Methodenbericht

BeDaX

Inhalt

1. Einführung 2

1.1 Ausgangssituation und Zielsetzung 2

1.2 Praktische Anwendung des BeDaX 3

1.3 Vorgehen bei der Entwicklung des BeDaX 3

2. Formativer Rahmen 5

3. Aufbau des BeDaX 7

3.1 Qualitätsmaßstäbe und Faktoren 8

3.2 Die Elemente des BeDaX im Überblick 12

4. Bewertungsmodell 12

4.1 Grundprinzip der Wertezuweisung 13

4.2 Besonderheiten der Wertezuweisung 14

4.3 Gewichtungen 16

5. Ergebnisdarstellung 16

© INPUT Consulting gGmbH, Theodor-Heuss-Str. 2, 70174 Stuttgart, 9/2023

Autoren: Ines Roth, Karl-Heinz Brandl

Der Methodenbericht einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der INPUT Consulting gGmbH unzulässig und strafbar.

Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Speicherung und Verarbeitung in elektronischen Systemen.

www.input-consulting.de

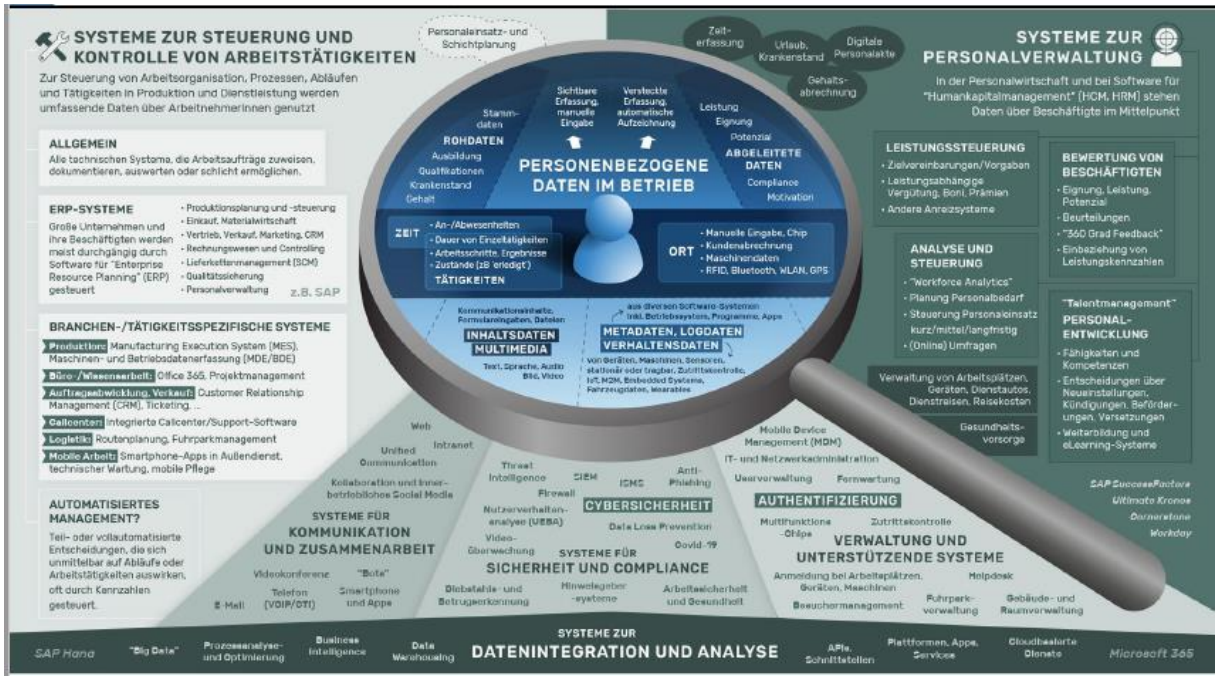
INPUT consulting

1. Einführung

1.1 Ausgangssituation und Zielsetzung

Vor dem Hintergrund des digitalen Umbruchs sind der Datenschutz und die konkrete Umsetzung von Schutzvorschriften wie der Datenschutz-Grundverordnung der EU oder des Bundesdatenschutzgesetzes zentrale Handlungsfelder in Betrieben und Verwaltungen. Denn Aktivitäten in digitalen Arbeitsumgebungen und sozialen Netzwerken hinterlassen immer größere „Datenschatten" der Beschäftigten, die durch den Einsatz entsprechender Analyseinstrumente zur Durchleuchtung, Leistungskontrolle und Verhaltenssteuerung genutzt werden können.

Die Studie von Christl (2021) zeigt, dass die Bandbreite der für den Beschäftigtendatenschutz relevanten IT-Anwendungen und -Systeme enorm groß ist. Die Autoren untergliedern sie in Systeme zur Steuerung und Kontrolle von Arbeitstätigkeiten, zur Personalverwaltung, für Kommunikation und Zusammenarbeit, für Sicherheit und Compliance und in Verwaltung und unterstützende Systeme. Die folgende Abbildung zeigt die Systematisierung der Studie mit Erläuterungen und Beispielen:



