Handlungshilfe Beschäftigten-datenschutz bei betrieblichen Digitalisierungsprojekten –

Strategien für Arbeitgeber und Beschäftigte

Impressum

Autoren:

Frank Steinwender, TBS NRW
Markus Dempki, TBS NRW
Dr. Urs Peter Ruf, TBS NRW

Grafik/Layout:

Vera Kurilo, TBS NRW

Bilder:

© Cover: BGStock72-stock.adobe.com, © pexels.com/@cottonbro,
© Microstocker.Pro-stock.adobe.com, © rawpixel.com,
© unsplash.com/@visualsbyroyalz, © Gina Sanders-stock.adobe.com,
© WavebreakMediaMicro-stock.adobe.com, © pexels.com/@fauxels,
© pixabay.com/@elvtimemaster

Herausgeber:

Technologieberatungsstelle beim DGB NRW e.V.
Westenhellweg 92–94 | 44137 Dortmund

Tel. 0231 249 69 80
www.tbs-nrw.de

Dortmund, Oktober 2021

Gefördert vom

**Ministerium für Arbeit,
Gesundheit und Soziales
des Landes Nordrhein-Westfalen**

INHALT

Vorwort

Liebe Leserinnen und Leser,

sind die Regelungen des Beschäftigtendatenschutzes Fluch oder Segen in einer digitalen Arbeitswelt? Sind sie ein Bremsklotz für Innovation im Betrieb, oder bieten sie verlässliche Leitplanken im Umgang mit den Daten der Mitarbeiterinnen und Mitarbeiter? Über diese Fragen lässt sich lang und breit diskutieren. In den Unternehmen geht derweil die Digitalisierung weiter voran und die Betriebsparteien sind bestrebt, im Rahmen der bestehenden Regelungen gute und praxisnahe Lösungen zu finden.

Die Veröffentlichung, die Sie gerade in den Händen halten, unterstützt Sie bei diesem pragmatischen Weg. Die TBS NRW zeigt Ihnen bewährte Wege auf, wie Unternehmensleitungen und Beschäftigte bei anstehenden Digitalisierungsprojekten gemeinsam und strukturiert die wichtigsten Fragen des Beschäftigtendatenschutzes klären können: Welche Personen sollen in den Prozess einbezogen werden? Welche Daten sollen zu welchem Zweck erfasst und verarbeitet werden? Wie kommen wir zu einer tragfähigen Einigung, die uns als Basis für das betriebliche Digitalisierungsprojekt dient? Kompetente Antworten auf diese und viele weitere Fragen finden Sie in dieser Broschüre.

Diese Publikation ist jedoch nicht nur ein Wegweiser durch den Beschäftigtendatenschutz. Sie ist auch eine Einladung an Unternehmensleitungen, Betriebsräte, Beschäftigte, IT-Fachleute und Datenschutzbeauftragte, Digitalisierungsprojekte als Gemeinschaftsvorhaben zu verstehen und von vorneherein auf Kooperation zu setzen. Wir sind überzeugt, dass sich in diesem Geist nicht nur die anstehenden Datenschutzfragen deutlich schneller klären lassen, sondern Digitalisierungsprojekte auch von allen mitgetragen und daher erfolgreicher realisiert werden können.

Wir wünschen Ihnen alles Gute für Ihre Digitalisierungsvorhaben und hoffen, dass diese Broschüre Ihnen den Weg durch die Welt des Beschäftigtendatenschutzes erleichtert.

Ihre

Initiative Wirtschaft & Arbeit 4.0

Wer wir sind: Die Initiative Wirtschaft & Arbeit 4.0 bestehend aus Landesregierung, Wissenschaft und Sozialpartnern versteht Technologieentwicklung als einen gestaltbaren Prozess. Für die Initiative ist es ein zentrales Anliegen, digitale Transformation und Arbeitsgestaltung gleichermaßen im Blick zu haben.

Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

IG Metall Bezirk Nordrhein-Westfalen

NRW DGB

unternehmer nrw

Bundesagentur für Arbeit Regionaldirektion Nordrhein-Westfalen

IHK NRW

Westdeutscher Handwerkskammertag

baua: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin

alanus hochschule

Fraunhofer IEM

it's owl

1. Digitalisierung und Datenschutz

1.1. Digitalisierung und Datenschutz zusammendenken

Digitale Technologien sind in der Arbeits- und Lebenswelt mittlerweile allgegenwärtig. Die Digitalisierung ermöglicht in immer kürzeren Abständen schnellere Kommunikation sowie die Erfassung, Vernetzung und Verarbeitung einer kaum abschätzbaren Menge an Informationen. Digitale Anwendungen bieten vielfältige Chancen in einer zunehmend komplexeren Welt. Es liegt im Interesse der Unternehmen und der Beschäftigten, diese wertvollen Informationen bzw. das „digitale Gold" sicher zu verwahren und zu schützen.

Wenn hier von Chancen die Rede ist, so gelten diese sowohl für das Unternehmen und die unternehmerischen Ziele als auch für die Beschäftigten in den Unternehmen. So bietet beispielsweise eine Smartphone-App für die Zeiterfassung durchaus Vorteile. Die Beschäftigten können auch im Rahmen mobiler Arbeit jederzeit auf einfache Weise den Beginn, die Pausen und das Ende der Arbeitszeit dokumentieren. Für Unternehmen, die diese vollständige digitale Erfassung der Arbeitszeiten nutzen möchten, wird mit einer solchen App die Verwaltung der Arbeitszeitkonten ebenfalls einfacher.

Wenn wir über Daten und Schutz bzw. Sicherheit sprechen, gilt es, verschiedene Schutzinteressen zu berücksichtigen. Zum einen ist es der Schutz wichtiger Unternehmensdaten. Die Schutzmaßnahmen dieser Daten fallen unter den Begriff Datensicherheit. Zum anderen steht der Datenschutz für den Schutz der Persönlichkeitsrechte und damit für den Schutz von Personendaten. In beiden Fällen existieren gesetzliche Grundlagen. So regelt das IT-Sicherheitsgesetz (IT-SiG 2.0) die Datensicherheit bei den Unternehmen, die zur sogenannten kritischen Infrastruktur gehören. Hierzu zählen z. B. Energieversorger, Gesundheitseinrichtungen oder große Lebensmittelunternehmen. Für Unternehmen, die nicht hierzu gehören, existiert kein eigenes IT-Sicherheitsgesetz. Der Datenschutz ist im Wesentlichen in der europäischen Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) geregelt. Zusätzlich existieren bzgl. des Datenschutzes in einigen Gesetzen weitergehende Regelungen, die zu beachten sind. Hierzu zählen u. a. das Sozialgesetzbuch (SGB) oder die Abgabenordnung (AO), Regelwerke, in denen Aufbewahrungsfristen vorgegeben werden.

Diese Broschüre bietet Hilfestellungen bei der Einführung digitaler Systeme in Bezug auf die Umsetzung des Beschäftigtendatenschutzes. Sie zeigt auf, wie Unternehmen gemeinsam mit ihren Beschäftigten zu Lösungen finden. Dort, wo die Zustimmung von gesetzlichen Interessenvertretungen (Betriebsrat, Personalrat oder Mitarbeitervertretung) oder die Einwilligung von Beschäftigten erforderlich ist, wird dies explizit benannt. Fragen zum Datenschutz bezüglich der Kunden- und Lieferantendaten werden in dieser Publikation nicht thematisiert. Umfassende Hilfestellungen zur technischen Datensicherheit liefert u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI). Im Hinblick auf die Anforderungen des Datenschutzes für Geschäftspartnerinnen und Geschäftspartner finden sich hilfreiche Informationen u. a. bei den Landesdatenschutzbehörden, dem Bundesdatenschutzbeauftragten, der Datenschutzkonferenz (DSK) oder der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD).

Abbildung 1: Beschäftigtendaten

1.2. Datenschutz und Beschäftigtendatenschutz

Im Wesentlichen wird durch den Datenschutz geregelt, wie Unternehmen, Selbstständige, Behörden und Vereine mit personenbezogenen Daten umgehen müssen. Diese Regelungen sind in der Europäischen Datenschutz-Grundverordnung (DSGVO) und im Bundesdatenschutzgesetz (BDSG) verankert. Beide Rechtsnormen sind in Deutschland anzuwenden. Zu den Zielen des Datenschutzes gehört insbesondere das Recht natürlicher Personen auf den Schutz ihrer Daten.

Verantwortlich im Sinne des Datenschutzrechtes für die Verarbeitung von Beschäftigtendaten ist immer die gesetzliche Vertreterin oder der gesetzliche Vertreter des Unternehmens. Daneben existiert ein Mitbestimmungsrecht der Interessenvertretungen (Betriebs- und Personalräte sowie Mitarbeitervertretungen) bei der Verarbeitung von Daten, die zur Leistungs- und Verhaltenskontrolle geeignet sind, sowie bei Überwachungsaufgaben hinsichtlich des Datenschutzes. Der Gesetzgeber hat mit § 26 BDSG „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“ eine Vorschrift geschaffen, die den Beschäftigtendatenschutz in Deutschland gesondert regelt. Die Vorschrift ist – gegenüber den Vorschriften der EU-DSGVO – spezieller und in Bezug auf die Beschäftigtendaten vorrangig anzuwenden. Damit hat der Gesetzgeber für die Durchführung oder Beendigung eines Beschäftigungsverhältnisses die Rechtsgrundlage geschaffen.

Eine Erlaubnis, beliebige Daten zu verarbeiten, ergibt sich daraus allerdings nicht. Beschäftigtendaten, die über die Zwecke des konkreten Beschäftigungsverhältnisses hinaus verarbeitet werden sollen, bedürfen anderer Regelungen, wie Dienst- oder Betriebsvereinbarungen (Kollektivvereinbarungen) oder individuelle Einwilligungen der Beschäftigten.

Schon die Bewertung, ob § 26 BDSG eine bestimmte Datenverarbeitung rechtfertigt, kann bei den verschiedenen betrieblichen Akteurinnen und Akteuren zu unterschiedlichen Einschätzungen führen. Es bietet sich daher an, die Bewertung eines IT-Verfahrens und dessen datenschutzrechtliche Behandlung gemeinsam mit den relevanten Akteursgruppen im Unternehmen durchzuführen. Dies sind zum Beispiel Datenschutzbeauftragte, IT-Beauftragte, betroffene Beschäftigte und Betriebsräte.

1.3. Was sind Beschäftigtendaten?

Zunächst klären wir an dieser Stelle den Begriff der Beschäftigtendaten, der beim Datenschutz im Mittelpunkt steht.

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“ (s. Art. 4 EU DSGVO). Beschäftigtendaten sind ausschließlich personenbezogene Daten von Beschäftigten in einem Unternehmen. Dabei umfassen Beschäftigtendaten nicht nur Daten, die einen direkten Bezug zu einer Person haben, wie z. B. der Name oder eine E-Mail-Adresse, sondern auch alle Daten, mit denen ein Bezug zu einer natürlichen Person hergestellt werden kann (Abbildung 1: Beschäftigtendaten). Als Beschäftigte zählen nach § 26 Abs. 8 BDSG u. a. Arbeitnehmerinnen und Arbeitnehmer, leitende Angestellte, Auszubildende, Leiharbeitnehmerinnen und Leiharbeitnehmer (in der Praxis wird der Begriff Zeitarbeit verwendet), Bewerberinnen und Bewerber oder ehemalige Beschäftigte.

Der wohl wichtigste Grundsatz für die Praxis lautet: Der Datenschutz ist auf alle Beschäftigtendaten anzuwenden.

Der wohl zweitwichtigste Grundsatz für die Praxis lautet: Alle Daten, die nicht einer Person zuzuordnen sind, werden als anonym bezeichnet und fallen nicht unter den Datenschutz. Diese Daten können ohne jede Datenschutzeinschränkung verarbeitet werden.

Anonyme Daten, beispielsweise auch statistische Daten von Beschäftigten, sind oftmals für die Anwendung der sogenannten „Künstlichen Intelligenz“, z. B. bei der Mustererkennung, erforderlich.

1.4. Bedeutung der DSGVO

Mit dem Inkrafttreten der DSGVO und der damit einhergehenden Aktualisierung des BDSG im Jahr 2018 erhält der Datenschutz eine wachsende Bedeutung in den Unternehmen. Als EU-Richtlinie ist die DSGVO EU-weit verbindlich. Nationale Regelungen können diese nur ergänzen und konkretisieren, nicht aber das Schutzniveau der DSGVO unterschreiten.

Die Ziele der DSGVO sind gleichermaßen der Schutz der Persönlichkeitsrechte bei der Verarbeitung personenbezogener Daten sowie der freie Verkehr personenbezogener Daten in der EU.

Ein größeres Gewicht hat der Datenschutz auch durch die in der DSGVO festgelegten hohen Geldbußen für Verstöße bekommen. So sind Bußgelder durch die Behörden bei Verstößen verpflichtend zu verhängen und können bis zu 4 % des weltweiten Umsatzes betragen (lt. Art. 83 DSGVO: Allgemeine Bedingungen für die Verhängung von Geldbußen). In den Datenschutz zu investieren, lohnt sich somit doppelt: Prozesse werden geklärt und Risiken, die durch Bußgelder bei Datenschutzverstößen drohen, werden deutlich verringert.

Was sind Beschäftigtendaten?

Beispiele für Beschäftigtendaten

Direkter Bezug zu Beschäftigten: Vorname und Nachname, ein biometrisches Merkmal (Foto, Fingerabdruck, etc.), Sozialversicherungsnummer, Steueridentifikationsnummer, Personalnummer, Telefonnummer, E-Mailadresse, KFZ-Kennzeichen, Kontonummer.

Indirekter Bezug zu Beschäftigten: IP-Adressen, Online-Kennungen, Standortdaten, Protokolldaten in IT-Systemen (z. B. Verlauf der Internetnutzung, Sende- und Empfangsprotokolle von Kommunikationssystemen).

