

Christian K. Bosse, Aljoscha Dietrich, Andreas Weßner

Selbstbewertungsinstrument für den betrieblichen Datenschutz

Unterstützung für die Umsetzung des Beschäftigtendatenschutzes in KMU

Die rechtskonforme Umsetzung des betrieblichen Datenschutzes stellt für kleine und mittlere Unternehmen (KMU) mitunter teils große Herausforderungen dar. Wird ein Datenschutzbeauftragter oder ein Verarbeitungsverzeichnis benötigt? Decken die umgesetzten Maßnahmen die rechtlichen Anforderungen ab? Sind die Beschäftigten ausreichend bezüglich des Datenschutzes sensibilisiert? Dies sind nur einige Fragen, die Geschäftsführung oder weitere Mitglieder der Leitungsebene zu beachten haben. Das dafür notwendige Durcharbeiten und Verstehen der entsprechenden Gesetze und Verordnungen ist für juristische Laien ein zeitaufwendiger Prozess. An dieser Stelle setzt das in diesem Beitrag vorgestellte Selbstbewertungsinstrument an. Es unterstützt Verantwortliche im Unternehmen bei der Umsetzung des Beschäftigtendatenschutzes und zeigt Entwicklungspotenziale auf.

1 Hintergrund

In einer digitalisierten Arbeitswelt nimmt der Einsatz neuer Technologien einen zentralen Stellenwert ein. Der steigende Grad der Digitalisierung in den Unternehmensbereichen und -prozessen trägt u. a. dazu bei, dass unterschiedliche Daten nicht nur zu Produkten und Produktionsanlagen, sondern auch zu den Beschäftigten erfasst und ausgewertet werden. Beispielsweise ist dies beim Einsatz eines informatorischen Assistenzsystems zu erkennen, das den Mitarbeiter¹ bei der fehlerfreien und variablen Ausführung seiner Tätigkeiten unterstützt.² Gleichzeitig ermöglicht die Speicherung der (Meta-)Daten durch das Assistenzsystem, also bspw. welcher Mitarbeiter wann welchen Arbeitsschritt ausgeführt hat, eine Auswertung der individuellen Arbeitsgeschwindigkeit bzw. Effektivität. Auch beim Einsatz physischer Assistenzsysteme, wie z. B. eines Exoskeletts, das den Mitarbeiter bei der Ausführung von körperlich schweren Tätigkeiten unterstützt, werden große Mengen an personenbezogenen Sensordaten verarbeitet.³

Dies verdeutlicht den existierenden Konflikt in vielen Unternehmen: Einerseits kann die Verarbeitung personenbezogener



Christian K. Bosse

Wissenschaftlicher Mitarbeiter am Institut für Technologie und Arbeit e.V. an der Technischen Universität Kaiserslautern.

E-Mail: christian.bosse@ita-kl.de



Aljoscha Dietrich

Wissenschaftlicher Mitarbeiter am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes.

E-Mail: aljoscha.dietrich@uni-saarland.de



Andreas Weßner

Wissenschaftlicher Mitarbeiter am Institut für Technologie und Arbeit e. V. an der Technischen Universität Kaiserslautern.

E-Mail: andreas.wessner@ita-kl.de

¹ Aufgrund der besseren Lesbarkeit wird auf eine Nennung aller Geschlechter im Folgenden verzichtet.

² Vgl. *Hinrichsen/Bendzioch, How Digital Assistance Systems Improve Work Productivity in Assembly*, in: Nunes (Hrsg.), *Advances in Human Factors and Systems Interaction. AHFE 2018. Advances in Intelligent Systems and Computing*, Bd. 781, Cham 2019, S. 332–342.

³ Vgl. *Gesmann-Nuissl, Rechtliche Herausforderungen in der Arbeitswelt 4.0 im Mittelstand anhand von zwei Beispielen*, in: Zink/Bosse (Hrsg.), *Arbeit 4.0 im Mittelstand, Chancen und Herausforderungen des digitalen Wandels für KMU*, Berlin, Heidelberg 2019, S. 35–53.