Quelle: Christl (2021) https://crackedlabs.org/dl/CrackedLabs_Christl_UeberwachungKontrolleArbeitsplatz.pdf zuletzt geprüft am 12.4.2022

Betriebliche Interessenvertretungen sind angesichts der wachsenden Vielzahl eingesetzter IT-Systeme zunehmend mit Mitbestimmungsthemen rund um den Beschäftigtendatenschutz konfrontiert. Die Vielschichtigkeit und die Menge der in Betrieben und Verwaltungen eingesetzten Instrumente, ebenso wie die teils sehr komplexen gesetzlichen Datenschutzvorgaben stellen nicht nur Betriebs- und Personalräte vor große Herausforderungen.

Entstehung des Index Beschäftigtendatenschutz (BeDaX)

Vor dem Hintergrund dieser Entwicklungen wird ein Index für den Beschäftigtendatenschutz im Weißbuch Arbeiten 4.0 des Bundesministeriums für Arbeit und Soziales als wichtiges Instrument verstanden, um Arbeitgeber, Betriebsräte und kleine und mittlere Unternehmen (KMU) hinsichtlich der

Umsetzung von gesetzlichen Datenschutzvorgaben in einer digitalisierten Arbeitswelt zu unterstützten. Mit dem Projekt Index Beschäftigtendatenschutz (kurz: BeDaX) wird dieser von ver.di eingebrachte Vorschlag aus dem Weißbuch Arbeit 4.0 von INPUT Consulting in Zusammenarbeit mit ver.di aufgegriffen.

Das Projekt wird von einem Beirat fachlich begleitet. Mitglieder des Beirats sind Prof. Dr. Jürgen Taeger, Universitätsprofessor i. R. für Bürgerliches Recht, Handels- und Wirtschafts- sowie Rechtsinformatik an der Carl von Ossietzky Universität Oldenburg, Mitglied des Datenschutz-Beirats DB-Konzern, und Lothar Schröder, Vorsitzender des Datenschutzbeirates der Deutschen Telekom und ehemaliges Mitglied in den Enquete-Kommissionen „Internet und digitale Gesellschaft“ und „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“.