Besondere Kategorien personenbezogener Daten

Besonders hohe Anforderungen an die Umsetzung des Datenschutzes stellt die Verarbeitung der „besonderen Kategorien personenbezogener Daten“. Hierbei handelt es sich um Daten, die aus der Perspektive der Betroffenen einem besonderen Schutzbedarf unterliegen. Beispiele sind politische Meinungen oder weltanschauliche Überzeugungen.

Im betrieblichen Kontext sind dies z. B. Gesundheitsdaten, Gewerkschaftszugehörigkeit und Kirchenzugehörigkeit. Zu den Gesundheitsdaten zählen Arbeitsunfähigkeitsbescheinigungen genauso wie Informationen aus einem Verfahren zum betrieblichen Eingliederungsmanagement.

2. Partnerschaftliche Umsetzung des Datenschutzes

Der Datenschutz ist eine gesamtbetriebliche Aufgabe und kann am einfachsten im Einvernehmen zwischen den eingebundenen Personen umgesetzt werden. Dabei ist der Unternehmer oder die Unternehmerin für den Datenschutz gegenüber den Aufsichtsbehörden verantwortlich. Die Beschäftigten sollen durch den Datenschutz in ihren Persönlichkeitsrechten geschützt werden. Gleichzeitig besitzen aber auch die Beschäftigten eine Verantwortung für die Beschäftigtendaten, die sie selbst verarbeiten. Nicht zuletzt spielen die Interessenvertretungen eine wichtige Rolle. Zum einen haben sie per Mitbestimmungsrecht die Pflicht, die Einhaltung der für die Beschäftigten geltenden Gesetze zu überwachen. Zum anderen können die Interessenvertretungen durch den Abschluss von Betriebs- oder Dienstvereinbarungen eine rechtliche Grundlage für die Verarbeitung von Beschäftigtendaten schaffen, sofern dies sinnvoll ist.

Zu den einzubindenden Personen zählen zuerst die Partnerinnen und Partner, die im rechtlichen Rahmen vorgesehen sind.

- Betriebliche Datenschutzbeauftrage mit ihren Beratungs- und Überwachungsaufgaben und
- Interessenvertretungen mit ihren Prüfpflichten und ggf. als Vertragspartnerinnen und -partner über (Kollektiv-) Vereinbarungen zum Datenschutz.
- Gibt es keine Interessenvertretung im Betrieb, können die einzelnen Beschäftigten im Rahmen einer freiwilligen Zustimmung zur Verarbeitung Ihrer Daten eingebunden werden.
- Darüber hinaus können alle betroffenen Beschäftigtengruppen zur datenschutzkonformen Verarbeitung beitragen.

Damit die Umsetzung des Datenschutzes gut funktioniert, sind alle Beteiligten eingeladen zusammenzuarbeiten. Neben den durchaus möglichen Interessenkonflikten gibt es auch eine Reihe gemeinsamer Interessen. Auf diesen lässt sich eine vertrauensvolle Zusammenarbeit aufbauen, welche in den Mitbestimmungsgesetzen eingefordert wird. Dieses Vertrauen muss sich häufig erst entwickeln und kann aktiv gefördert werden. Ein Schlüssel hierzu ist das gegenseitige Verständnis für die unterschiedlichen Interessen.

Vor dem gegenseitigen Verständnis steht das gegenseitige Verstehen. Unternehmen, Beschäftigte und Interessenvertretungen sprechen manchmal unterschiedliche „Sprachen", die übersetzt werden müssen. Die folgenden Beispiele gelten sicher nicht für alle Unternehmen, aber die Praxis hat gezeigt, dass es sich lohnt, sich über die verwendeten Begriffe auszutauschen (s. Tabelle 1: Auflösung möglicher Interessenkonflikte). Vielfach wird durch das Erreichen einer gemeinsamen Sprache die Zusammenarbeit deutlich erleichtert und verbessert.

In vielen Unternehmen ist beispielsweise die Effizienzsteigerung, die Verbesserung der Transparenz und eine höhere Flexibilität von hoher Bedeutung. Beschäftigte und Interessenvertretungen haben allerdings oft die Befürchtung, dass damit Arbeitsverdichtung, Überwachung und Kontrolle sowie eine ständige Verfügbarkeit verbunden sein können.

Eine Abstimmung über die Bedeutung der verschiedenen Begriffe ergibt in der Regel viele gemeinsame Positionen. Effizienz im Rahmen von Digitalisierung schafft genauso unternehmerische Kostenvorteile, wie möglicherweise auch Arbeitserleichterungen durch Technikeinsatz. Ein gemeinsames Interesse ist sicher eine positive Entwicklung des Unternehmens am Markt. So kann Vertrauen dadurch hergestellt werden, dass auch die Sicherheit der Arbeitsplätze nicht in Frage gestellt wird.

Der Beschäftigtendatenschutz und die Forderung nach Transparenz müssen ebenfalls kein Widerspruch sein. Transparenz von Prozessen und Verantwortlichkeiten sind für die Zusammenarbeit wertvoll. Eine Überwachung jeglichen Handelns der Beschäftigten hingegen schafft sicher kein Vertrauen unter den beteiligten Personen und ist daher auch nicht im Interesse des Unternehmens.

Begriff	Arbeitgeber	Interessenvertretung und Beschäftigte	Gemeinsames Interesse
Höhere Flexibilität	Durch die höhere Flexibilität des neuen Systems kann dynamischer auf veränderte Situationen und Anforderungen am Markt reagiert werden.	Birgt die erhöhte Flexibilität Risiken für eine Überschreitung der gesetzlich zulässigen Arbeitszeit sowie für die Balance von Arbeit und Privatleben?	Flexible persönliche Arbeits- und Lebensgestaltung und bedarfsorientierte Personalplanung.
Verbesserte Transparenz	Das zukünftige System sorgt für Transparenz und lässt uns unsere Prozesse besser nachvollziehen und optimieren.	Ergibt sich aus der erhöhten Transparenz mehr Überwachung und Kontrolle von Leistung und Verhalten der Beschäftigten?	Optimale Zusammenarbeit durch guten Informationsaustausch, auch bei mobiler Arbeit.
Erhöhte Effizienz	Durch das neue System können Durchlauf- und Bearbeitungszeiten verringert werden.	Kommt eine Arbeitsverdichtung auf die Beschäftigten zu?	Durch neue Technologien werden Arbeitserleichterungen und eine bessere Marktpositionierung des Unternehmens erreicht.

Tabelle 1: Auflösung möglicher Interessenkonflikte

In dieser Broschüre werden an weiteren Stellen mögliche unterschiedliche Positionen der verschiedenen Beteiligten aufgegriffen und erläutert. Diese Differenzen in Einschätzungen und Bewertungen können nur gemeinsam aufgelöst werden. Wenn hier von „gemeinsam“ die Rede ist, sind neben der Unternehmerin bzw. dem Unternehmer, den Beschäftigten, den Interessenvertretungen und dem betrieblichen Datenschutz auch Personen zu berücksichtigten, die im Unternehmen zum Beispiel Aufgaben auf den Gebieten IT, Technik, Projektmanagement etc. übernehmen (s. Abbildung 2: Funktionen und Akteurinnen und Akteure im Beschäftigtendatenschutz). In kleinen Unternehmen werden häufig mehrere Funktionen wie Projektleitung, IT-Leitung und Geschäftsleitung von nur einer Person wahrgenommen. Unabhängig von der Größe des Unternehmens lohnt es sich, alle Beteiligten frühzeitig an einen Tisch zu holen, alle Perspektiven anzuhören und offen zu diskutieren. Dann stehen die Chancen sehr gut, eine nachhaltige und von allen mitgetragene Lösung zu finden.

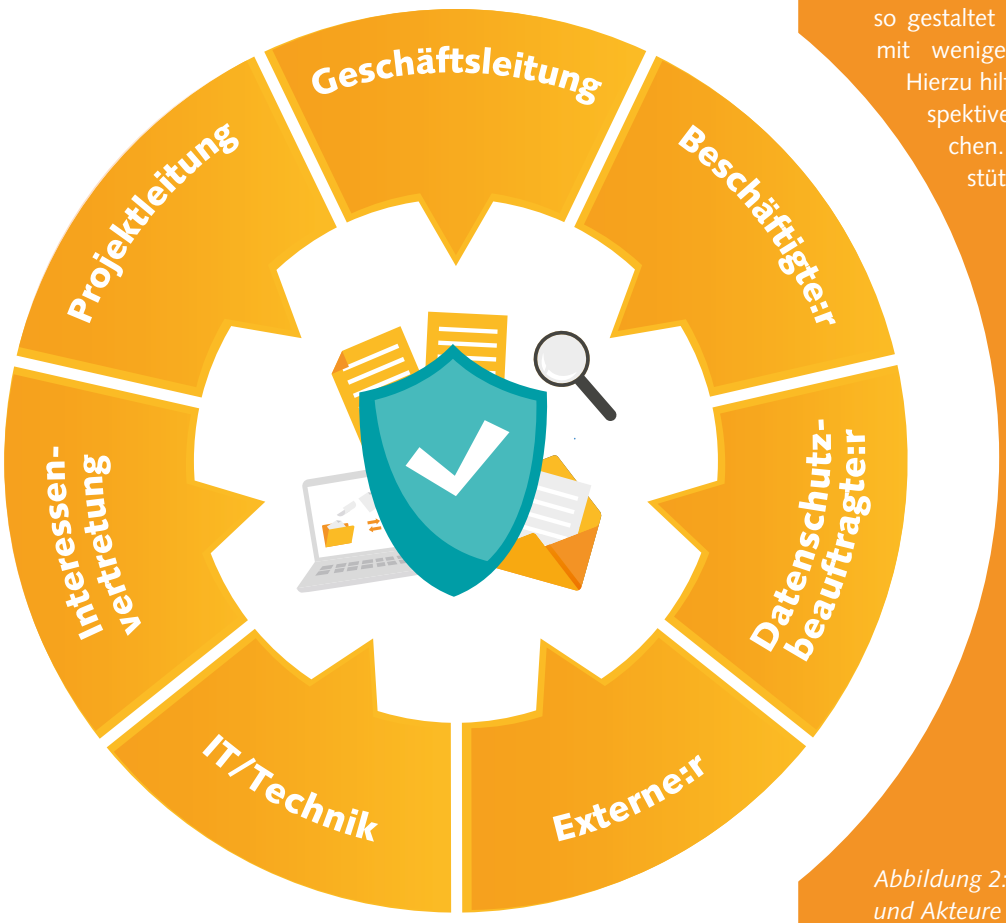


Abbildung 2: Funktionen und Akteurinnen und Akteure im Beschäftigtendatenschutz

Beschäftigtendatenschutz ist von Anfang an mitzudenken. Schon zu Beginn der Gestaltung eines IT-Systems kann ein sehr weitreichender Einfluss auf die Datenschutzanforderungen (s. 4.1 Privacy by Design) genommen werden. Vor dem Start eines Digitalisierungsprojektes stellt sich die Frage, welche IT-Lösungen bzw. -Verfahren eingeführt und zu welchen Zwecken diese genutzt werden sollen. Die Entscheidung darüber hat erheblichen Einfluss darauf, welche Kategorien von Beschäftigtendaten in welchem Umfang verarbeitet werden. Wurden die gewünschten IT-Lösungen sowie die damit verbundenen Zwecke betrachtet, lässt sich auch die Relevanz der Datenverarbeitungen für den Datenschutz bestimmen. Damit kann der Aufwand für Datenschutzmaßnahmen bereits abgeleitet werden. Dieser Aufwand (Abbildung 3: Datenschutzrelevanz von Beschäftigtendaten) lässt sich bei der Systemgestaltung beeinflussen bzw. reduzieren. Dies geschieht dadurch, dass z. B. die Verarbeitung von Beschäftigtendaten auf den erforderlichen Teil eingeschränkt werden. Die Frage lautet daher: Wie kann eine Datenverarbeitung bzw. ein IT-System so gestaltet werden, dass der Datenschutz mit wenigen Regelungen erfüllbar ist? Hierzu hilft es, die unterschiedlichen Perspektiven im Unternehmen abzugleichen. Die folgenden Kriterien unterstützen dabei:

1. Sind eindeutige und konkrete Zwecke der Verarbeitung von Beschäftigtendaten festgelegt? Lassen sich mit wenig Aufwand Datenempfängerinnen und -empfänger, Datenweitergaben und Auswertungen definieren? In diesem Fall ist die erforderliche Dokumentation unaufwändig.
2. Bei der Verarbeitung anonymer Daten, wenn also kein Bezug zwischen Daten und einzelnen Beschäftigten hergestellt werden kann, sind keine Datenschutzmaßnahmen erforderlich.
3. Wenige Datenkategorien erfordern auch weniger Datenschutzmaßnahmen.
4. Eine ständige Erfassung von Beschäftigtenverhalten führt zu einer größeren Einschränkung der Persönlichkeitsrechte und damit zu einem größeren Datenschutzaufwand.
5. Moderne Datenanalyse-Systeme (Business Intelligence) bieten umfassende Auswertungsmöglichkeiten – teilweise mit Unterstützung von Künstlicher Intelligenz. Sollen für Beschäftigtendaten flexible Auswertungsmöglichkeiten genutzt werden, besteht ein hoher Regelungsbedarf im Hinblick auf den Datenschutz. Werden nur vorab definierte, in Bezug auf Inhalte und Zweck eng umrissene Auswertungen festgelegt, ist der Aufwand zur Sicherstellung des Datenschutzes deutlich geringer.
6. Wenn der Kreis der Datenempfängerinnen und -empfänger auf die erforderlichen Personen eingeschränkt wird, sind weniger Datenschutzmaßnahmen erforderlich, als wenn viele Personen auf viele Beschäftigtendaten zugreifen können.
7. Werden keine Algorithmen im Sinne automatisierter Entscheidungen oder Bewertungen verwendet, entfallen hierzu Risikobewertungen oder Datenschutzfolgeabschätzungen.