Daten durchaus im Interesse von Arbeitnehmern sein, etwa wenn dadurch präventiv vermeidbaren Belastungen oder Krankheiten entgegengesteuert werden kann. Andererseits wird die Gefahr einer ggf. unzulässigen Überwachung der Mitarbeiter deutlich. Um die Verarbeitung personenbezogener Daten rechtskonform auszugestalten, ergeben sich aus der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) verschiedene Pflichten für Arbeitgeber. Diese werden in der unternehmerischen Praxis jedoch eher als hinderlich wahrgenommen, wie eine Studie der Bitkom zeigt. Hiernach sehen 79 Prozent von 603 befragten Unternehmen in den Anforderungen an den Datenschutz die größte Hürde für den Einsatz neuer Technologien.⁴

Selbst wenn einzelne Maßnahmen im Unternehmen bereits ergriffen wurden, bestehen oft von Arbeitgebern unbedachte oder bis dato unbekannt Lücken im Beschäftigtendatenschutz. Gleichzeitig führen die potenziell drohenden Strafen, die bei erkannten und geahndeten Verstößen bis in Millionenhöhe verhängt werden können, in vielen Unternehmen zu großen Unsicherheiten.⁵ Dies führt zu der Herausforderung, vor der insbesondere KMU bei der rechtskonformen Umsetzung gesetzlicher Vorgaben stehen. Um die in juristischer Fachsprache verfassten rechtlichen Verordnungen und Gesetze zu verstehen sowie den aktuellen Stand des Beschäftigtendatenschutz zu überprüfen, fehlen meist das interne Fachwissen sowie die finanziellen Ressourcen für das Heranziehen einer Beratungsdienstleistung.

2 Lösungsansatz für die Praxis: Selbstbewertungsinstrument

Um den Ist-Zustand des Beschäftigtendatenschutzes im Unternehmen ohne großen Ressourcenbedarf oder Unterstützung externer Berater zu ermitteln, bietet sich der Einsatz eines Selbstbewertungsinstruments an. Das Konzept der Selbstbewertung entstammt ursprünglich dem Bereich des Qualitätsmanagements und findet sich daher auch als durchgängiger Bestandteil der Normreihe ISO 9000, die den Aufbau von Qualitätsmanagementsystemen im Fokus hat. Entsprechend wird die Selbstbewertung als eine systematische Analyse anhand von im Voraus festgelegten Kriterien definiert, die mit einer gewissen Objektivität eine Standortbestimmung oder Selbstdiagnose ermöglicht. Diese wiederum ist eine Grundvoraussetzung für eine kontinuierliche Verbesserung, sodass die Selbstbewertung am Anfang eines solchen Prozesses zur Verbesserung bzw. Weiterentwicklung steht.⁶

Im Zuge der Digitalisierung und Weiterentwicklung im Bereich der Künstlichen Intelligenz etablierte sich in den letzten Jahren das Instrument der Selbstbewertung als digitaler Check. Dieses findet sich in den verschiedensten Anwendungsfeldern, in denen mit Hilfe von Checklisten und/oder Fragenkatalogen eine Selbstbewertung vor dem Hintergrund eines Reifegradmodells ermöglicht wird. Beispiele hierfür sind u.a. der Readiness-Check Digitalisierung des Mittelstand 4.0-Kompetenzzentrums Kaiserslautern⁷ zur Standortbestimmung bezüglich der digitalen Reife eines Unternehmens oder der Online-Check zum Arbeitsschutz der Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege⁸. Die Vorteile dieser Online-Checks liegen zum einen in der leichten Handhabung des Instruments, zum anderen in der meist direkten Auswertung der Ergebnisse, die dem Nutzer eine aktuelle „Standortbestimmung“ und Orientierung gibt. Bei mehreren Checks werden darüber hinaus im Ergebnisprofil der Selbstbewertung ergänzend Entwicklungspotenziale aufgezeigt und Lösungen aus Expertensicht vorgeschlagen.⁹ Auf diese Weise generieren Selbstbewertungsinstrumente einen zusätzlichen Nutzen insbesondere für KMU.