Ziel des Index Beschäftigtendatenschutz

Das Ziel des Projekts BeDaX orientiert sich an den Anforderungen, wie sie im Weißbuch Arbeiten 4.0 formuliert sind, nämlich wissenschaftlich fundierte, anwendungsbezogene Qualitätsmaßstäbe für den Beschäftigtendatenschutz zu entwickeln, die – im Sinne eines wissenschaftlichen Tools für die Selbstbewertung oder auch im Rahmen einer Zertifizierung – den Beschäftigtendatenschutz in Betrieben vergleichbarer und handhabbarer machen (BMAS: Weißbuch Arbeiten 4.0, 2017, S. 150). Mit dem Index Beschäftigtendatenschutz (BeDaX) kann das im Betrieb, in Verwaltungen und an Arbeitsplätzen jeweils erreichte Schutzniveau bei der Verarbeitung von Beschäftigtendaten gemessen werden. Er zeigt zudem Stärken und Schwächen hinsichtlich des betrieblichen Beschäftigtendatenschutzes auf. Grundlage des Indexes ist der in Kapitel 2 vorgestellte formative Rahmen.

1.2 Praktische Anwendung des BeDaX

Der Index Beschäftigtendatenschutz wird nicht für die Berichterstattung gebildet, sondern dient ausschließlich der eigenen Überprüfung des jeweiligen betrieblichen Beschäftigtendatenschutzniveaus. Ein Vergleich mit anderen Unternehmen oder eine akkumulierte Auswertung mehrerer Bögen findet nicht statt. Der BeDaX ist als Screeninginstrument zu verstehen, das aufbauend auf den Ergebnissen des Checks Hinweise darauf gibt, in welchen Bereichen nachgebessert werden sollte. Dabei berücksichtigt der BeDaX nicht nur rechtliche Anforderungen des Beschäftigtendatenschutzes, sondern auch ethische Aspekte.

Seine Nutzung setzt keine detaillierte Expertise in Datenschutzfragen voraus. Der Fragebogen beinhaltet umfassende Erläuterungen zu allen relevanten Aspekten, so dass er auch zu Schulungs- und Weiterbildungszwecken genutzt werden kann. Gleichzeitig ist davon auszugehen, dass nicht alle Fragen auf Anhieb beantwortet werden können, weil den betrieblichen Interessenvertretungen möglicherweise die notwendigen Informationen fehlen. Eine Zusammenarbeit mit den jeweils für den Beschäftigtendatenschutz verantwortlichen betrieblichen Akteuren wie dem/der Datenschutzbeauftragten wird daher in den meisten Fällen notwendig sein.

Der BeDaX richtet sich an Personal- und Betriebsräte ebenso wie an Mitarbeitervertretungen. Das zur Nutzung notwendige Kennwort des Onlinetools kann über die Projekthomepage (www.bedax.net) bei unserem Projektleiter Karl-Heinz (Charly) Brandl angefordert werden.

1.3 Vorgehen bei der Entwicklung des BeDaX

Für die Entwicklung des BeDaX wurden zunächst grundlegende Anforderungskataloge und Qualitätsmaßstäbe für die Ziele und Verfahren des Beschäftigtendatenschutzes ermittelt. Grundlage waren die für den Beschäftigtendatenschutz wesentlichen technischen, rechtlichen, ethischen, arbeits- und

sozialwissenschaftlichen Aspekte, die sich aus gesetzlichen Vorgaben und der einschlägigen Literatur (siehe Kapitel 2 Formativer Rahmen) ergeben.

Der erste Entwurf des BeDaX-Modells wurde auf der Grundlage umfangreicher Literaturrecherchen und Diskussionen im BeDaX-Beirat erarbeitet. Nachdem das Grundmodell mit acht Qualitätsmaßstäben und den entsprechenden Faktoren erstellt und inhaltlich begründet vorlag, erfolgte die Entwicklung der jeweils zugeordneten Fragen, die im Laufe des Prozesses angepasst und reduziert wurden. Das BeDaX-Modell besteht nun aus 84 Erhebungsfragen, 42 Faktoren und 8 Qualitätsmaßstäben (siehe Kapitel 3 Aufbau des BeDaX).