Abbildung 3: Datenschutzrelevanz von Beschäftigtendaten

3. Umsetzung der Datenschutzgrundsätze in 6 Schritten

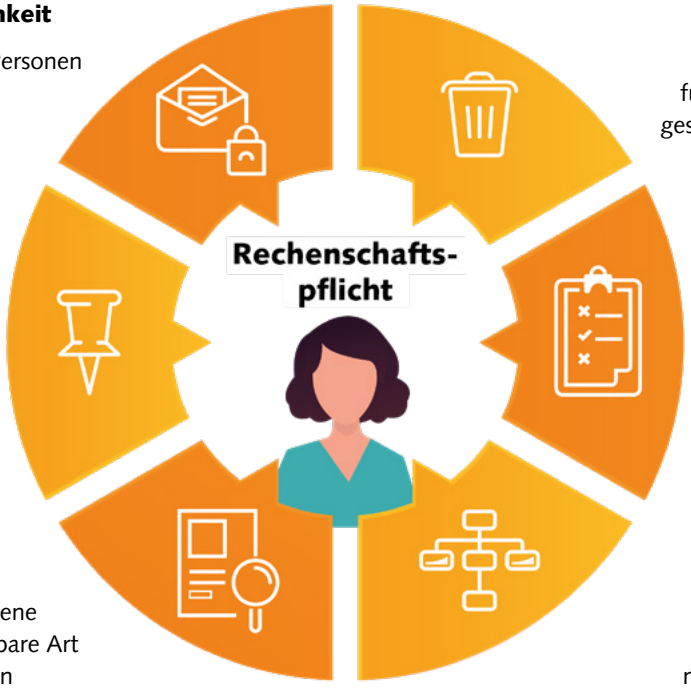
Im Folgenden werden einige Aspekte aus den Datenschutzgrundsätzen (s. Abbildung 4: Grundsätze des Datenschutzes zu Beschäftigtendaten (Art. 5 DSGVO)) aufgegriffen, die eine besondere Bedeutung für den Beschäftigtendatenschutz haben. Von der Richtigkeit der Beschäftigtendaten wird in dieser Broschüre ausgegangen und diese daher nicht weiter betrachtet. Der Datenschutz baut auf sechs Grundsätzen auf (vgl. Art. 5 DSGVO):

Integrität und Vertraulichkeit

Daten dürfen nur befugten Personen zugänglich gemacht werden

Speicherbegrenzung

Daten dürfen nur so lange, wie für die Zweckerreichung nötig ist, gespeichert werden (Löschkonzept)



Zweckbindung

Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden

Richtigkeit

Daten müssen sachlich richtig sein und auf dem neusten Stand sein – andernfalls sind sie zu löschen oder zu korrigieren

Rechtmäßigkeit und Transparenz

Daten müssen für die betroffene Person auf eine nachvollziehbare Art und Weise verarbeitet werden

Datenminimierung

Daten müssen dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein

Abbildung 4: Grundsätze des Datenschutzes zu Beschäftigtendaten (Art. 5 DSGVO)

Auch bei der Gestaltung des Beschäftigtendatenschutzes ist es im betrieblichen Dialog hilfreich, die Grundsätze des Datenschutzes aufzugreifen: Zweckbindung, Integrität und Vertraulichkeit, Rechtmäßigkeit und Transparenz, Speicherbegrenzung, Richtigkeit und Datenminimierung. Ebenso sind als Fundament für die Datenverarbeitung die Rechtsgrundlagen für die Verarbeitung der Beschäftigtendaten sowie der Grundsatz der Datenminimierung zu beachten.

Im Kontext des Beschäftigtendatenschutzes werden jedoch an dieser Stelle nur die Aspekte herausgestellt, die gemeinsam zwischen den beteiligten Akteurinnen und Akteuren zu klären sind. Dies ist die Zweckbindung, die Vertraulichkeit, die Rechtmäßigkeit, die Speicherbegrenzung und Kernelemente der Transparenz und der Rechenschaftspflicht. Zusätzlich wird auf den Kern der Grundsätze – die verarbeiteten Beschäftigtendaten – eingegangen.

Auch wenn die Datenschutzvorgaben im Wesentlichen Schutzgesetze sind und Einschränkungen und Verbote beinhalten, gilt es, die Chancen und die Risiken für die Beschäftigten und das Unternehmen abzuschätzen. Es ist nicht verboten, Beschäftigtendaten zu verarbeiten. Es ist aber nicht zulässig, die Daten beliebig und ohne einen Grund bzw. einen Zweck zu erfassen und zu nutzen. Die Grenze kann im Unternehmen zwischen den Akteurinnen und Akteuren festgelegt werden, sofern das gesetzliche Datenschutzniveau nicht unterschritten wird. Dabei sind Positionen wie der Wunsch, alle Datenvorgänge im Unternehmen zu digitalisieren und zu erfassen, im Regelfall ebenso wenig hilfreich wie die Position, dass überhaupt keine Daten verarbeitet werden. Das sollte bei den folgenden Hilfestellungen zur Umsetzung der Datenschutzgrundsätze berücksichtigt werden.

Die Bearbeitung der folgenden sechs Schritte bildet die Grundlage für die Umsetzung der Anforderungen des Beschäftigtendatenschutzes. Die Verantwortung für die Umsetzung liegt bei der gesetzlichen Vertretung des Unternehmens. Der oder die Datenschutzbeauftragte informiert und unterstützt durch die eigene Sachkunde. Da in der Regel Belange der Beschäftigten betroffen sind, ist eine frühzeitige Information und Einbindung von Beschäftigten und der gesetzlichen Interessenvertretung sinnvoll. Zusätzlich zu den Fragen des Beschäf-

tigtendatenschutzes können auch Mitbestimmungsrechte der Interessenvertretungen berührt sein und so einen Mitbestimmungsprozess auslösen. Dies gilt insbesondere für den Fall, dass eine Betriebs- oder Dienstvereinbarung die Rechtsgrundlage gem. Art. 88 DSGVO bzw. § 26 BDSG (s. 3.5.2 Kollektivvereinbarungen als Rechtsgrundlage nach Art. 88 DSGVO) bilden soll.

Falls es nicht nur um eine juristische Umsetzung des Datenschutzes geht, sondern auch alle Chancen der Digitalisierung nutzbar gemacht werden sollen, kann es sinnvoll und zweckmäßig sein, wenn die betrieblichen Akteurinnen und Akteure gemeinsam an der Umsetzung des Datenschutzes arbeiten. Hierzu müssen sie eine dem Vorhaben angepasste Organisationsform finden. Dies kann ein etablierter Steuerkreis sein, der in vielen Unternehmen bereits vorzufinden ist. Dieser würde das Thema Beschäftigtendatenschutz bearbeiten. Der Steuerkreis Datenschutz wäre also eine Gruppe von relevanten interessierten Personen, die sich regelmäßig treffen und im Digitalisierungsvorhaben die Datenschutzmaßnahmen abstimmen.

Der Datenschutz kann auch als Teilprojekt im Digitalisierungsvorhaben definiert werden. Hier wären die relevanten Akteurinnen und Akteure Projektbeschäftigte, sie entwickeln direkt die Datenschutzmaßnahmen.

Eine wichtige Rolle spielen die Beschäftigten, die das Projekt von Beginn an als betriebliche Experten und Expertinnen begleiten und darin verschiedene Aufgaben haben. Hierzu zählen die Gestaltung von Prozessen, die Schulung oder die Unterstützung von Kolleginnen und Kollegen im späteren Betrieb des Systems. Sie werden häufig als Key-User bezeichnet. Mit ihren Kenntnissen können sie, bei entsprechender Qualifizierung zum Datenschutz, eine wertvolle Unterstützung sein. So können sie z. B. aufgrund ihrer Funktion und Aufgaben Einfluss auf die Systemgestaltung nehmen. Siehe hierzu auch das Kapitel 4.1: Privacy by design.

Die 6 Schritte zur Umsetzung des Beschäftigtendatenschutzes zeichnen sich wie folgt aus:

1. **Festlegung von Zwecken,**
2. **Erfassung und Festlegung der zu verarbeitenden Kategorien von Beschäftigtendaten,**
3. **Festlegung der Datenempfängerinnen und -empfänger,**
4. **Klärung und Schaffung von Rechtsgrundlagen,**
5. **Festlegung der Aufbewahrungs- und Löschfristen,**
6. **Umsetzung der begleitenden Dokumentation.**

Die Schritte 1 bis 5 werden bei diesem Verfahren nacheinander abgearbeitet und in Schritt 6 dokumentiert. Ein wesentlicher Vorteil dieser Methodik besteht darin, dass sich die erarbeiteten Ergebnisse direkt nutzen lassen, um das gesetzlich erforderliche Verzeichnis der Verfahrenstätigkeiten zu erstellen.

„Die drei ersten Schritte“

Die ersten drei Schritte (s. Abbildung 5: Datenschutzdreieck) bilden den Kern der Datenschutzumsetzung. Daher fassen wir diese hier noch einmal zusammen.

1. **Festlegung von Zwecken**
   Was sind die konkreten Zwecke der Verarbeitung von Beschäftigtendaten?
2. **Erfassung und Festlegung der zu verarbeitenden Kategorien von Beschäftigtendaten**
   Welche konkreten Datenkategorien werden verarbeitet?
3. **Festlegung der Datenempfängerinnen und -empfänger**
   Welche Personengruppen erhalten Zugriff auf die Daten?

Die drei Schritte lassen sich in einer Frage zusammenfassen:

Welche Beschäftigtendaten werden zu welchen Zwecken durch wen verarbeitet? Weitere Antworten zur datenschutzkonformen Umsetzung des IT-Systems lassen sich danach leicht ableiten:

- Wie lange sind die Beschäftigtendaten aufzubewahren?
- Welche Auswertungen sind für die Zweckerfüllung erforderlich?
- Welche Risiken bestehen für die Persönlichkeitsrechte der Beschäftigten?
- Welche technischen und organisatorischen Maßnahmen sind zum Schutz der Daten zu ergreifen?

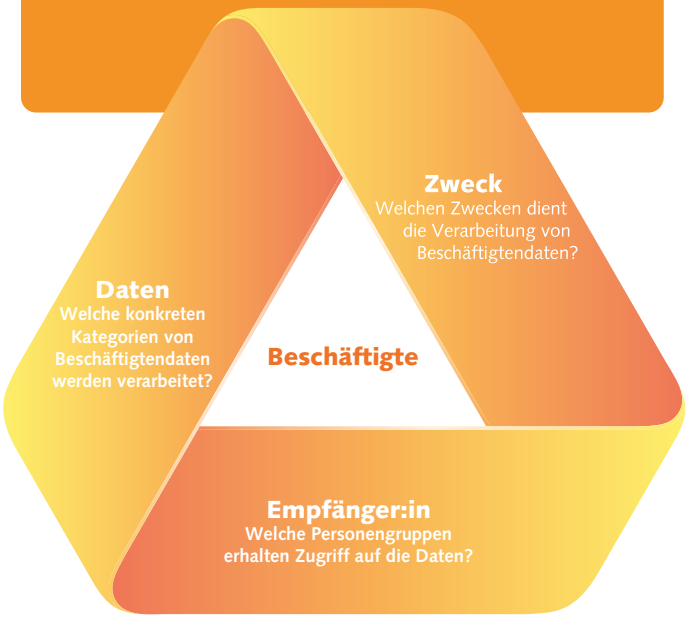


Abbildung 5: Datenschutzdreieck

Schritt 1:
Festlegung von Zwecken

Die Festlegung von Zwecken kann auch so formuliert werden:
Wozu benötige ich die Daten der Beschäftigten?

Die Antwort sollte nicht einseitig gegeben, sondern mit allen betrieblichen Akteurinnen und Akteuren abgestimmt werden. So lassen sich mögliche Missverständnisse frühzeitig klären. Auch hier ist eine praktische Zweckbestimmung anzuraten. Werden die Zwecke zu allgemein gehalten, dann lassen sich keine Maßnahmen daraus ableiten. Zu kleinteilige Definitionen sind praktisch nicht umsetzbar. Die Zwecke sollten aber so gestaltet sein, dass sich daraus z. B. die Löschfristen oder die Empfängerinnen und Empfänger zuordnen lassen (s. Tabelle 2: Festlegung von Zwecken (Schritt 1)). Dies ist ein entscheidender Schritt bei der Abstimmung zwischen den betrieblichen Akteurinnen und Akteuren. Eine spätere Korrektur oder Anpassung der Zweckbestimmungen ist immer möglich.

Beispiel:

Ein elektronisches Schließsystem soll das alte Schlüsselsystem ablösen. Der Zweck des elektronischen Schließsystems soll die Beschränkung von Zutritten im Gebäude sein. Dies ist für die Beschäftigten und auch für die Interessenvertretungen ein nachvollziehbares und transparentes Digitalisierungsvorhaben.

Ein möglicher Interessenkonflikt entsteht, wenn die Benutzung des digitalen Schlüssels protokolliert und ausgewertet wird. In diesem Fall werden Daten von den Beschäftigten verarbeitet, die es vorher nicht gab. Damit wird auch der Zweck des Schließsystems ausgeweitet. Dem ursprünglichen Zweck der Zutrittsberechtigung wird nun die Kontrolle der Zutritte hinzugefügt – eine Kontrolle des Verhaltens der Beschäftigten. Eine Klärung zwischen den Beteiligten ist erforderlich, um den tatsächlichen Zweck und damit auch die Nutzung des Systems festzulegen.

Die Zwecke werden in der im Schritt 6 skizzierten, begleitenden Dokumentation eingetragen. Wie sich den jeweiligen Funktionen bzw. Verfahren Zwecke zuordnen lassen, zeigt beispielhaft die folgende Tabelle.