Wie Recherchen im Rahmen des Projekts „Transparente und selbstbestimmte Datennutzung im Unternehmen (TrUSD)“ ergeben haben, ist ein Selbstbewertungsinstrument, das den Beschäftigtendatenschutz in Unternehmen zum Gegenstand hat, aktuell noch nicht verfügbar. Entsprechend wurden die Entwicklung und Umsetzung eines solchen angestoßen. Ziel des Instruments ist zum einen Unternehmen für das Thema Datenschutz zu sensibilisieren. Zum anderen soll Geschäftsführern, Führungskräften und weiteren Verantwortlichen eine praxisgerechte Unterstützung bei der (Weiter-)Entwicklung einer unternehmensspezifischen und rechtskonformen Umsetzung des Beschäftigtendatenschutzes zur Verfügung gestellt werden. So kann das Instrument z. B. auch Empfehlungen für die Erarbeitung einer Betriebsvereinbarung liefern. Dies ermöglicht, im Rahmen eines fairen Interessensausgleiches zwischen Arbeitnehmern, Arbeitnehmervertretung und Arbeitgebern, die vollen Potenziale der Technologie rechtskonform auszuschöpfen und (Arbeits-)Prozesse zu optimieren.

Eine wichtige Rolle spielt ebenso das Verzeichnis von Verarbeitungstätigkeiten (auch Verarbeitungsverzeichnis) im Sinne des Art. 30 DSGVO, wonach alle Verarbeitungstätigkeiten in der Zuständigkeit des Verantwortlichen zu erfassen sind. Ein existierendes Verarbeitungsverzeichnis kann sich als sehr nützlich bei der Beantwortung des Selbstbewertungsinstruments erweisen. Fehlt es, kann dies ein erstes Versäumnis des Unternehmens offenbaren. In diesem Fall kann ein entsprechend ausgestaltetes Selbstbewertungsinstrument ggf. den Verantwortlichen bei der Erstellung des Verzeichnisses unterstützen. Ein Verarbeitungsverzeichnis ist nicht verpflichtend von jedem Unternehmen zu führen.¹⁰ Dennoch empfiehlt sich die Umsetzung grundsätzlich, da ein Verarbeitungsverzeichnis vielfachen Nutzen haben kann. Vordringend steht die Schaffung von Transparenz über die Verarbeitung von personenbezogenen Daten im Unternehmen, es kann jedoch auch der rechtlichen Absicherung dienen. So lässt sich ein Nachweis über eine rechtskonforme Umsetzung der Verordnung bringen.¹¹ Auch erweist es sich als nützlich bei der Befolgung allgemeiner Verpflichtungen der DSGVO, etwa der Betroffenenrechte gemäß Art. 12-23 DSGVO.

7 Vgl. Bosse/Hellge, Digitalisierung im Mittelstand, Zeitschrift für Organisationsentwicklung ZOE 2018, S. 102-103.
8 Vgl. Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege, Online-Check zum Arbeitsschutz, Heilberufe 2017, S. 41.
9 Vgl. Hellge/Schröder/Zink, Der Readiness-Check Digitalisierung als Instrument im digitalen Transformationsprozess, in: Lingnau/Müller-Seitz/Roth (Hrsg.), Management der digitalen Transformation, München 2019, S. 171-186.
10 Siehe hierzu Art. 30 Abs. 5 DSGVO.
11 Vgl. Erwägungsgrund 82 der DSGVO.

4 Vgl. Bitkom (Hrsg.), Digitalisierung der Wirtschaft, 2020, URL: https://www.bitkom.org/sites/default/files/2020-03/bitkom-charts-digitalisierung-der-wirtschaft-01-04-2020_final.pdf (letzter Abruf 21.10.2020).

5 Vgl. Becker/Ulrich/Fibitz/Schuhknecht/Reitelshöfer, Digitale Arbeitswelten im Mittelstand, Veränderungen und Herausforderungen, Springer 2019; Bergt, Sanktionierung von Verstößen gegen Datenschutz-Grundverordnung, DuD 2017, S. 555-561.

6 Vgl. Kamiske/Brauer, Qualitätsmanagement von A-Z, München 2011.

3 Grundlage für die Entwicklung

Den Ausgangspunkt für die Entwicklung des Selbstbewertungsinstrumentes bildet ein Kriterien- bzw. Fragenkatalog, der eine systematische Erfassung des Ist-Zustands und eine Bewertung der Umsetzung datenschutzrechtlicher Anforderungen sowohl aus arbeitswissenschaftlicher als auch aus rechtswissenschaftlicher Perspektive ermöglicht. Beide Perspektiven werden in den folgenden Abschnitten 3.1 und 3.2 beleuchtet.