Da die Fragen, Faktoren und Qualitätsmaßstäbe zwar allesamt wesentlich, aber nicht gleichbedeutend für die Analyse des Datenschutzniveaus in den Betrieben und Verwaltungen sind, wurden sie im weiteren Prozess unterschiedlich gewichtet. Die Gewichtung ist inhaltlich begründet und basiert auf der Praxiserfahrung der BeDaX-Beiratsmitglieder sowie der Auswertung der Tätigkeitsberichte der Aufsichtsbehörden, aktuellen Gerichtsurteilen und entsprechender Literaturauswertungen (siehe Kapitel 4.1 Grundprinzip der Wertezuweisung).

Zur Verifizierung des Instruments wurden im Zeitraum zwischen dem 22. März und dem 24. Mai 2022 insgesamt sieben Interviews mit Datenschutzexperten bzw. Datenschutzexpertinnen zur Auswahl der Qualitätsmaßstäbe, Faktoren und Fragen, zur Verständlichkeit der Fragen sowie der Gewichtung der Qualitätsmaßstäbe durchgeführt. Die Interviews fanden per Videokonferenz statt, wurden anonym verschriftlicht und ausgewertet.

Als Expertin und Experten standen folgende Sachverständige zur Verfügung: ein ehemaliger Leiter einer Aufsichtsbehörde und aktueller Datenschutzexperte, eine ver.di Bereichsleiterin mit Datenschutzbezug, ein ver.di Gewerkschaftssekretär (ausgebildeter Datenschutzberater), ein DGB-Abteilungsleiter mit Bezug zum Beschäftigtendatenschutz, ein Betriebsrat (IT-Ausschussvorsitzender) sowie ein Datenschutzbeauftragter eines großen IT-Unternehmens.

Im Vorfeld der Interviews wurden das BeDaX-Modell, die konkreten Fragen sowie die Gewichtung der Qualitätsmaßstäbe zugesandt, verbunden mit den folgenden Fragestellungen:

1. **BeDaX - Modell**
   Das BeDaX-Modell definiert 8 Qualitätsmaßstäbe, die in Faktoren und konkrete Fragen unterteilt sind.
   a. Ist das BeDaX-Modell für Sie/Dich nachvollziehbar?
   b. Passt der Aufbau des BeDaX-Modells – ist er logisch nachvollziehbar?
   c. Fehlen (wesentliche) Bestandteile (weitere Qualitätsmaßstäbe oder Faktoren) zur Beurteilung des Beschäftigtendatenschutzes? Wenn ja, welche?

2. **Fragen – BeDaX – Interessenvertretungen**
   Der erstellte Fragenkatalog richtet sich konkret an die gesetzlichen Interessenvertretungen.
   a. Sind die Fragen vollständig? Wenn nein, welche sollten ergänzt werden?
   b. Sind Fragen zu streichen? Wenn ja, welche sollten gestrichen werden.
   c. Sind die Fragen für die Zielgruppe verständlich?

3. **Gewichtung Qualitätsmaßstab**
   Die Qualitätsmaßstäbe werden zur Auswertung zueinander gewichtet. Die Gewichtung wird inhaltlich begründet (z.B. Rechtskonformität und Transparenz als wichtige Vorgaben aus der DSGVO/BDSG zusammen stellen 50 % Gewichtung dar, so unser Vorschlag).
   a. Erstellen Sie/Erstelle bitte eine Gewichtung der Qualitätsmaßstäbe. Im Auswertungsgespräch würden wir gerne auch nach Ihrer/deiner inhaltlichen Begründung fragen.

In den Interviews begrüßten alle Expertinnen und Experten das Projekt BeDaX mit den bisher vorliegenden Dokumenten, vor allem die erste Fokussierung auf die Interessenvertretungen. Insbesondere die Tatsache, dass hier kein kommerzielles Produkt entstehen soll, sondern ein kostenfreies Angebot für Mitglieder von Betriebs- und Personalräten, wurde begrüßt. Neben der allgemeinen Zustimmung brachten die Interviewten einige konkrete Vorschläge bezüglich der Indikatoren und der Fragestellungen sowie der Gewichtung ein. Diese wurden im BeDaX-Beirat bewertet und entsprechend eingearbeitet.