Anwendung bzw. Verfahren	Zweck der Verarbeitung
Videokonferenz-systeme	Übersichten mit ein- und abgegangenen Anrufen Audio- und videogestützte Kommunikation für Gesprächspartnerinnen, Geschäftspartner und Gruppen Bereitstellung von weiteren Kommunikations- und Zusammenarbeitswerkzeugen wie Kurznachrichten oder wechselseitige Bildschirmfreigabe Informationen für Nutzerinnen und Nutzer zur Anrufhistorie, Kontaktverwaltung und Kalenderintegration
Reisekosten-App	Reisekostenabrechnung
Elektronisches Schließsystem	Zutrittsgewährung
Qualifikations-Management	Organisation von Weiterbildung und Aufgabenzuordnung

Tabelle 2: Festlegung von Zwecken (Schritt 1)

Schritt 2:
Festlegung der Beschäftigtendaten

Der zweite Schritt besteht in der Erfassung und Festlegung der zu verarbeitenden Kategorien von Beschäftigtendaten (s. Tabelle 3: Erfassung und Festlegung der zu verarbeitenden Kategorien von Beschäftigtendaten (Schritt 2)). Die Festlegung der Beschäftigtendaten kann auch so formuliert werden:
Welche Daten der Beschäftigten benötige ich für die genannten Zwecke?

Dabei werden nicht einzelne Datenfelder betrachtet. Vielmehr sollten die Daten in Kategorien zusammengefasst werden. Beispiele hierfür sind Kontaktdaten, Reisedaten, Inhaltsdaten von Sprach- und Schriftkommunikation oder Systemprotokolle mit Benutzerdaten in IT-Systemen.

Die in Schritt 2 festgelegten Kategorien von Beschäftigtendaten werden ebenfalls in der im Schritt 6 aufgeführten Dokumentation hinterlegt. Wie sich den jeweiligen Funktionen bzw. Verfahren Kategorien von Beschäftigtendaten zuordnen lassen, zeigt die untenstehende Tabelle.

Anwendung bzw. Verfahren	Zweck der Verarbeitung	Kategorie von Beschäftigtendaten
Videokonferenz-systeme	Übersichten mit ein- und abgegangenen Anrufen Audio- und videogestützte Kommunikation für Gesprächspartnerinnen, Geschäftspartner und Gruppen Bereitstellung von weiteren Kommunikations- und Zusammenarbeitswerkzeugen, wie Kurznachrichten, wechselseitige Bildschirmfreigabe Informationen für Nutzerinnen und Nutzer zur Anrufhistorie, Kontaktverwaltung und Kalenderintegration	Verbindungsdaten Kontaktdaten Nachrichten und Dateien aus Chat-Verläufen Aufzeichnungen von Bildschirmfreigaben, Gesprächs- und Bilddaten
Reisekosten-App	Reisekostenabrechnung	Reisezeiten Reisekostenbelege Zahlungsinformationen Kontaktdaten
Elektronisches Schließsystem	Zutrittsgewährung	Zutrittsberechtigungen
Qualifikations-Management	Organisation von Weiterbildung und Aufgabenzuordnung	Kompetenzen Zertifikate Zeugnisse Weiterbildungen

Tabelle 3: Erfassung und Festlegung der zu verarbeitenden Kategorien von Beschäftigtendaten (Schritt 2)

In welchen IT-Systemen werden Beschäftigtendaten verarbeitet?

In Unternehmen werden in nahezu allen IT-Lösungen Beschäftigtendaten verarbeitet. Ein klassischer Anwendungsfall ist die Verarbeitung von Beschäftigtendaten in Personalsystemen. Hier wird eine Vielzahl an Personaldaten zum Zweck der Personalverwaltung verarbeitet. Diese reichen von Daten für Lohnabrechnungen bis hin zu Arbeitsunfähigkeitsbescheinigungen oder auch Zeitdaten, wie z. B. Urlaubs- oder Weiterbildungstage. In größeren Unternehmen findet die Verarbeitung solcher Daten in den Personalabteilungen statt. Diese Datenverarbeitungen werden aber oftmals auch von externen Dienstleistern erbracht.

IT-Systeme zur Steuerung des Unternehmens, oft als Customer-Relationship-Management-System (CRM) oder Enterprise-Ressource-Management-System (ERP) bezeichnet, verarbeiten ebenfalls umfassend Beschäftigtendaten. So entstehen z. B. Daten im Arbeitsprozess als Leistungs- bzw. Ergebnisdaten. Hierbei handelt es sich um messbare Daten, z. B. über produzierte Stückzahlen, erbrachte Umsätze oder für die Kundin oder den Kunden erbrachte Arbeitszeiten. Diese Daten werden zu Zwecken der Abrechnung von Leistungen mit der Kundin und dem Kunden, zur Nachkalkulation eines Auftrages oder auch zur Kapazitätsplanung für zukünftige Aufträge verarbeitet.

Die umfangreichsten Daten sind die Systemdaten, die sich auf der technischen Ebene befinden. Also Systemprotokolle, in denen festgehalten wird, wer sich wann in welchem System angemeldet hat, wer wann welche Daten geändert hat, wer mit wem kommuniziert hat oder wann im Internet auf welchen Websites unterwegs gewesen ist. Ein wesentlicher Zweck ist die Aufrechterhaltung des Betriebes der IT-Systeme durch die technischen Administratoren.

Die Infobox zeigt, welche IT-Systeme mit Beschäftigtendaten vielfach eingesetzt werden.

Beispiele für IT-Systeme mit Beschäftigtendaten

Einführung und Nutzung von

- Auftragsverwaltungssystemen, Warenwirtschaftssystemen, CRM-Systemen (Customer Relationship Management),
- Office-, Kommunikations- und Kollaborationslösungen,
- Videokonferenzsystemen,
- Personalmanagementsoftware (z. B. Zeiterfassungssoftware, Personalentwicklungssysteme),
- Sicherheitssoftware (Compliance- oder Security-Systeme, z. B. Firewall, Security Information and Eventmanagement (SIEM)).

Schritt 3:
Festlegung der Daten-empfängerinnen und -empfänger

Im dritten Schritt geht es darum, die Kategorien der Datenempfängerinnen und -empfänger festzulegen. Die Festlegung kann auch so formuliert werden:
Welche Personen erhalten Zugriff auf die Beschäftigtendaten?

Nachdem die Zwecke der Datenverarbeitungen und die hierzu erforderlichen Datenkategorien feststehen, sind die Kategorien der Datenempfängerinnen und -empfänger zu bestimmen (s. Tabelle 4: Festlegung der Datenempfängerinnen und -empfänger (Schritt 3)). Es gilt das Prinzip der Vertraulichkeit. Deshalb sollen nur Personen benannt werden, die die Beschäftigtendaten zur Erfüllung ihrer Aufgaben und Funktionen im Unternehmen benötigen. In der Praxis besitzen diese Personen in den IT-Systemen entsprechende Berechtigungen, um die erforderlichen Daten zu sehen, zu bearbeiten oder auch zu löschen. Diese Berechtigungen werden den einzelnen Personen nicht individuell, sondern über eine technische Rolle erteilt. Vereinfacht gesagt beinhaltet beispielsweise die technische Rolle „Lohnbuchhaltung" die Berechtigungen, die eine Person für die Lohnabrechnung benötigt. Den Personen in der Lohnbuchhaltung wird diese Rolle zugewiesen. Damit entspricht eine solche Rolle auch der genannten Kategorie der Empfängerdaten.

Wie sich Datenempfängerinnen und -empfänger / Zugriffsberechtigte hinterlegen lassen, zeigt die Tabelle unten.

Anwendung bzw. Verfahren	Zweck der Verarbeitung	Kategorie von Beschäftigtendaten	Datenempfänger/-in Zugriffsberechtigte
Videokonferenz-systeme	Übersichten mit ein- und abgegangenen Anrufen Audio- und videogestützte Kommunikation für Gesprächspartnerinnen, Geschäftspartner und Gruppen Bereitstellung von weiteren Kommunikations- und Zusammenarbeitswerkzeugen wie Kurznachrichten, wechselseitige Bildschirmfreigabe Informationen für Nutzerinnen und Nutzer zur Anrufhistorie, Kontaktverwaltung und Kalenderintegration	Verbindungsdaten Kontaktdaten Nachrichten und Dateien aus Chat-Verläufen Aufzeichnungen von Bildschirmfreigaben, Gesprächs- und Bilddaten	Teilnehmerinnen und Teilnehmer sowie Adressaten der Videokonferenz
Reisekosten-App	Reisekostenabrechnung	Reisezeiten Reisekostenbelege Zahlungsinformationen Kontaktdaten	Reisekostenstelle Vorgesetzte
Elektronisches Schließsystem	Zutrittsgewährung	Zutrittsberechtigungen	Schlüsselausgabe Facilitymanager Hausmanagement
Qualifikations-Management	Organisation von Weiterbildung und Aufgabenzuordnung	Kompetenzen Zertifikate Zeugnisse Weiterbildungen	Personalentwicklung Vorgesetzte

Tabelle 4: Festlegung der Datenempfängerinnen und -empfänger (Schritt 3)

Schritt 4:
Klärung und Schaffung von Rechtsgrundlagen

Im vierten Schritt erfolgt die Klärung der jeweiligen Rechtsgrundlage. Die Frage nach der Rechtsgrundlage kann auch so formuliert werden:
Auf welcher rechtlichen Grundlage sollen die Beschäftigtendaten verarbeitet werden?

Für jede Verarbeitung von personenbezogenen Daten, egal ob Beschäftigtendaten, Kundendaten etc., ist eine rechtliche Grundlage erforderlich. Die Gesetze zum Datenschutz setzen auf das Prinzip eines „Verbots mit Erlaubnisvorbehalt". Die Verarbeitung der personenbezogenen Daten muss also gesetzlich erlaubt sein. Ist dies nicht eindeutig der Fall und die Rechtsgrundlage damit unklar, ist die Datenverarbeitung nicht zulässig. Rechtsgrundlagen für die Verarbeitung von Beschäftigtendaten im Betrieb sind Gesetze, Verordnungen, Tarifverträge, Kollektivvereinbarungen (Betriebs- und Dienstvereinbarungen) oder Einwilligungen der betroffenen Personen.

Besonders ist der § 26 BDSG „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses" hervorzuheben. Diese Vorschrift ist die zentrale Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten im Unternehmen. Sie erlaubt eine Verarbeitung von Beschäftigtendaten, wenn sie zur Begründung, Durchführung und Beendigung eines Beschäftigungsverhältnisses erforderlich sind. Eindeutige Beispiele dafür sind Daten der Entgeltabrechnung, Arbeitszeiten, Weiterbildung der Beschäftigten oder Gesundheitsdaten. Auch Daten, die die Erfüllung der arbeitsvertraglichen Pflichten dokumentieren, sind zulässig. Dies geschieht häufig im Interesse aller Beteiligten. So belegt die Erfassung der Arbeitszeiten gegenüber dem Unternehmen die Erfüllung der arbeitsvertraglichen Pflichten hinsichtlich der vereinbarten Arbeitszeit. Mit Blick auf § 26 BDSG kann von einer grundsätzlichen Zulässigkeit der Verarbeitung der genannten Daten ausgegangen werden. Gleichwohl ist es empfehlenswert, den konkreten Umfang der verarbeiteten Daten zu prüfen. Der Umfang der verarbeiteten Daten sollte auf das erforderliche Maß begrenzt sein. Beginn und Ende der Arbeit, die Pausenzeiten sowie Abwesenheitszeiten ermöglichen bereits die vollständige Erfassung der Arbeitszeit. Die Erfassung weitergehender Daten erfordert insofern zusätzliche Ziele und Zwecke der Datenverarbeitung. Hierbei sind die Interessen der Beschäftigten mit den Interessen des Unternehmens nach dem Prinzip der Verhältnismäßigkeit abzuwägen. Diese Abwägung ist, sofern die verschiedenen betrieblichen Akteurinnen und Akteure beteiligt waren, bei der Umsetzung der Schritte 1 bis 3 bereits erfolgt. Falls dann Unsicherheit darüber herrscht, ob damit schon § 26 als Rechtsgrundlage genügt, kann mit Abschluss einer Kollektivvereinbarung Rechtssicherheit hergestellt werden. Ebenso ist eine Verarbeitung von Beschäftigtendaten zulässig, wenn die einzelnen Beschäftigten dieser zugestimmt haben.

Vertreter der Interessenvertretungen erhalten im Rahmen ihrer Aufgaben Einblick in Beschäftigtendaten und verarbeiten diese. Dabei unterliegt die Datenverarbeitung durch die Interessenvertretung ebenfalls den Anforderungen des Datenschutzes. Beschäftigtendaten dürfen durch die Interessenvertretung nur eingesehen und verarbeitet werden, wenn dies für die Wahrnehmung der Informations- und Mitbestimmungsrechte nach dem BetrVG erforderlich ist. Hierbei kann es sich beispielsweise um die Mitbestimmung bei personellen Einzelmaßnahmen, die Überprüfung der für die Beschäftigten geltenden Gesetze, Verordnungen, Tarife und Kollektivvereinbarungen handeln.

Wenn die relevanten Rechtsgrundlagen geklärt bzw. geschaffen wurden, können sie in der Tabelle 5, wie unten dargestellt, hinterlegt werden.

Anwendung bzw. Verfahren	Zweck der Verarbeitung	Kategorie von Beschäftigtendaten
Videokonferenzsysteme	Übersichten mit ein- und abgegangenen Anrufen Audio- und videogestützte Kommunikation für Gesprächspartnerinnen, Gesprächspartner und Gruppen Bereitstellung von weiteren Kommunikations- und Zusammenarbeitswerkzeugen wie Kurznachrichten, wechselseitige Bildschirmfreigabe Informationen für Nutzerinnen und Nutzer zur Anrufhistorie, Kontaktverwaltung und Kalenderintegration	Verbindungsdaten Kontaktdaten Nachrichten und Dateien aus Chat-Verläufen Aufzeichnungen von Bildschirmfreigaben, Gesprächs- und Bilddaten
Reisekosten-App	Reisekostenabrechnung	Reisezeiten Reisekostenbelege Zahlungsinformationen Kontaktdaten
Elektronisches Schließsystem	Zutrittsgewährung	Zutrittsberechtigungen
Qualifikations-Management	Organisation von Weiterbildung und Aufgabenzuordnung	Kompetenzen Zertifikate Zeugnisse Weiterbildungen

Einwilligung als Rechtsgrundlage nach § 26 BDSG und Art. 7 DSGVO

Falls weder das BDSG noch sonstige Gesetze oder Verordnungen die Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten bilden und auch keine Kollektivvereinbarung existiert, kommt als Rechtsgrundlage für die Datenverarbeitung nur die individuelle Einwilligung der Betroffenen in Frage. Es gibt auch gute Gründe, wie im folgenden Beispiel aufgeführt, in Unternehmen mit Interessenvertretungen die Rechtsgrundlage über eine Einwilligung der Beschäftigten zu schaffen.