Der Kriterienkatalog basiert zum einen auf den Ergebnissen des TrUSD-Projekts, insbesondere der Anforderungserhebung mit mehreren potentiellen Anwendungspartnern, den erhobenen Datennutzungs- und Schutzbedarfen sowie den Selbstbestimmungs- und Transparenzbedarfen.¹² Zum anderen spiegeln sich darin die Anforderungen der DSGVO sowie die Gewährleistungsziele des Standard-Datenschutzmodells¹³ wider, ebenso wie aktuelle Erkenntnisse aus der arbeitswissenschaftlichen Forschung. Im Kriterienkatalog werden somit auch „weiche“ Faktoren adressiert, die ebenfalls ein wichtiger Bestandteil der praktischen Umsetzung eines effektiven Beschäftigtendatenschutzes in Unternehmen sind. Dazu gehören die Information, Sensibilisierung und Qualifizierung der Mitarbeiter in Bezug auf den Beschäftigtendatenschutz.¹⁴ Dies gilt umso mehr, wenn das Unternehmen die personenbezogenen Daten – unter Einhaltung der rechtlichen Voraussetzungen und mit Zustimmung der Mitarbeiter – für die Optimierung organisationaler Prozesse heranziehen will.

Basierend auf dieser umfassenden Grundlage werden mit der Umsetzung eines Selbstbewertungsinstrumentes für den Beschäftigtendatenschutz folgende Ziele angestrebt:

- ♦ eine möglichst vollständige, umfassende und praxisnahe Abschätzung der verschiedenen Facetten des Beschäftigtendatenschutzes in Unternehmen,
- ♦ allgemeine Verständlichkeit der aus den rechtlichen Verordnungen resultierenden Anforderungen und damit einhergehenden Fragestellungen für juristische Laien,
- ♦ Identifikation von Optimierungspotenzialen sowie ggf. bestehender Lücken des Beschäftigtendatenschutzes in Unternehmen,
- ♦ Unterstützung bei der Umsetzung eines vollumfänglichen, rechtskonformen und eventuell technologiebasierten Beschäftigtendatenschutzes,
- ♦ Beitrag zu dem Aufbau einer Vertrauenskultur im Unternehmen im Hinblick auf die Transparenz und Verständlichkeit der Datennutzung v. a. im Zuge fortschreitender Digitalisierung.

12 Vgl. Hierzu u. a. *Polst/Kelbert/Feth*, Company Privacy Dashboards: Employee Needs and Requirements, in: HCl for Cybersecurity, Privacy and Trust: First International Conference, HCl-CPT 2019, Held as Part of the 21st HCl International Conference, HCII 2019.

13 Vgl. AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.), Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0, 98, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 5.-7. November 2019. Hierzu gehören auch die umfassenderen Maßnahmenkataloge, die in einzelnen Bausteinen zu verschiedenen Themenbereichen veröffentlicht werden.

14 Vgl. *Wagner*, Datenschutz als Bildungsauftrag, DuD 2012, S. 83-87.

3.1 Rechtswissenschaftliche Perspektive

Was die Umsetzung datenschutzrechtlicher Anforderungen der DSGVO angeht, bietet unter anderem das Standard-Datenschutzmodell (SDM)¹⁵ des AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine systematische Handreichung für Unternehmen und Organisationen. Das SDM soll beispielsweise bei der Überführung von rechtlichen Anforderungen in technische und organisatorische Maßnahmen unterstützen. Zu diesem Zweck wird ein Katalog von sogenannten Referenz- und generischen Maßnahmen bereitgestellt, deren Zweck es ist, dass bei jeder einzelnen Verarbeitung geprüft werden kann, ob das rechtliche „Soll“ mit den passenden Maßnahmen entsprochen wird. Der Maßnahmenkatalog des SDM ist jedoch zu komplex und umfangreich, als dass er direkt in einen Kriterienkatalog oder gar eine Checkliste überführt werden kann.¹⁶ Jedoch kann er eine Hilfestellung hierfür bieten. Weitere Unterstützung bei der Fragestellung der rechtskonformen Umsetzung von Verarbeitungsvorgängen mit Beschäftigtenbezug finden sich u. a. auch in den öffentlichen Informationsangeboten der Landesdatenschutzbehörden. So bietet das Bayerische Landesamt für Datenschutzaufsicht ein Musterdokument zur Prüfung der DSGVO-Umsetzung bei KMU.¹⁷ Das Unabhängige Landeszentrum für Datenschutz Schleswig Holstein (ULD) gibt Hilfestellung bei der Durchführung der Datenschutzfolgenabschätzung, inklusive eines abstrakten Ablaufmodells einer Prüfung nach dem SDM.¹⁸ Für die Strukturierung des Kriterienkatalogs wurde entschieden, dem Aufbau der DSGVO zu folgen, da dieser der Systematik der Verordnung entspricht und Praktikern bereits bekannt ist.