(Das ausführliche Dokument „Auswertung Experteninterview" kann beim Projetleiter BeDaX angefordert werden.)

Nach ausführlichen internen Tests wurde der Fragebogen für den Beta-Test online zugänglich gemacht. Insgesamt 19 Beta-Testerinnen und -Tester haben das Selbstbewertungstool BeDaX in der Zeit von 6.3. bis 1.6.2023 anonym getestet. Die Testpersonen waren Betriebsräte bzw. Betriebsrätinnen, Gewerkschaftssekretäre sowie Datenschutz-Experten. Von 10 Testpersonen gab es konkrete schriftliche Rückmeldungen. 6 Testpersonen waren zu ausführlichen Feedback-Gespräche bereit. Von 3 Testpersonen gab es keine Rückmeldung. Inhaltliche Anregungen sowie Hinweise zum Layout und zur Ergebnisdarstellung wurden entsprechend berücksichtigt.

(Das ausführliche Dokument „Beta-Test BeDaX-Tool" kann beim Projetleiter BeDaX angefordert werden.)

2. Formativer Rahmen

Der formative Rahmen des BeDaX-Fragebogens beschreibt die Grundlage, auf der die Qualitätsmaßstäbe und Faktoren entwickelt wurden.

Eine wichtige Quelle ist der Abschlussbericht der **Enquete-Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale"** des Bundestags (2017-2021). Der Bericht beinhaltet *unter anderem Themen wie den Umgang mit Datenbias und Risiko* im Zusammenhang mit Künstlicher Intelligenz (KI) und Datenschutzfragen und damit verbundene Handlungsempfehlungen. Einige den Handlungsempfehlungen zugrundeliegende ethische Prinzipien wie Autonomie, Vertrauen, Transparenz, Gerechtigkeit und Diskriminierungsfreiheit waren für das BeDaX-Tool besonders relevant.

Quelle:

Schröder, Lothar/Röspel, René (2020): Künstliche Intelligenz (KI). Textauszüge aus dem Bericht der Enquete-Kommission. Eine Lesefassung relevanter Themen aus gewerkschaftlicher Sicht. https://www.input-consulting.de/publikationen/publikation/kuenstliche-intelligenz-ki-textauszuege-aus-dem-bericht-der-enquete-kommission-eine-lesefassung-relevanter-themen-aus-gewerkschaftlicher-sicht.html (letzter Abruf: 8.09.2023)

Abschlussbericht der Enquete-Kommission Künstliche Intelligenz. https://dserver.bundestag.de/btd/19/237/1923700.pdf (letzter Abruf 8.9.2023)

Das **Standard-Datenschutzmodell** der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder beinhaltet unter anderem eine Systematisierung der Anforderungen der DSGVO durch die Gewährleistungsziele (Datenminimierung – Verfügbarkeit – Integrität – Vertraulichkeit – Nichtverkettung – Transparenz – Intervenierbarkeit), an der sich auch der BeDaX orientiert.

Quelle:

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2022): Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.0. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Themen/Standard-Datenschutzmodell.pdf?__blob=publicationFile&v=4 (letzter Abruf 8.9.2023)

Vor dem Hintergrund der zunehmenden Digitalisierung in Wirtschaft und Gesellschaft setzte die Bundesregierung am 18. Juli 2018 die **Datenethikkommission (DEK)** ein. Ihr Auftrag war es, „innerhalb eines Jahres ethische Maßstäbe und Leitlinien sowie konkrete Handlungsempfehlungen für den Schutz des Einzelnen, die Wahrung des gesellschaftlichen Zusammenlebens und die Sicherung und Förderung des Wohlstands im Informationszeitalter zu entwickeln." (DEK 2019, S. 13) Die allgemeinen ethischen und rechtlichen Grundsätze und Prinzipien (die Würde des Menschen – Selbstbestimmung – Privatheit – Sicherheit – Demokratie - Gerechtigkeit und Solidarität – Nachhaltigkeit) der DEK waren für das BeDaX-Tool entscheidend.