Ein Beispiel für eine Datenverarbeitung ohne gesetzliche oder tarifliche Rechtsgrundlage ist die Bekanntgabe einer Geburtstagsliste oder eines Urlaubskalenders. Die enthaltenen Namen der Beschäftigten und die Geburtsdaten oder Abwesenheitszeiten stellen personenbezogene Daten dar. Da die betriebsöffentliche Geburtstagsliste oder der betriebsöffentliche Urlaubsplan für die Umsetzung des Beschäftigungsverhältnisses nicht erforderlich ist, stellt § 26 BDSG keinen hinreichenden Erlaubnistatbestand für die Datenverarbeitung dar. Ebenso wenig finden sich hierfür andere gesetzliche Regelungen oder Tarifverträge.

Die Einwilligungen der Beschäftigten, in diese Listen aufgenommen zu werden, ist freiwillig und muss dokumentiert werden. Der Gesetzgeber macht deutlich, dass von Freiwilligkeit in einem abhängigen Beschäftigungsverhältnis ausgegangen werden kann, wenn für den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erzielt wird oder der Arbeitgeber und der Beschäftigte gleichgelagerte Interessen verfolgen. In den genannten Beispielen lassen sich hierfür hinreichende Anhaltspunkte finden.

Allerdings können freiwillige Einwilligungen im Regelfall jederzeit und ohne Begründung zurückgenommen werden. Während dies im Fall einer Geburtstagsliste keine nennenswerten betrieblichen Folgen hat, könnte der Nutzen einer Vielzahl anderer betrieblicher Prozesse hierdurch eingeschränkt werden. Daher empfiehlt es sich – wenn möglich – Kollektivvereinbarungen abzuschließen.

Tabelle 5:
Klärung und Schaffung von Rechtsgrundlagen (Schritt 4)

	Datenempfangende/ Zugriffsberechtigte	Rechtsgrundlage
	Teilnehmerinnen und Teilnehmer sowie Adressaten der Videokonferenz	Kollektiv-vereinbarung
	Reisekostenstelle Vorgesetzte	GoB
	Schlüsselausgabe	§ 26 BDSG
	Personalentwicklung Vorgesetzte	§ 26 BDSG

Kollektivvereinbarungen als Rechtsgrundlage nach Art. 88 DSGVO

Unternehmen mit Interessenvertretungen können mit Hilfe von Kollektivvereinbarungen, etwa Betriebs- oder Dienstvereinbarungen, die Umsetzung des Beschäftigtendatenschutzes sicherstellen. In nicht mitbestimmten Betrieben müssen die Unternehmen ihre Datenverarbeitungsprozesse auf andere Rechtsgrundlagen stützen. Diese können sich aus der DSGVO oder dem BDSG, aber auch aus anderen Gesetzen, aus vertraglichen Regelungen oder aus individuell mit dem Beschäftigten vereinbarten Einwilligungen ergeben. Lassen sich zwischen den Interessenvertretungen und den Unternehmensvertretern gemeinsame Grundsätze zur Verarbeitung von Beschäftigtendaten festlegen, kann dies in einer pragmatischen Vereinbarung festgehalten werden. Allerdings dürfen auch Kollektivvereinbarungen das Schutzniveau der DSGVO und des BDSG nicht unterschreiten. Ebenso sind in einer solchen Vereinbarung die Maßnahmen zur Wahrung des Datenschutzes (Art. 88 Abs. (2) DSGVO) aufzunehmen. Hierbei handelt es sich u. a. um Maßnahmen zum Schutz der Daten, zur Transparenz der Verarbeitung und zur Übermittlung von Beschäftigtendaten innerhalb einer Unternehmensgruppe und der Überwachungssysteme am Arbeitsplatz.

Schritt 5:
Festlegung der Aufbewahrungs- und Löschfristen

Daten mit Beschäftigtenbezug sind nur so lange aufzubewahren, wie sie für die genannten Zwecke erforderlich sind bzw. eine gesetzliche Vorgabe dies vorschreibt. Wie die folgende Tabelle 6 zeigt, werden wichtige Aufbewahrungsfristen unter anderem im Handelsgesetzbuch (HGB), der Abgabenordnung (AO), dem Bürgerlichen Gesetzbuch (BGB), dem Allgemeinen Gleichbehandlungsgesetz (AGG) oder dem Arbeitszeitgesetz (ArbZG) geregelt.

Kategorie von Beschäftigtendaten	Aufbewahrungsfristen	Rechtsgrundlage
Bewerbungsunterlagen	6 Monate	§ 61 b Abs. 1 ArbGG i.V.m. § 15 AGG
Arbeitszeiten	bis 2 Jahre	§ 16 Abs. 2 ArbZG
Handels- oder Geschäftsbriefe	6 Jahre	HGB, AO
Buchungsbelege	10 Jahre	HGB, AO
Reisekosten	6 Jahre	EStG
Fahrtenschreiber	1 Jahr	Straßenverkehrszulassungsordnung (StvZO)
Urlaubsanspruch, der durch den Betrieb nicht stattgegeben werden konnte	3 Jahre	Bürgerliches Gesetzbuch (BGB) § 195 Regelmäßige Verjährungsfrist

Tabelle 6: Beispiele für Aufbewahrungsfristen

Wie eingangs beschrieben, empfiehlt es sich, unterschiedliche Datenkategorien so zu gestalten, dass sich daraus die Löschfristen und die Datenempfängerinnen und -empfänger bezogen auf den Zweck ableiten lassen.

Unsere drei Beispiele sind nun inkl. der Löschfristen in der Tabelle 7 dokumentiert:

Anwendung bzw. Verfahren	Zweck der Verarbeitung	Kategorie von Beschäftigtendaten
Videokonferenzsysteme	Übersichten mit ein- und abgegangenen Anrufen Audio- und videogestützte Kommunikation für Gesprächspartnerinnen, Gesprächspartner und Gruppen Bereitstellung von weiteren Kommunikations- und Zusammenarbeitswerkzeugen wie Kurznachrichten, wechselseitige Bildschirmfreigabe Informationen für Nutzerinnen und Nutzer zur Anruf-historie, Kontaktverwaltung und Kalenderintegration	Verbindungsdaten Kontaktdaten Nachrichten und Dateien aus Chat-Verläufen Aufzeichnungen von Bildschirmfreigaben, Gesprächs- und Bilddaten
Reisekosten-App	Reisekostenabrechnung	Reisezeiten Reisekostenbelege Zahlungsinformationen Kontaktdaten
Elektronisches Schließsystem	Zutrittsgewährung	Zutrittsberechtigungen
Qualifikations-Management	Organisation von Weiterbildung und Aufgabenzuordnung	Kompetenzen Zertifikate Zeugnisse Weiterbildungen

Tabelle 7: Verzeichnis der Verarbeitungstätigkeiten (Schritt 5)

	Datenempfangende/ Zugriffsberechtigte	Rechtsgrundlage	Aufbewahrungsfrist
	Teilnehmerinnen und Teilnehmer sowie Adressaten der Videokonferenz	Kollektivvereinbarung	Keine Aufbewahrung von Audio- und Bilddaten Speicherung von Chatnachrichten und Texten für drei Monate
	Reisekostenstelle Vorgesetzte	GoB	6 Jahre für Zeit- und Kontaktdaten, 10 Jahre für Belege
	Schlüsselausgabe	§ 26 BDSG	Bis zum Ende der Zutrittsberechtigung
	Personalentwicklung Vorgesetzte	§ 26 BDSG	Bis Ende des Beschäftigungsverhältnisses

Schritt 6:
Umsetzung der begleitenden Dokumentation

Wie in den vorherigen Schritten ausgeführt, werden die in den Schritten 1 bis 5 gewonnenen Parameter entweder prozessbegleitend oder zum Schluss in Gänze in der Dokumentationsübersicht hinterlegt. Diese lässt sich wiederum für

- die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten,
- die Information der betroffenen Beschäftigten,
- die Vereinbarungen mit den Interessenvertretungen,
- die Erfüllung der Auskunftspflichten,
- die Schaffung eines Überblicks über die verarbeiteten Daten im Unternehmen

nutzen.

Wurden die genannten Schritte gemeinsam angegangen, sollten mit der Dokumentation nun alle wesentlichen praktischen Aufgaben zur Umsetzung erledigt sein. Die betrieblichen Akteurinnen und Akteure haben dabei sicher einige Diskussionen geführt, die möglicherweise auch ein neues Verständnis für die Sichtweisen und Interessen der Gegenseite erbracht haben. Neben dem Datenschutzthema kann dies auch bei weiteren unternehmerischen Entwicklungen hilfreich sein.

Die Verarbeitung von Beschäftigtendaten wird im Verzeichnis der Verarbeitungstätigkeiten (VVT) nach Art. 30 DSGVO sowie § 70 BDSG dokumentiert. Damit kann man gleichzeitig die Anforderungen der Informationspflicht gemäß Art. 13 DSGVO und das Auskunftsrecht gemäß Art. 15 DSGVO erfüllen. Ebenso bildet das VVT eine zentrale Dokumentation im Rahmen der Rechenschaftspflicht. Viele bezeichnen dieses umgangssprachlich als Verarbeitungsverzeichnis.

Gemäß dem Kurzpapier Nr. 1 „Verzeichnis von Verarbeitungstätigkeiten" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) gilt: „Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7) durch entsprechende Dokumentationen nachgewiesen werden."

Gemäß Art. 30 DSGVO und § 70 BDSG sind Unternehmen zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten verpflichtet. Kleine und mittlere Unternehmen mit bis zu 249 Beschäftigten sind von dieser Verpflichtung ausgenommen. Unabhängig von der Unternehmensgröße ist in den folgenden Fällen (Art. 30 (5) DSGVO) ein Verzeichnis der Verarbeitungstätigkeiten zu führen:

- Die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen,
- die Verarbeitung erfolgt nicht nur gelegentlich oder
- es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO bzw. eine Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO.

In den meisten Unternehmen wird einer der genannten Aspekte zutreffen. Daher sollte mit dem oder der betrieblichen Datenschutzbeauftragten (bDSB) geklärt werden, ob ein Verfahrensverzeichnis zu führen ist.

Der Gesetzgeber spricht von einem einzigen Verfahrensverzeichnis (VVT) für das gesamte Unternehmen. Die einzelnen IT-Systeme bzw. deren Funktionen werden als Verfahren bezeichnet und im VVT getrennt aufgenommen. Im Verfahrensverzeichnis sind die verschiedenen im Unternehmen ablaufenden Datenverarbeitungsprozesse und die hierfür eingesetzten IT-Systeme aufzulisten. Ebenso zu dokumentieren sind der Name und die Kontaktdaten der für den Datenschutz verantwortlichen Personen sowie der oder des betrieblichen Datenschutzbeauftragten.

Anwendung bzw. Verfahren	Zweck der Verarbeitung	Kategorie von Beschäftigtendaten	Datenempfangende/ Zugriffsberechtigte
Fuhrparkmanagement Software	Dokumentation der gesetzlichen Voraussetzungen zur Führung eines KFZ	Führerschein vorhanden	Fuhrparkmanagement
Buchhaltungssoftware	Lohnbuchhaltung	Bankdaten Stundenkonten	Lohnbuchhaltung

Tabelle 8: Beispiel für ein Verzeichnis der Verarbeitungstätigkeiten (VVT) nach § 70 BDSG (Schritt 6)

Bewährt hat sich eine Darstellung, in der die nachfolgenden Informationen in Formblättern oder tabellarisch erfasst werden:

- Die Zwecke werden sinnvollerweise dem Datenverarbeitungsverfahren zugeordnet. Damit ist auch eine Zuordnung zur betrieblichen Praxis erkennbar.
- Kategorien personenbezogener Daten: Sind die Zwecke hinreichend konkret formuliert, lassen sich daraus die erforderlichen Kategorien der Beschäftigtendaten bestimmen.
- Betroffene Personen: Die Nennung der betroffenen Personen kann entfallen, wenn nur von Beschäftigtendaten gesprochen wird. Wenn andere Betroffenengruppen, wie Kundinnen bzw. Kunden oder Lieferanten, dokumentiert werden sollen, so ist eine solche Spalte hinzuzufügen.
- Bei den Kategorien von Empfängerinnen und Empfängern sind keine Namen, sondern Organisationseinheiten zu nennen. So sind zum Beispiel die Empfängerinnen und Empfänger von Reisekostendaten, die Reisekostenstelle und die Vorgesetzten aufzuführen. Auch die Empfängerkategorien lassen sich aufgrund der benannten Zwecke bestimmen.
- Vorgesehene Fristen zur Löschung der Daten sind, sofern möglich, aufgrund gesetzlicher Vorgaben zu nennen. Existieren diese nicht, so sind sie aufgrund der genannten Zwecke ableitbar. Wenn Daten zur Zweckerfüllung nicht mehr benötigt werden, sollten diese zeitnah gelöscht werden.
- Technische und organisatorischen Maßnahmen zum Datenschutz: Zu solchen Maßnahmen zählen z. B. ein Berechtigungsmanagement, Löschkonzepte oder Zugangskontrollen zu IT-Systemen. In der Regel werden sich die technischen und organisatorischen Maßnahmen zum Datenschutz mit denen zur Datensicherheit überschneiden. Wenn diese in einem Datenschutzkonzept oder Datensicherheitskonzept beschrieben sind, ist ein Verweis im Verzeichnis der Verarbeitungstätigkeiten sinnvoll.