Der Kriterienkatalog behandelt zunächst allgemeine Einstiegsfragen, bspw. die Anzahl der Beschäftigten und das Vorhandensein eines Datenschutzbeauftragten, eines Betriebsrats und von Betriebsvereinbarungen. Im weiteren Verlauf werden die Verarbeitungstätigkeiten fokussiert, die in der Regel einer Schwellwertanalyse zu unterziehen bzw. mit den Positiv- bzw. Negativlisten der Aufsichtsbehörden¹⁹ abzugleichen sind, um die Notwendigkeit einer Datenschutzfolgenabschätzung (DSFA) beurteilen zu können. Von höchster Bedeutung ist auch das Vorliegen einer passenden Rechtsgrundlage bzgl. der Verarbeitungsvorgänge.²⁰ Im Weiteren geht es um die (allgemeinen) Anforderungen der DSGVO. Dies umfasst vor allem die Grundsätze der Verarbeitung (Art. 5 DSGVO), die Umsetzung der Betroffenenrech-

15 Vgl. AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.): Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, 99, Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 17. April 2020.

16 Vgl. *Bieker/Hansen/Friedewald*, Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2016, S. 188-197.

17 Vgl. Bayerisches Landesamt für Datenschutzaufsicht, Prüfung DSGVO-Umsetzung bei kleinen und mittleren Unternehmen, 2018, https://www.lida.bayern.de/media/pruefungen/201811_kmu_fragebogen.pdf (letzter Abruf 21.10.2020).

18 *Gonschowski/Herber/Robrahn/Rost/Weichelt*, Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive“-Verfahrens, 2017, S. 3, <https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf> (letzter Abruf 21.10.2020); vgl. auch *Bieker/Hansen/Friedewald*, a. a. O.

19 Vgl. Art. 35 Abs. 4 und 5 DSGVO.

20 Vgl. hierzu Art. 6 DSGVO i. V. m. § 26 BDSG.

te (Art. 12-23 DSGVO), den passenden Einsatz von technischen und organisatorischen Maßnahmen (Art. 25 Abs. 1 i. V. m. Art. 32 DSGVO) sowie den Umgang mit Datenschutzverletzungen und der Kooperation mit den zuständigen Aufsichtsbehörden.

Die genannten Kriterien sollen die wesentlichen rechtlichen und grundsätzlich verbindlichen Anforderungen im Kontext des Beschäftigtendatenschutzes widerspiegeln. Um die Anforderungen unterschiedlicher Organisationen zu berücksichtigen, wird etwa nach Betriebsgrößenklassen differenziert. An dieser Stelle sollen jedoch auch die Limitierungen des Kriterienkatalogs bzw. des Selbstbewertungsinstruments explizit genannt werden: Ein Kriterienkatalog kann nicht den Anspruch auf Vollständigkeit haben oder gar eine weitere und tiefere Rechtsberatung ersetzen. Ziel ist es, ein Verständnis für die Anforderungen der DSGVO und des BDSG zu schaffen sowie Unternehmen dabei zu helfen, den Zustand hinsichtlich der eigenen Rechtskonformität und Prüffähigkeit einschätzen zu können.

