer Empfänger der Daten sein kann.
- **Zugriffsrechte begrenzen**: Stellen Sie sicher, dass nur berechtigte Personen auf Zeitdaten zugreifen können.
- **Korrekturprozesse regeln**: Legen Sie fest, wie fehlerhafte Buchungen, vergessene Einträge oder nachträgliche Änderungen bearbeitet werden.
- **Protokollierung sicherstellen**: Das System sollte nachvollziehbar festhalten, wer welche Änderungen vorgenommen hat.
- **Aufbewahrungsfristen festlegen**: Definieren Sie, wie lange Arbeitszeitdaten gespeichert werden und wann eine Löschung erfolgt.
- **Löschkonzept umsetzen**: Speicherung der Daten nicht länger als nötig.
- **Technische Schutzmaßnahmen prüfen**: Achten Sie auf Verschlüsselung, sichere Übertragung, Zugriffsschutz, Passwortsicherheit und eine geschützte Speicherung der Daten.
- **Auftragsverarbeitung kontrollieren**: Wenn externe Anbieter eingesetzt werden, muss geprüft werden, ob ein AV-Vertrag erforderlich ist und ob der Dienstleister geeignete Sicherheitsmaßnahmen bietet.
- **Betriebsrat einbinden**: Falls ein Betriebsrat vorhanden ist, sollte die Einführung oder Änderung des Systems frühzeitig abgestimmt werden.
- **Mitarbeitende schulen**: Erklären Sie, wie das System funktioniert, welche Meldewege es bei Fehlern gibt und welche Regeln für Korrekturen oder mobile Buchungen gelten.
- **Regelmäßige Überprüfung durchführen**: Kontrollieren Sie stetig, ob das System korrekt, sicher und zweckgebunden eingesetzt wird.
- **Verantwortlichkeiten dokumentieren**: Halten Sie schriftlich fest, wer fachlich und organisatorisch für das System zuständig ist.

Praktischer Abschluss

Eine gut umgesetzte Zeiterfassung schafft nicht nur Rechtssicherheit, sondern auch Klarheit im Arbeitsalltag. Unternehmen, die auf eine datensparsame, transparente und kontrollierbare Lösung setzen, erfüllen die gesetzlichen Anforderungen und stärken zugleich das Vertrauen ihrer Beschäftigten.

Juli | 2026



Impressum

NBW Beratungsgesellschaft mbH
Alstadener Str. 27
46049 Oberhausen
Tel.: +49 (0208) 20770700
Web: https://www.nbw-beratung.com/
E-Mail: Kontakt@NBW-Beratung.com

Handelsregister:
Duisburg Nr.35757
NBW Beratungsgesellschaft mbH
Geschäftsführer: Burghard Wolf

Haftungsausschluss
Mit dieser Broschüre soll ein Überblick über aktuelle Datenschutz-Themen vermittelt werden. Die Informationen haben nicht den Anspruch einer Rechtsberatung. Die Verantwortung liegt immer beim umsetzenden Unternehmen. Eine Haftung für Fehler jeder Art wird ausgeschlossen.

Redaktion
NBW-Beratung: Bereich Datenschutz

Bildnachweise
Diese Unterlage wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, in 97491 Aidhausen erstellt. Alle verwendeten Bilder sind von https://pixabay.com/de/ einer Plattform für lizenzfreie Bilder.

Nutzung von künstlicher Intelligenz
Bei der Recherche und zur Kontrolle der Richtigkeit der Aussagen, wurde bei der Erstellung dieser Unterlage zum Teil auf KI zurückgegriffen.