Quelle:

Gutachten der Datenethikkommisson (DEK) der Bundesregierung (2019). Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbH (bud): Berlin. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (letzter Abruf 08.09.2023)

Für die Entwicklung des BeDaX-Tools stellte der **Kommentar zur Datenschutzgrundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG) und dem TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz) von Jürgen Taeger und Detlev Gabel** eine weitere wichtige Grundlage dar. Insbesondere die DSGVO-Schutzziele im Hinblick auf die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten (gesetzliche oder vertragliche Erlaubnisnorm oder Einwilligung erforderlich) und die Verarbeitung nach Treu und Glauben (Integrität und Vertraulichkeit – Datenminimierung und Speicherbegrenzung – Aktualität und Richtigkeit der Daten – Rechenschaftspflicht) haben den BeDaX maßgeblich geprägt.

Quelle:

Taeger, Jürgen/Gabel, Detlev (Hrsg.) (2022): DSGVO – BDSG – TTDSG. Kommentar. Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, 4. Aufl., Frankfurt/M.

Eine wesentliche Basis des BeDaX stellt zudem **quid! Qualitätsmodell Arbeitsplätze**, das Gütesiegel für Qualität im betrieblichen Datenschutz dar. Es beinhaltet die Elemente Rechtskonformität, Kundenfreundlichkeit, Mitarbeiterfreundlichkeit, Anwenderfreundlichkeit, Transparenz, Qualifikation, Datensicherheit, Qualitätsmanagement, Mitarbeiterschulung / Information, Organisation / Rahmenbedingungen, die auch Berücksichtigung bei der Entwicklung des BeDaX fanden.

Quelle:

quid! – Das Gütesiegel für Qualität im betrieblichen Datenschutz
Wedde, Peter/Schröder, Lothar (2001); quid! Projektbüro, Frankfurt am Main.
Ein Kooperationsprojekt der Fachhochschule Frankfurt am Main gemeinsam mit Deutsche Postgewerkschaft e.V. (DPG in ver.di), ISBN 3-00-008417-7;

Bei der Entwicklung der BeDaX-Qualitätsmaßstäbe und Kriterien, die sich überwiegend auf den Datenschutz beziehen, stellte der **Kriterienkatalog Querschnittsprüfung der Landesbeauftragten für Datenschutz Niedersachsen** eine wesentliche Grundlage dar. Dies gilt insbesondere für folgende Elemente des Katalogs: Verzeichnis von Verarbeitungstätigkeiten – Zulässigkeit der Verarbeitung – Betroffenenrechte – Technischer Datenschutz – Datenschutz-Folgenabschätzung – Auftragsverarbeitung – Datenschutzbeauftragter – Meldepflichten – Dokumentation.

Quelle:

Die Landesbeauftragte für den Datenschutz Niedersachsen (2019): Kriterienkatalog zur Querschnittsprüfung in der Wirtschaft 2018/19. https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/kriterien-querschnittspruefung-179455.html (letzter Abruf 08.09.2023)