3.2 Arbeitswissenschaftliche Perspektive

Aus arbeitswissenschaftlicher Perspektive sind weitere Faktoren zu betrachten, um sich ein realistisches Bild von den Datenschutz-, Selbstbestimmungs- und Transparenzbedarfen der Beschäftigten im Unternehmen zu machen. Sie erscheinen zwar – verglichen mit den rechtlichen Anforderungen – auf den ersten Blick möglicherweise verzichtbar, für die praktische Umsetzung des Beschäftigtendatenschutzes im Kontext einer digitalisierten Arbeitswelt sind sie jedoch von ebenso hoher Relevanz. Insbesondere, wenn eine effektive und produktive Nutzung von in den Geschäftsprozessen verarbeiteter Daten zur Prozessoptimierung vorgesehen ist. In diesem Kontext geht es nicht zuletzt um einen fairen Ausgleich der Interessen des Arbeitgebers wie auch der Beschäftigten bei der Nutzung von Beschäftigtendaten in einer Unternehmenskultur des Vertrauens. In diesem Zusammenhang ist die Einbindung des Betriebsrates respektive der Mitarbeiter-/Personalvertretung, ggf. auch über die rechtlichen Erfordernisse hinaus, bereits im Vorfeld einer Technologieeinführung, spätestens jedoch bei der Anforderungserhebung, ein relevanter Aspekt. Denn im Gegensatz zu den rechtlichen Anforderungen zum Beschäftigtendatenschutz, welche grundsätzlich für alle Menschen in einem vergleichbaren Beschäftigungsverhältnis gelten, können die Datenschutz-, Selbstbestimmungs- und Transparenzbedarfe unter den Beschäftigten individuell variieren und ggf. zu einer ablehnenden Haltung gegenüber den Technologieeinsatz und negativen Auswirkungen für das Unternehmen führen. In der Praxis sind sie vielfach abhängig von:

- ◆ bestehenden mentalen Modellen, basierend auf dem Wissen und Vermutungen der Beschäftigten über die Verarbeitung ihrer personenbezogenen Daten,
- ◆ der persönlichen Sensibilität bezüglich Datenschutz,
- ◆ eigenen Erfahrungen mit digitaler Technologie sowie
- ◆ den Kompetenzen und Qualifikationen im Umgang damit.

Um dem entgegenzuwirken, gilt es zu prüfen, ob bzw. inwiefern die Beschäftigten im Unternehmen dem Thema Datenschutz gegenüberstehen und ggf. bereits über eigene Erfahrungen verfügen. Ebenso wichtig ist es, sich einen Überblick bezüglich der Sensibilisierung, der individuellen Einstellung und Kompetenzen der Beschäftigten in Zusammenhang mit dem Thema Datenschutz im Unternehmen zu verschaffen. Denn nur wenn die Mitarbeiter ausreichend für das Thema Datenschutz sensibilisiert sind,

werden sie die Datenschutzregelungen konsequent einhalten und nicht in ggf. einfacheren, bestehenden Mustern fortfahren.

Darüber hinaus ist es für eine optimale Umsetzung des Beschäftigtendatenschutzes im Unternehmen aus arbeitswissenschaftlicher Perspektive relevant, inwiefern die Arbeitnehmer verständlich darüber informiert sind, welche personenbezogenen Daten von wem und zu welchem Zweck verarbeitet bzw. geteilt werden. Auch Informationen darüber, wie bei Datenschutzvorfällen agiert werden muss, gilt als ein relevantes Kriterium für die Umsetzung des Beschäftigtendatenschutzes. Denn grundsätzlich sind Arbeitnehmer nur dann in der Lage fundierte Entscheidungen bezüglich der eigenen Privatsphäre bzw. der Weiterverarbeitung der personenbezogenen Daten am Arbeitsplatz zu treffen – also bspw. ob bestimmte Daten nur anonymisiert verwendet werden sollen oder nicht – wenn sie über eine adäquate Informationsgrundlage verfügen.²¹