Nachfolgend findet sich ein Beispiel für ein Verzeichnis der Verarbeitungstätigkeiten bezogen auf Beschäftigtendaten (s. Tabelle 8: Beispiel für ein Verzeichnis der Verarbeitungstätigkeiten (VVT) nach § 70 BDSG (Schritt 6)). In unserem Beispiel wurde die Einordnung der jeweiligen Vorschrift als Rechtsgrundlage für die Datenverarbeitung in das Verzeichnis mit aufgenommen. Dies ist im BDSG nicht vorgesehen. Der Vorteil ist eine einfachere Ableitung der Aufbewahrungsfristen. Außerdem kann den Beschäftigten die Erforderlichkeit der Verarbeitung Ihrer Daten transparent gemacht werden.

	Rechtsgrundlage	Aufbewahrungsfrist
	§ 21 StVG Straßenverkehrs-gesetz	Bis Ende der dienstlichen KFZ-Nutzung
	§ 26 BDSG	2, 6, 10 Jahre

Der Leitfaden „Das Verarbeitungsverzeichnis – Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-Datenschutz-Grundverordnung (DS-GVO)“ gibt ausführliche Hinweise zur Erstellung eines Verarbeitungsverzeichnisses. Herausgeber: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Download unter: *https://t1p.de/mnaf*

4. Weitere Aspekte zum Beschäftigten-datenschutz

4.1. Privacy by design

Ohne Zweifel stellt der Beschäftigtendatenschutz eine Reihe von Anforderungen. Gute Beispiele aus der Praxis zeigen, dass ein von Beginn an mitgedachter Beschäftigtendatenschutz wichtige Impulse für eine sachgerechte und effiziente Umsetzung betrieblicher Digitalisierungsprojekte liefern kann. Hohe Aufwände für den Datenschutz entstehen meist dann, wenn Anforderungen erst spät in die Projekte einfließen. Wird hingegen das von der DSGVO geforderte Prinzip des „Privacy by design" von Beginn an umgesetzt, lassen sich klare und gut dokumentierte Prozesse schaffen.

„Privacy by design" bedeutet, dass die Anforderungen des Datenschutzes von Anfang an Grundlage für die Konzeption einer Datenverarbeitung und des dazu genutzten IT-Systems sind. Das heißt, der Datenschutz wird bereits bei der Erarbeitung eines Datenverarbeitungsvorgangs im Entwicklungsstadium technisch berücksichtigt. Im Ergebnis entstehen in Bezug auf den Schutzbedarf angemessene technische und organisatorische Maßnahmen zum Datenschutz. Dieser „Datenschutz durch Technikgestaltung" (Privacy by Design) zeichnet sich wie folgt aus:

- Begrenzung der erfassten Beschäftigtendaten und Umsetzung des Grundsatzes der Datenminimierung,
- Löschfristen und automatisierte Löschroutinen für nicht mehr benötigte Beschäftigtendaten,
- Auswertungsfunktionen zur Kontrolle, inwiefern Beschäftigtendaten nur zu berechtigten Zwecken genutzt werden,
- Einbindung von Interessenvertretungen und Beschäftigten zur Schaffung von Transparenz und Identifizierung von Einwänden und Verbesserungsmöglichkeiten, die in der Umsetzung konstruktiv aufgegriffen werden können,
- frühzeitige Einbindung von Schlüsselanwendern und Schlüsselanwenderinnen z. B. aus der IT und den Fachabteilungen.

4.2. Rechte der Beschäftigten

Eng verzahnt mit dem Beschäftigtendatenschutz sind die Rechte der Beschäftigten, was die Verarbeitung von Daten betrifft. Beschäftigte können sich gegenüber dem Unternehmen als datenverarbeitende Stelle auf eine Reihe von Rechten berufen. Dies sind im Kern dieselben Rechte, die die von einer Datenverarbeitung betroffenen Personen gegenüber der datenverarbeitenden Stelle geltend machen können (vgl. Abbildung 4). In diesem Zusammenhang sind hier etwa die Transparenz- und Rechenschaftspflichten der Unternehmen zu nennen.

Das Unternehmen muss seine Beschäftigten über die verarbeiteten Beschäftigtendaten und die Zwecke der Datenverarbeitung informieren. Dies kann mit der Bekanntmachung des Verfahrensverzeichnisses erfolgen. Des Weiteren haben die Beschäftigten ein Recht auf Auskunft zu den über sie gespeicherten Daten und auf Berichtigung falscher Daten. Ebenso besteht ein Recht auf Löschung der Daten, wenn deren Verarbeitung unzulässig ist.

4.3. Risikobewertung und Datenschutzfolgeabschätzung (DSFA)

Die Verarbeitung von Beschäftigtendaten im Unternehmen kann ein Risiko für die Beschäftigten bedeuten, auch wenn die Verarbeitung rechtmäßig erfolgt. Solche Risiken können z. B. dadurch entstehen, dass Unbefugte Einblick in die Beschäftigtendaten nehmen – z. B. infolge eines Hackerangriffs oder einer fehlerhaften Vergabe von Berechtigungen. Handelt es sich dabei um ein hohes Risiko für die Rechte und Freiheiten der Beschäftigten, muss eine Datenschutzfolgeabschätzung durchgeführt werden. Art. 35 DSGVO gibt Hinweise darauf, wann dies der Fall ist. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) veröffentlicht hierzu ergänzend eine Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist.

Dies bedeutet für die Praxis, dass der Verantwortliche der Datenverarbeitung eine Vorabprüfung bzw. Risikobewertung vornehmen sollte, ob ein hohes Risiko existiert und damit eine Datenschutzfolgeabschätzung überhaupt erst erforderlich wird. Im Beschäftigtenkontext ist dies möglicherweise die Verarbeitung von biometrischen Daten, Gesundheitsdaten oder Daten, mit denen eine durchgängige Erfassung des Verhaltens der Beschäftigten vorgenommen werden.

4.4. Datensicherheit und Beschäftigtendatenschutz

Mit der wachsenden Digitalisierung aller Geschäftsprozesse wächst die Anforderung, die Systeme und die Daten zu schützen. Ein Aspekt des Schutzes ist die Überprüfung der Einhaltung von Regelungen zur Datensicherheit. Moderne IT-Systeme bieten hierzu Datenauswertungen und Algorithmen an, die es ermöglichen, verdächtiges, kritisches oder unplausibles Verhalten zu identifizieren.

Die Umsetzung dieser Funktionen ist oftmals mit der Verarbeitung einer Vielzahl von personenbezogenen Daten von Beschäftigten verbunden. Damit einher geht ein tiefer Eingriff in die Persönlichkeitsrechte der Beschäftigten.

Im Hinblick auf die Datensicherheit erfordern automatisierte Kontrollen häufig eine Risikobewertung und ggf. eine Datenschutz-Folgeabschätzung. Darüber hinaus berührt der Einsatz dieser Systeme Mitbestimmungsrechte einer betrieblichen Interessenvertretung. Bei der Umsetzung solcher Sicherheitssysteme ist eine frühzeitige Einbindung des Sachverstands der Anbieter der jeweiligen Software-Lösung, des oder der Datenschutzbeauftragten, der Beschäftigten und der Interessenvertretung hilfreich.

Die Sicherheit der IT-Systeme und die Einhaltung von betrieblichen und gesetzlichen Regelungen liegt im Sinne aller Beteiligten. In welchem Umfang hierzu Beschäftigtendaten gespeichert und analysiert werden müssen, ist zwischen den Beteiligten zu klären.

5. Praxisbeispiel – Einführung eines digitalen Zeiterfassungssystems

Die wesentlichen Aspekte zum Beschäftigtendatenschutz kennen Sie nun. An einem praktischen Beispiel zur „Digitalen Zeiterfassung“ zeigen wir Ihnen jetzt die Umsetzungsschritte. Im Vordergrund steht die Frage: **Wie lässt sich der Beschäftigtendatenschutz konkret im Rahmen der Einführung eines Zeiterfassungssystems umsetzen?**

Der eine oder andere kennt sie wahrscheinlich noch – die gute alte Stempelkarte. Nach dem Einführen in die Stechuhr druckt diese die Stempelzeit auf einen Papierstreifen. Warum der ganze Aufwand? Zum einen, um die Löhne berechnen zu können. Zum anderen, um nachzuvollziehen, wie viel Zeit gearbeitet wurde. Egal, ob eine bestehende Technik abgelöst oder ein Zeiterfassungssystem neu eingeführt wird – der Kernprozess ist auch bei digitalen Zeiterfassungssystemen identisch: Digitale Zeiterfassungslösungen zeichnen die Arbeitszeiten von Arbeitnehmerinnen und Arbeitnehmern auf. Einziger Unterschied: Die Erfassung erfolgt jetzt mit neuer Hardware und/oder Software. Dabei werden z. B. Zeitterminals mit Chipkarten, Zeiterfassungs-Apps für das Smartphone und Browseranwendungen genutzt. In der Praxis können digitale Zeiterfassungssysteme ganz unterschiedlich aussehen:

Formen der digitalen Zeiterfassung

- Zeiterfassungsmodul/-software
- Self-Service/Portallösungen
- Terminal, Industrie-PC, Kiosk-PC in Kombination mit einem Transponder (Karte, Chip)
- PC, Notebook, Tablet, Smartphone, App
- Telefon-/Handyerfassung per Sprache

Die Zeiterfassung per Software kann zum einen über den eigenen PC erfolgen. Darüber hinaus lässt sich die Erfassung von Arbeitszeiten auch per Notebook, Tablet oder Smartphone realisieren.

Inzwischen kommen im Rahmen der Zeiterfassung vermehrt biometrische Verfahren zum Einsatz. Hierbei kann es sich zum Beispiel um eine Fingerabdruckerkennung handeln, die mit Hilfe eines Terminals umgesetzt wird. Biometrische Daten stuft die DSGVO gemäß Art. 4 Nr. 13 und 14 als besonders schützenswert ein, wodurch sich basierend auf Art. 9 Abs. 1 der DSGVO zunächst ein Verarbeitungsverbot ergibt. Aber auch hier gilt wie so oft: Ausnahmen sind möglich. Eine Verarbeitung von biometrischen Daten kann zulässig sein, wenn im zu prüfenden Einzelfall ein in Art. 9 Abs. 2 DSGVO genannter Tatbestand vorliegt. Grundsätzlich gilt: Die Erfassung darf nur im Rahmen einer Kollektivvereinbarung, einer Einwilligung durch die Beschäftigten und unter Wahrung der Verhältnismäßigkeit erfolgen. Eine individuelle, datenschutzrechtliche Prüfung wird daher empfohlen. Ergänzend sind die Mitbestimmungsrechte zu beachten.

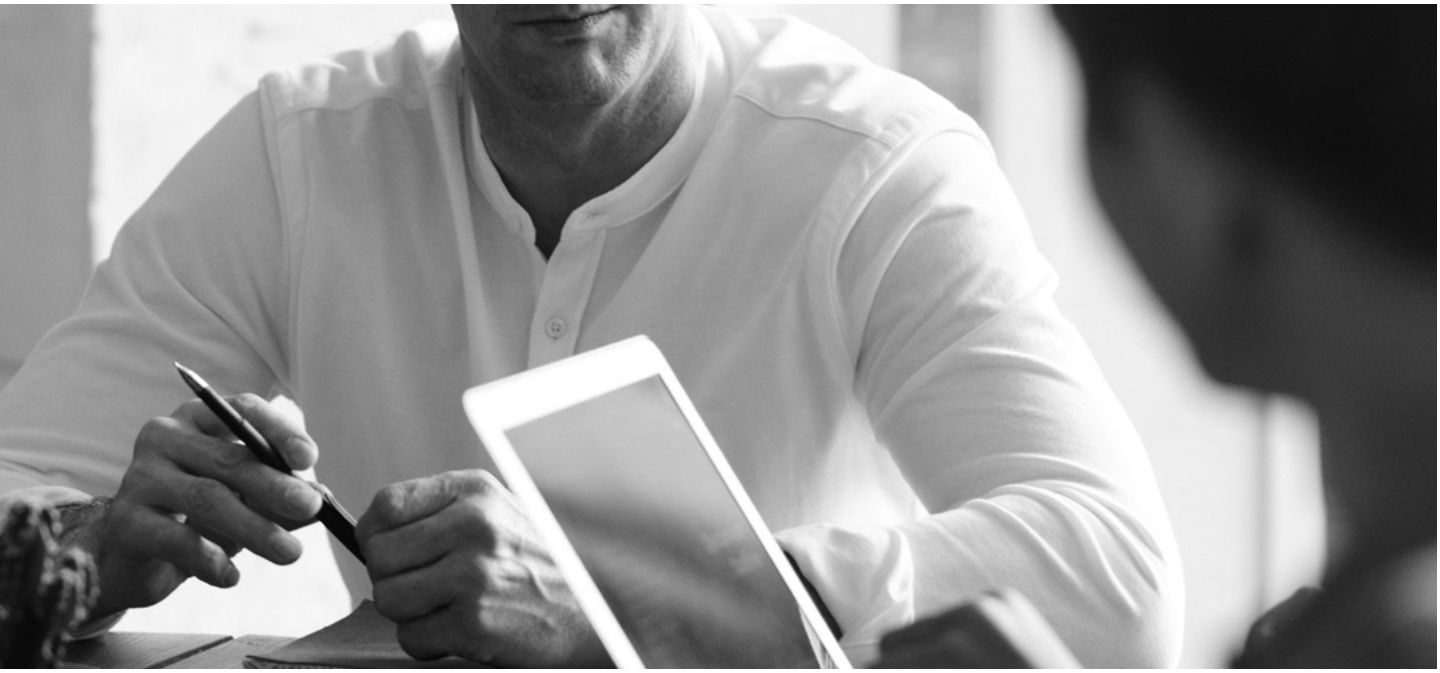
Die Erfassung von Arbeitszeiten kann mit verschiedenen Endgeräten und Software-Applikationen dezentral erfolgen, um diese dann zentral zu speichern. Wird das Zeiterfassungssystem nicht vor Ort im Unternehmen betrieben, erfolgt die Datenspeicherung bei externen Anbietern der Software oder in der Cloud. Zur Wahrung des Beschäftigtendatenschutzes ist es sinnvoll, sich ein Bild darüber zu verschaffen, wo, wie und durch wen die Zeiterfassungsdaten gespeichert und verarbeitet werden. Dabei ist sicherzustellen, dass sich die externen Dienstleister an die Datenschutzmaßnahmen des Unternehmens halten. Hierzu ist ein Vertrag zur Auftragsdatenverarbeitung (§ 11 BDSG) abzuschließen.