Außerdem ist zu beachten, welche Kommunikationswege und Medien geeignet sind, um ggf. heterogenen Beschäftigtengruppen diese Informationen zur Verfügung zu stellen und für welche Beschäftigtengruppen Schulungen oder andere zusätzlichen Hilfestellungen erforderlich sind. Im Optimalfall findet eine bewusste Auseinandersetzung mit den Möglichkeiten und Grenzen der Verarbeitung von Beschäftigtendaten vor dem Hintergrund der Abwägung legitimer Interessen des Unternehmens (Steuerung, Kontrolle) und der Erhaltung bzw. Förderung vertrauensvoller und fairer Arbeitsbeziehungen durch die Berücksichtigung der Interessen, Wünsche und Erwartungshaltungen der Beschäftigten statt.²² Nachteilige Auswirkungen, die aus dem Wissen der Beschäftigten um die Erfassung ihrer personenbezogenen Daten entstehen können, sollten durch eine bewusste Gestaltung und Implementierung der Monitoringsysteme abgefedert werden. Beispielsweise kann dies durch die Vermeidung von Einzelüberwachung, eine partizipative Einführung unter Beteiligung der Beschäftigten sowie durch eine sinnvolle Begründung umgesetzt werden.²³

Negative Effekte oder eine mangelnde Akzeptanz der Technologie lassen sich vermeiden, wenn der Aspekt der Überwachung ex ante berücksichtigt und die Technologie entsprechend gestaltet wird. Akzeptanzförderlich sind Transparenz, Nachvollziehbarkeit und Vorhersagbarkeit des Systems, die Gestaltung des Feedbacks sowie die Einbeziehung der betroffenen Beschäftigten bereits im Vorfeld der Einführung.²⁴ Vor diesem Hintergrund lag eine besondere Herausforderungen bei der Entwicklung des Instruments darin, sich mit dem zu erarbeitenden Kriterienkatalog auch diesen komplexen Fragestellungen zu nähern und sie im Rahmen eines praktikablen Werkzeuges zugänglich zu machen.

21 Vgl. Bosse/Dietrich/Kelbert/Küchler/Schmitt/Tolsdorf/Weßner, Beschäftigtendatenschutz, Rechtliche Anforderungen und technische Lösungskonzepte, in: Schweighofer/Hötendorfer/Kummer/Saarenpää (Hrsg.), Verantwortungsbewusste Digitalisierung, Tagungsband des 23. Internationalen Rechtsinformatik Symposiums, IRIS 2020, Bern 2020, S. 175-182.

22 Vgl. Mohammad, IT Surveillance and Social Implications in the Workplace. In: Proceedings of the 2015 SIGMIS Conference on Computers and People Research. Newport Beach, USA 2015, 4.-6. Juni 2015, ACM, S. 79-85.

23 Vgl. Backhaus, Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz, Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte, Z. für Arbeitswissenschaft 2019, S. 2-22.

24 Vgl. ebd.

4 Umsetzung und Erprobung

Ausgangspunkt für die Umsetzung des Selbstbewertungsinstrumentes ist die Erfüllung zentraler Anforderungen, die im Austausch mit potenziellen Anwendern zusammengetragen wurden. Hierzu zählen unter anderem:

- ◆ Das Selbstbewertungsinstrument muss für den Anwender leicht handhabbar und im Umgang selbsterklärend sein.
- ◆ Der Zugang muss kostenfrei und niedrigschwellig gehalten sein, sodass man sich nicht vorab erst registrieren oder mit persönlichen Daten anmelden muss.
- ◆ Das Selbstbewertungsinstrument muss derart umgesetzt sein, dass die bestehenden rechtlichen Regelungen des Datenschutzes eingehalten werden.
- ◆ Die Erhebung der für die Bewertung relevanten Faktoren muss übersichtlich strukturiert und nicht zu überladen gestaltet sein. Die Anzahl der Fragen sollte überschaubar sein.
- ◆ Die Zeitspanne, die für das Ausfüllen der Fragen bis zur Präsentation des Ergebnisprofils in Anspruch genommen wird, darf nicht länger als 15-20 Minuten sein.
- ◆ Für Anwender sollte es eine Möglichkeit geben, sich mit Hilfe von Checklisten und weiterführenden Informationen intensiver mit der Thematik zu beschäftigen.
- ◆ Neben einer Bewertung des Ist-Standes liegt ein Mehrwert in den sich daran anknüpfenden Empfehlungen zur Weiterentwicklung des betrieblichen Datenschutzes.

Um einen größtmöglichen Nutzen für Anwender zu erreichen, wurden bei der Umsetzung die benannten Anforderungen berücksichtigt. Das Selbstbewertungsinstrument ist als Online-Befragung mit der Open-Source-Software LimeSurvey umgesetzt, die unter Einhaltung datenschutzrelevanter Vorgaben auf eigenen Servern in Deutschland betrieben wird. Diese Art der Umsetzung bietet den Vorteil, dass der Umgang mit Online-Fragebögen keine speziellen Kenntnisse voraussetzt. Gleichzeitig ist der Zugang ohne technische Hürden oder Anmeldeverfahren möglich, sodass das Selbstbewertungsinstrument frei verfügbar ist. Um mögliche Lücken und logische Brüche des Instruments frühzeitig zu identifizieren, ist zunächst eine intensive Test- und Evaluierungsphase geplant.²⁵

Die Online-Befragung ist in Themenbereiche strukturiert, um sie übersichtlicher zu gestalten. Darüber hinaus wird die Anzahl der zu beantwortenden Fragen durch den Einsatz von Filterfragen optimiert, sodass gegebenenfalls im Unternehmenskontext irrelevante Fragen nicht angezeigt werden. Auf diese Weise wird das Verhältnis von Aufwand zu Nutzen bei Einsatz des Selbst-

bewertungsinstruments unternehmensspezifisch optimiert. Im Mittel wird eine Bearbeitungsdauer angestrebt, die 20 Minuten nicht überschreitet.

Das Selbstbewertungsinstrument bietet die Möglichkeit, den Ist-Zustand des Beschäftigtendatenschutzes zu erheben. Diese Einschätzungen zur Rechtskonformität erfolgen anhand der Antworten bzgl. der bisher umgesetzten Maßnahmen im Unternehmen. Jeder Teilnehmer erhält unmittelbar die Auswertung seiner individuellen Ergebnisse und daran anknüpfende Handlungsempfehlungen zur Weiterentwicklung des Beschäftigtendatenschutzes. Zudem stehen Checklisten und vertiefende Informationsmaterialien bereit, mit deren Hilfe die rechtskonforme Umsetzung insbesondere in Unternehmen mit einem niedrigen Reifegrad unterstützt werden kann. Die Ergebnisse insgesamt können von den Teilnehmenden ausgedruckt oder als PDF-Dokument gespeichert werden.

5 Zusammenfassung und Fazit

Ein Selbstbewertungsinstrument für den betrieblichen Datenschutz kann ein nützliches Werkzeug sein, um die Rechtskonformität des eigenen Betriebs festzustellen. Die Limitierungen müssen dem Anwender jedoch ebenso bewusst sein. So kann die Anwendung eines Selbstbewertungsinstrumentes selbstverständlich keine vollständige Rechtsberatung ersetzen. Ziel ist es jedoch, eine Sensibilität für die allgemeinen Anforderungen des Beschäftigtendatenschutz zu schaffen und auf Optimierungspotenziale im eigenen Betrieb hinzuweisen.

Das Vorgehen bei der Erstellung eines solchen Werkzeugs basiert auf der Erfassung und Modellierung der Anforderungen in einem Kriterienkatalog, welcher schließlich in einen Fragekatalog überführt wird. Die Anforderungen lassen sich direkt aus DSGVO und BDSG ableiten. Ergänzend helfen die Informationen und Hilfen der Datenschutzaufsichtsbehörden, insbesondere das Standard-Datenschutzmodell, und der juristischen Literatur. Um mögliche Widerstände bei der Umsetzung der Rechtskonformität zu berücksichtigen und vorzubeugen, ist die arbeitswissenschaftliche Perspektive von hoher Relevanz. Der Versuch, Änderungen in einem Betrieb einzuführen, kann in der Praxis häufig an der mangelnden Einbindung und Berücksichtigung der Interessen der Beschäftigten scheitern.

Schließlich sind bei der erfolgreichen Umsetzung eines Selbstbewertungsinstrument ebenso die Anforderungen potenzieller Nutzer zu beachten. Zum Beispiel sollten die Fragen gut und logisch strukturiert und das Werkzeug im Umgang nahezu selbsterklärend sein. Zudem sollte das Instrument nicht zu überladen und die Bearbeitung in einer angemessenen Zeitspanne möglich sein.

²⁵ Weiterführende Informationen sowie ein Zugang zum Selbstbewertungsinstrument sind auf der Projektwebseite unter folgender URL verfügbar: <https://www.trusd-projekt.de> (letzter Abruf 21.10.2020).