Mit digitalen Zeiterfassungssystemen lassen sich Arbeitsbeginn, Arbeitsende, Pausen und Abwesenheiten festhalten. Insbesondere die Abwesenheitsformen sind zwischen den betrieblichen Akteurinnen und Akteuren abzustimmen. Abwesenheiten wie Urlaub und Krankheit sind erforderlich. Weitere Funktionen können auch zur gegenseitigen Information oder für Genehmigungsprozesse z. B. bei Dienstreisen oder Weiterbildungen dienen.

Ausschlaggebend für den Beschäftigtendatenschutz sind die Zwecke, für die das digitale Zeiterfassungssystem unmittelbar eingesetzt wird. Zwecke, die unmittelbar der Durchführung des Arbeitsverhältnisses dienen, sind z. B. die Aufzeichnung von Beginn und Ende der Arbeitszeit. Ähnlich verhält es sich mit der Erfassung von Abwesenheiten, sofern diese – wie im Krankheitsfall – einer gesetzlichen Verpflichtung unterliegt oder die Erfassung von Abwesenheiten der Planung von Personal-Ressourcen dient. Bei der Planung der Prozesse sind die unterschiedlichen Zwecke daraufhin zu prüfen, ob die Umsetzung unterschiedliche Anforderungen an den Datenschutz stellt. Während die Information „Dienstreise“ zur Information für andere Beschäftigte sinnvoll und datenschutzkonform umsetzbar sein kann, gilt dies nicht für die Abwesenheit „Krankheit“. Diese Information unterliegt einem besonderen Schutzbedarf. Dementsprechend eng sind Zugriffsrechte bspw. auf unmittelbare Kolleginnen und Kollegen sowie die Personalbearbeitung zu beschränken.

Eng verknüpft mit der Zeiterfassung ist die Personaleinsatzplanung. Die Zeiterfassung erfasst zunächst nur die Arbeitszeiten von Beschäftigten. Das heißt, es werden die Ist-Daten verarbeitet. Mit Hilfe einer Personaleinsatzplanung wird einem Unternehmen ermöglicht, zur Verfügung stehende Beschäftigte entsprechend ihren Fähigkeiten an den jeweils „richtigen“ Stellen im Betrieb einzusetzen. Eine Verarbeitung von Soll-Daten wird in diesem Fall vorgenommen. Daten aus beiden Systemen können in der Zeiterfassungssoftware miteinander kombiniert, gegenübergestellt und verglichen werden.

An dieser Stelle werden jetzt die bereits vorgestellten fünf Schritte praktisch auf das Beispiel angewandt. Im Mittelpunkt steht bei dem Praxisbeispiel die Dokumentation von Arbeitszeiten sowie die Planung von Personal-Ressourcen, d. h. von Verfügbarkeiten. In einigen Betrieben werden mit Hilfe von digitalen Zeiterfassungssystemen ergänzend Bearbeitungszeiten verarbeitet. Hierzu zählen beispielsweise Auftragszeiten, Projektzeiten, Aufgabenzeiten, Kostenstellenzeiten und vieles mehr. Da eine Verarbeitung von Bearbeitungszeiten innerhalb von Zeiterfassungssystemen in vielen Betrieben jedoch nicht zum Tragen kommt und mit einer Verarbeitung solcher Daten eine andere Zweckbindung einhergeht, wird dieser besondere Sachverhalt in unserem Praxisbeispiel außen vorgelassen.



Schritt 1:
Zweckbestimmung festlegen

Im ersten Schritt sind die Zwecke zu bestimmen. Die Kernfrage hier: Zu welchen Zwecken wird das digitale Zeiterfassungssystem im Betrieb eigentlich genutzt? Dabei fällt auf, dass konkrete Antworten auf diese Frage oft schwerer fallen als gedacht.

Hilfreich für die Festlegung von Zwecken sind die beiden folgenden Fragen:

a) Zu welchen Zwecken wird das Zeiterfassungssystem grundsätzlich genutzt?

b) Zu welchen konkreten Zwecken dienen die einzelnen Verfahren des IT-Systems?

Zu welchen Zwecken wird das Zeiterfassungssystem grundsätzlich genutzt? Die Zeiterfassung wird grundsätzlich zur Dokumentation, Prüfung und Genehmigung von Arbeitszeiten und Abwesenheiten im Rahmen der arbeitsvertraglichen und/oder tariflichen Pflichten sowie zur Erfüllung gesetzlicher und ggf. tariflicher Dokumentationspflichten (Urlaub, Krankheit, etc.) verwendet.

Zu welchen konkreten Zwecken dienen die einzelnen Verfahren des IT- Systems? Um die konkreten Zwecke in Ergänzung festzulegen, sind die durch das Zeiterfassungssystem bereitgestellten Verfahren zu betrachten:

1. Verwaltung von Arbeitszeiten und Abwesenheiten zur Lohnabrechnung,
2. Auswertung von Arbeitsunfähigkeitstagen zum Zweck des betrieblichen Eingliederungsmanagements und der Lohnfortzahlung im Krankheitsfall,
3. Genehmigungen von Zeiteinträgen und Abwesenheitsanträgen,
4. Planung von Personal,
5. Auswertungen von Arbeitszeiten unter anderem zur Kontrolle der Einhaltung der Arbeitszeitgesetze und Tarifvereinbarungen.

Verwaltung von Arbeitszeiten und Abwesenheiten

Die Dokumentation der Arbeitszeiten kann als negative oder positive Zeiterfassung erfolgen. Bei der negativen Zeiterfassung wird die Arbeitszeit aus der Regelarbeitszeit oder aus einem Schichtplan ermittelt. Es werden nur die Abweichungen hiervon erfasst. Bei der positiven Zeiterfassung werden alle Arbeitszeiten genau festgehalten. Dies erfolgt in der Regel über eine Kommen-, Gehen- und Pausenerfassung. Die Verwaltung von Arbeitszeiten und Abwesenheiten ist erforderlich, um gesetzliche Dokumentationspflichten einzuhalten und Arbeitszeitkonten zu führen.

Auswertung von Arbeitsunfähigkeitstagen (AU)

Im Zeiterfassungssystem werden Tage der Arbeitsunfähigkeit hinterlegt. Eine Auswertung von AU-Tagen ist erforderlich, um zum Beispiel beurteilen zu können, ob ein Anspruch auf Lohnfortzahlung im Krankheitsfall besteht oder ob ein Verfahren zum betrieblichen Eingliederungsmanagement erforderlich ist. Ebenso muss die vorgesetzte Person wissen, welche Beschäftigten für die Arbeitsplanung zur Verfügung stehen.

Genehmigung von Zeiteinträgen und Abwesenheitsanträgen

Von den Beschäftigten erfasste Zeitbuchungen werden im Zeiterfassungssystem hinterlegt. Diese Buchungen und etwaige Zeitkorrekturen bzw. Nachbuchungen durch Beschäftigte oder hierzu beauftrage Personen lassen sich mit einem Genehmigungsprozess verknüpfen. Dieser Genehmigungsprozess greift zudem, wenn Beschäftigte Abwesenheiten (Urlaub, Sonderurlaub, Gleitzeit, Elternzeit etc.) beantragen. Ebenso lässt sich die Genehmigung von Urlaubsanträgen mit Vertretungsregelungen verknüpfen.

Anwendung bzw. Verfahren	Zweck der Verarbeitung	Kategorie von Beschäftigtendaten
Verwaltung von Arbeitszeiten und Abwesenheiten	Erfüllung gesetzlicher und ggf. tariflicher Dokumentationspflichten (Urlaub, Krankheit, etc.)	Anwesenheitszeiten Abwesenheitszeiten
Auswertung von AU-Tagen	Lohnfortzahlung im Krankheitsfall	AU-Tage
Genehmigungen von Zeiteinträgen und Abwesenheitsanträgen	Genehmigungen	Anwesenheitszeiten Abwesenheitszeiten Nicht Arbeitsunfähigkeit
Planung von Personal	Erstellung von Einsatzplänen	Zukünftige An- und Abwesenheiten ohne genaue Bezeichnung
Auswertungen der Arbeitszeiten	Überprüfung, ob die gesetzl. und tarifl. Arbeitszeitvorgaben eingehalten werden	Arbeitszeiten

Planung von Personal

Neben der Dokumentation von Arbeitszeiten wird mit einer digitalen Zeiterfassung im Regelfall der Zweck verfolgt, die Planung der Personaleinsätzen zu unterstützen. Im Kern geht es hierbei meist um die Frage, welche Personen für welche Tätigkeiten zur Verfügung stehen bzw. ob bestimme Personen momentan „verfügbar" sind. Erforderlich hierfür sind Informationen zu An- und Abwesenheiten. In der Regel ist es dabei unerheblich, um welche Abwesenheitsform es sich handelt. Ein Ziel kann dabei sein, Einsatzpläne zu erstellen, um hierdurch eine Mindestbesetzung für bestimmte Abteilungen zu gewährleisten oder Vertretungspersonal zu hinterlegen.

Auswertungen von Arbeitszeiten

Digitale Zeiterfassungssysteme bieten im Regelfall umfangreiche Auswertungsmöglichkeiten. Dabei werden meist Standardreports und individuelle Auswertungsmöglichkeiten unterschieden. Auswertungen werden mit digitalen Zeiterfassungssystemen häufig durchgeführt, um die Einhaltung von gesetzlichen und ggf. tariflichen Arbeitszeitvorgaben zu überprüfen. Derartige Überprüfungen nehmen zum Beispiel das Personalwesen oder Interessenvertretungen vor. Auch Auswertungen erfordern einen konkreten Zweck. So ist beispielsweise eine beliebige Auswertung von Krankheitsdaten ohne Grund nicht zulässig.

Im Rahmen der einzelnen Schritte sind die erarbeiteten Punkte in das Verzeichnis der Verarbeitungstätigkeiten (VVT) einzutragen. Wie dies in diesem Schritt beispielhaft ausgestaltet werden kann, zeigt die Tabelle 9: Verzeichnis der Verarbeitungstätigkeiten.

Einbindung von betrieblichen Akteurinnen und Akteuren

Zeiterfassungssysteme bieten an verschiedensten Stellen Möglichkeiten einer (un-)beabsichtigten Leistungs- und/oder Verhaltenskontrolle. Zudem sind im Sinne des Beschäftigtendatenschutzes die benötigten Rechtsgrundlagen zu klären bzw. zu schaffen. Um einen reibungslosen Projektverlauf zu gewährleisten, ist es in den meisten Fällen vorteilhaft, alle relevanten Interessengruppen von Anfang an eng in das Projekt einzubinden. Fragen zur Mitbestimmung sowie zur Rechtmäßigkeit der Verarbeitung lassen sich hierdurch frühzeitig klären. Bei der Einführung einer digitalen Zeiterfassung setzt sich der Kreis der Interessengruppen beispielsweise aus den folgenden Gruppen zusammen:

- Beschäftigte,
- Führungskräfte,
- Interessenvertretung,
- der oder die betriebliche Datenschutzbeauftragte,
- der oder die Zeitbeauftragte,
- Key-User,
- Projektmanagement,
- Personalwesen,
- interne oder externe IT,
- Hersteller Gehaltsabrechnungssoftware.

Die Tabelle 9: Verzeichnis der Verarbeitungstätigkeiten

	Datenempfangende/ Zugriffsberechtigte	Rechtsgrundlage	Aufbewahrungsfrist
	Vorgesetze Personalwesen	§ 26 BDSG	6 Jahre und 10 Jahre
	Vorgesetze Personalwesen	§ 26 BDSG	3 Jahre
	Vorgesetzte Beschäftigte	Einwilligung	6 Jahre
	Vorgesetzte	Einwilligung	2 Jahre
	Personalwesen Interessenvertretungen	§ 26 BDSG	2 Jahre

Schritt 2:
Erfassung und Festlegung der zu verarbeitenden Kategorien von Beschäftigtendaten

Nachdem im ersten Schritt die Zwecke bestimmt wurden, werden in dieser Phase die zu verarbeitenden Kategorien von Beschäftigtendaten geprüft und festgelegt.

In unserem Fallbeispiel lassen sich Kategorien von Beschäftigtendaten wie folgt bilden:

- Zeitbuchungen: Kommen, Gehen, Pausenbeginn und -ende,
- Abwesenheiten: Urlaub, Gleitzeit, Dienstgang, Weiterbildung, Arbeitsunfähigkeit,
- Personenstammdaten: Name, Personalnummer, Abteilung, MA-Ausweisnummer, registrierter Token / ID,
- ggf. weitere Personendaten, wie Kontaktdaten, Fähigkeiten, Zertifikate etc.

Wie sich die Kategorien von Beschäftigtendaten in das VVT eintragen lassen, zeigt exemplarisch die Tabelle 9: Verzeichnis der Verarbeitungstätigkeiten.

Schritt 3:
Festlegung der Datenempfängerinnen und -empfänger

Nach der Erfassung und Festlegung der zu verarbeitenden Kategorien werden im nächsten Schritt die Datenempfängerinnen und -empfänger bestimmt. Damit sind alle Personen gemeint, die innerhalb und außerhalb des Betriebes Zugriff auf die Beschäftigtendaten im System erhalten. Sinnvoll ist es, anstelle von Personen die Kategorien von Datenempfängerinnen und -empfänger zu dokumentieren. In unserem Fall sind dies Zeitbeauftragte, direkte Vorgesetzte, Administratoren, Personalwesen und – je nach konkreter Ausgestaltung des Systems – auch weitere Personengruppen. Dies können z. B. auch Mitarbeitende eines IT-Dienstleisters sein, die zur Administration und Pflege Zugriff auf das System erhalten. In der Regel werden die Grundsätze und die Berechtigungsgruppen in einem Berechtigungskonzept formuliert. In der praktischen Umsetzung bilden die festgestellten Datenempfänger- bzw. Nutzergruppen und deren Zwecke und Aufgaben die Grundlage für die Festlegung von Berechtigungsgruppen bzw. -rollen im IT-System.

Folgende Kategorien an Datenempfängerinnen und -empfänger können beispielhaft unterschieden werden:

- **Personalwesen:** Beschäftigte im Bereich der Personalabrechnung und Personaladministration verarbeiten Zeitdaten und An-/Abwesenheitsdaten zum Zweck der Zeitwirtschaft und der Umsetzung der gesetzlichen Pflichten. Bei Zeitlohn kann die Entgeltabrechnung ein weiterer Zweck sein.
- **Vorgesetzte:** Beschäftigte, die eine Leitungsrolle innehaben und als Führungskräfte tätig sind. Vorgesetzte entscheiden z. B. über Anträge von Beschäftigten bzgl. Urlaub, Fortbildung etc. Ebenso benötigen diese die aktuellen Arbeitsunfähigkeitsdaten zum Zwecke der Arbeitsplanung.
- **Beschäftigte:** Alle Beschäftigten verarbeiten zum Zweck der Zeiterfassung und der Überprüfung der erfassten Zeiten die eigenen Zeitdaten.
- **Betriebliche Interessenvertretung:** Betriebsrat, Personalrat oder Mitarbeitervertretung dürfen die Einhaltung der Datenschutzvorgaben, der Arbeitszeitgesetze und der Kollektivvereinbarungen überprüfen. Deshalb erhalten Sie einen lesenden Zugriff auf die Zeitdaten sowie Einstellungen und Konfigurationen des Zeiterfassungssystems. Diese Berechtigungen spiegeln, im Gegensatz zu einem Versand von Beschäftigtendaten mittels Excel, einen guten Datenschutz wider.
- **Technische Administratoren:** Systemadministratoren verarbeiten alle Systemdaten, wie Systemprotokolle, Systemkonfigurationen oder Berechtigungen. Sie haben in der Regel Zugriff auf alle im System erfassten Daten der Zeiterfassung.
- **Betriebliche Datenschutzbeauftragte:** Datenschutzbeauftragte verarbeiten lesend zum Zweck der Überprüfung der Einhaltung der Datenschutzvorgaben die Einstellungen und Konfigurationen des Zeiterfassungssystems.

Wie die Datenempfängerinnen und -empfänger in das Verzeichnis der Verarbeitungstätigkeiten hinterlegt werden, zeigt die Tabelle 9: Verzeichnis der Verarbeitungstätigkeiten.

Schritt 4:
Klärung und ggf. Schaffung einer Rechtsgrundlage

Um personenbezogene Daten rechtmäßig verarbeiten zu können, bedarf es einer entsprechenden Rechtsgrundlage. Hierdurch wird die Datenverarbeitung legitimiert.

An dieser Stelle kann auf die zu Beginn vorgenommene Bestimmung der Zwecke zurückgegriffen werden. Wie festgestellt wurde, dient das System zur Erfassung der Arbeitszeit sowie zur Verwaltung der tariflich und gesetzlich erforderlichen Abwesenheiten ausschließlich Zwecken des Beschäftigungsverhältnisses. Insofern liefert § 26 BDSG eine ausreichende Rechtsgrundlage.

Wie jedoch damit umgehen, wenn angedacht ist, personenbezogene Daten zu verarbeiten, die nicht dem Zwecke des Beschäftigtenverhältnisses dienen? Ist dies bei einem digitalen Zeiterfassungssystem realistisch? Diese Frage stellt sich dann, wenn zum beispielsweise bestimmte personenbezogene Auswertungen gewünscht werden. In solchen Fällen lassen sich vielfach individuelle Lösungen über Einwilligungen mit den Beschäftigten oder über Kollektivvereinbarungen – bei vorhandener Interessenvertretung – erreichen. Es empfiehlt sich zudem zu überprüfen, inwieweit bzw. welche Mitbestimmungsrechte der Interessenvertretung betroffen sind.

Ist eine Rechtsgrundlage vorhanden, wie zum Beispiel § 26 BDSG, werden nicht alle potentiell möglichen Verarbeitungen und Nutzungen von Beschäftigtendaten „automatisch" legitimiert. Wenn beispielsweise eine Erfassung von Krankheitstagen erforderlich ist, stellt sich dennoch die Frage, welche Personen in welchem Umfang Zugriff auf diese Informationen erhalten. In unserem Beispiel sind dies beispielsweise die direkten Vorgesetzten, die Kenntnis über aktuelle Krankheitsfälle für die Arbeitsplanung benötigen, oder Beschäftigte aus der Lohnbuchhaltung, welche diese Informationen zum Zweck der Lohnfortzahlung im Krankheitsfall verarbeiten.

Die Tabelle 9 zeigt, wie und welche Rechtsgrundlagen sich bei der Einführung einer digitalen Zeiterfassung verwenden lassen.

Schritt 5:
Festlegung der Aufbewahrungs- bzw. Löschfristen

Im letzten Schritt werden die Aufbewahrungs- bzw. Löschfristen festgelegt. Diese ergeben sich aus unterschiedlichen Rechtsquellen. Grundsätzlich gilt, dass Daten mit Beschäftigtenbezug so lange aufbewahrt werden dürfen, wie Sie für die genannten Zwecke erforderlich sind bzw. eine gesetzliche Vorgabe dies vorsieht. Sofern eine gesetzliche Pflicht zur Aufbewahrung besteht, ist es empfehlenswert, die Daten vor einer vorzeitigen Löschung zu schützen.

Bei dem digitalen Zeiterfassungssystem greifen mehrere gesetzliche Aufbewahrungs- und Verjährungsfristen, wie die untenstehende Aufzählung verdeutlicht. Neben den unten genannten Beispielen können sich aus dem SGB, AGG usw. noch weitere, anderslautende Aufbewahrungs- und Verjährungsfristen ergeben.

Beispiele für Aufbewahrungs- bzw. Löschfristen:

- **Zeitdaten für die Personaladministration.** Derzeit existiert für Beschäftigte eine Pflicht nach § 16 Abs. 2 ArbZG, die über die werktägliche Arbeitszeit des § 3 Satz 1 hinausgehende Arbeitszeit (8 h) aufzuzeichnen. Die Aufbewahrungsfrist beträgt 2 Jahre.
- **Arbeitszeitnachweis für Minijobs und Vollzeitbeschäftigte** gemäß § 17 Mindestlohngesetz und § 2a Schwarzarbeitsbekämpfungsgesetz. Die Aufbewahrungsfrist beträgt 2 Jahre.
- **Für den Lohnsteuerabzug bedeutsame Unterlagen**. Für Arbeitszeitlisten gilt zum Beispiel eine Aufbewahrungsfrist von 6 Jahren gemäß § 147 Abs. 1 Nr. 5 und Abs. 3 Abgabenordnung.
- **§ 19 Abs. 1 des Arbeitnehmerentsendegesetzes (AEntG).** Hiernach ist der Arbeitgeber verpflichtet, sowohl den Beginn, das Ende als auch die Dauer der täglichen Arbeitszeit seiner Beschäftigten aufzuzeichnen. Die Aufbewahrungsfrist beträgt 2 Jahre.
- **Handels- und Geschäftsbriefe u. a. nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO).** Damit ist der Austausch von Informationen mit externen Geschäftspartnerinnen und -partnern im Rahmen eines gemeinsamen Geschäftes gemeint. Hierzu gehören Bearbeitungszeiten, die für eine Abrechnung mit den Kundinnen und Kunden erforderlich sind. Die Aufbewahrungspflicht beträgt 6 Jahre.
- **Protokolle zu Auswertungen und Analysen von Beschäftigtendaten** (§ 26 BDSG Beschäftigungsverhältnisses in Kombination mit § 76 BDSG Protokollierung). Die Aufbewahrungspflicht besteht bis Ende des Folgejahres.

Wie sich die Aufbewahrungsfristen im Verzeichnis der Verarbeitungstätigkeiten hinterlegen lassen, veranschaulicht die Tabelle 9.

6. Fazit

Diese Broschüre stellt Verfahren vor, die dabei unterstützen, den Beschäftigtendatenschutz bei Digitalisierungsprojekten umzusetzen. Bei der Anwendung in der Praxis hat sich gezeigt, dass die folgenden Maßnahmen entscheidend zum Erfolg beitragen können:

- Erkennung und angemessene Einbindung aller Betroffenen in den Prozess.
- Gemeinsame Festlegung der Projekt- und Datenschutzziele sowie eine transparente Kommunikation mit alle Betroffenen.
- Einplanung der Datenschutz-Anforderungen in allen Projektschritten.

Die frühzeitige Information und Beteiligung von Beschäftigten ebenso wie ein nachvollziehbar organisierter Datenschutz in Digitalisierungsprojekten können einen entscheidenden Beitrag dazu leisten, um Vorbehalte abzubauen sowie Impulse zu liefern, die helfen Maßnahmen besser auf Bedarfe und Rahmenbedingungen anzupassen. Daraus entsteht häufig erheblicher Nutzen und eine Beschleunigung bei der Umsetzung von Digitalisierungsprojekten. Die in dieser Broschüre beschriebenen sechs Schritte zum Beschäftigtendatenschutz geben hierzu eine praktische Hilfestellung.

Wir wünschen Ihnen für Ihre künftigen Projekte gutes Gelingen. Teilen Sie uns gerne Ihre Erfahrungen mit. Wir freuen uns von Ihnen zu hören.

Ihre Initiative Arbeit & Wirtschaft 4.0

7. Wichtige Begriffe

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Bei der Verarbeitung personenbezogener Daten sind die Datenschutzgesetze anzuwenden. Bei nicht personenbezogenen Daten finden die Datenschutzgesetze keine Anwendung.

Personenbezogene Daten von Beschäftigten oder Beschäftigtendaten sind alle Informationen, die sich auf als Person identifizierbare Beschäftigte beziehen und durch das Unternehmen verarbeitet werden. Beschäftigtendaten sind somit eine Teilmenge der „personenbezogenen Daten". Bei der Verarbeitung von Beschäftigtendaten sind neben der DSGVO die einschlägigen Bestimmungen des BDSG zum Beschäftigtendatenschutz anzuwenden.

Datenkategorien und deren Abgrenzungen zueinander sind in der DSGVO nicht als Begriff definiert. Sie können sinnvoll für die Führung eines Verfahrensverzeichnisses verwendet werden. Datenkategorien können gleichartige Daten zusammenfassen und somit den Dokumentationsaufwand verringern. Als Datenkategorie können z. B. Bankdaten alle mit einem Bankkonto verbundenen Daten beschreiben.

Datenempfänger sind natürliche oder juristische Personen, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihnen um Dritte handelt oder nicht (s. Art. 4 DSGVO). Innerhalb des Unternehmens haben die Personen (Empfängerkategorie) Zugriff auf jene Beschäftigtendaten, die sie für die Durchführung Ihrer Aufgaben benötigen. Die Zugriffe werden bei den meisten Systemen über Rollen und Berechtigungen organisiert und in Berechtigungskonzepten dokumentiert.

Interessenvertretungen: Aufgrund von Mitbestimmungsgesetzen und -verordnungen in Unternehmen gewählte Betriebsräte, Personalräte oder Mitarbeitervertretungen. Diese Gremien besitzen bei der Verarbeitung von Beschäftigtendaten gesetzlich festgeschriebene Mitbestimmungsrechte insbesondere in Bezug auf die Regelung des zulässigen Umfangs möglicher Leistungs- und Verhaltenskontrolle. Bei der Umsetzung des Beschäftigtendatenschutzes haben Interessenvertretungen Informationsrechte und den Auftrag, über die Umsetzung der zum Schutz der Beschäftigten geltenden Gesetze zu wachen.

Verarbeitung Bei jedem Vorgang in Zusammenhang mit personenbezogenen Daten handelt es sich um eine Verarbeitung. Typische Vorgänge sind beispielsweise das Erheben, Abfragen, Speichern, Verwenden und Löschen von personenbezogenen Daten. Dabei spielt es keine Rolle, ob die Verarbeitung digital oder manuell erfolgt.

Als **betroffene Person** gelten die Personen, deren Daten verarbeitet werden. Im Rahmen des Beschäftigtendatenschutzes sind dies die Beschäftigten.

Verantwortlicher ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Diese natürliche oder juristische Person ist für die Umsetzung des Datenschutzes verantwortlich und haftet dafür. In der Praxis ist dies die juristische vertretungsberechtigte Person, in der Regel also die Geschäftsführung oder die Vorstände eines Unternehmens.

Betriebliche Datenschutzbeauftragte (bDSB) beraten den Arbeitgeber zu Anforderungen und Aufgaben des Datenschutzes und unterstützen bei der Umsetzung. Darüber hinaus haben sie eine eigenständige Überwachungsaufgabe und schulen Mitarbeitende. Die Funktion des/der betrieblichen Datenschutzbeauftragten kann von Beschäftigten des Unternehmens oder von spezialisierten externen Dienstleistern übernommen werden.

Die Pflicht zum Einsatz eines oder einer Datenschutzbeauftragten besteht für Unternehmen, die ständig 10 oder mehr Beschäftigte mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. In der Praxis ist dies oftmals schon gegeben, wenn 10 Personen ständig mit einem IT-System arbeiten.

8. Quellen

BMF-Schreiben vom 16.07.2001 (IV D 2 – S 0316 – 136/01):
„Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“

BMF-Schreiben vom 14.11.2014 (IV A 4 – S 0316/13/10003):
„Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“

Datenschutzgrundverordnung: DSGVO

Bundesdatenschutzgesetz: BDSG

Betriebsverfassungsgesetz: BetrVG

Landespersonalvertretungsgesetz NRW:; LPVG NRW

Landesdatenschutzgesetz NRW: LDSG NRW

Bundesamt für Sicherheit in der Informationstechnik: BSI

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.: Bitkom

Kommentar EU-DSGVO und BDSG Däubler / Wedde / Weichert / Sommer