3. Aufbau des BeDaX

Der formative Rahmen des Index Beschäftigtendatenschutz basiert auf acht Qualitätsmaßstäben, die die wesentlichen Bereiche des Beschäftigtendatenschutzes umfassen. Allgemein werden Qualitätsmaßstäbe im Rahmen von Qualitätsmanagementsystemen eingesetzt, um die Prozess-, Arbeits-, Produkt- und Dienstleistungsqualität zu verbessern. Die bekanntesten Qualitätsmanagementmodelle sind das EFQM-Modell (European Foundation for Quality Management-Modell) sowie die ISO 9001. Beide Modelle sind ein Werkzeug, das Hilfestellung für den Aufbau und die kontinuierliche Weiterentwicklung eines umfassenden (Qualitäts-) Managementsystems gibt. Es soll helfen, eigene Stärken, Schwächen und Verbesserungspotenziale zu erkennen und die Unternehmensstrategie darauf auszurichten. Anhand von Qualitätsmodellen können somit **allgemeine Qualitätsbegriffe** operationalisiert, messbar und bewertbar gemacht werden. In der Regel wird hierfür eine Unterteilung der betrachteten Qualität in Merkmale oder **Faktoren** und **Indikatoren** vorgenommen (vgl. TrUSD-Qualitätsmodell, Version 2 vom 21.2.2020).

Die **Qualitätsmaßstäbe** des Index Beschäftigtendatenschutz werden in **Faktoren** unterteilt. Jeder Faktor wird mit **Indikatoren (Fragen)** weiter untergliedert. Diese Indikatoren dienen als Anzeiger für die untersuchten Sachverhalte und Eigenschaften. Alle Qualitätsmaßstäbe, Faktoren und Indikatoren beziehen sich auf Fragen des Datenschutzes im Beschäftigungsverhältnis. Damit ermöglicht der BeDaX die **Überprüfung des Schutzniveaus für den Beschäftigtendatenschutz** und zeigt konkrete

Schutzlücken auf. Aus dem Ergebnis des Indexes können Empfehlungen für eine praxistaugliche, angemessene sowie rechtskonforme Lösung abgeleitet werden.

3.1 Qualitätsmaßstäbe und Faktoren

Die Qualitätsmaßstäbe des Index Beschäftigtendatenschutz gründen sich im Wesentlichen auf die Charta der Grundrechte der Europäischen Union (Grundrechtecharta, GrCh) und hier im Speziellen auf das Grundrecht auf Unantastbarkeit der Würde des Menschen (Art. 1 GrCh), dem Recht auf Nichtdiskriminierung (Art. 21 GrCh), dem Recht auf gesunde, sichere und würdige Arbeitsbedingungen (Art. 31 Abs. 1 GrCh), dem Recht auf Achtung des Privat- und Familienlebens (Art. 7) sowie dem Recht auf Schutz der personenbezogenen Daten (Art. 8 GrCH). Das Grundrecht auf Schutz der personenbezogenen Daten aus Art. 8 GrCH folgt dem in Deutschland vom Bundesverfassungsgericht aus dem Grundrecht auf Schutz der Persönlichkeit (Art. 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 Grundgesetz) abgeleiteten Recht auf informationelle Selbstbestimmung. Hieraus ergeben sich für den Index Beschäftigtendatenschutz folgende acht Qualitätsmaßstäbe:

- Ethik
- Rechtskonformität
- Verantwortung
- Transparenz
- Kontrollfähigkeit
- Qualitätssicherung
- Risikoangemessenheit
- Kompetenz

Die Qualitätsmaßstäbe werden im Folgenden kurz erläutert.

Ethik

Der Qualitätsmaßstab Ethik prüft den Schutz und die Fairness im Umgang mit den Beschäftigten, der Respektierung der Würde des Menschen am Arbeitsplatz, die Gleichbehandlung sowie die Teilhabe von Beschäftigten im Zusammenhang der Verarbeitung personenbezogener Daten der Beschäftigten im Betrieb bzw. in der Behörde.
Neben der Grundrechte-Charta der EU verpflichtet auf der nationalen einfachgesetzlichen Ebene auch § 75 Abs. 2 Satz 1 BetrVG den Arbeitgeber und den Betriebsrat, „die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern.“.

Rechtskonformität

Der Qualitätsmaßstab Rechtskonformität prüft die Zulässigkeit der Verarbeitung personenbezogener Beschäftigtendaten, insbesondere die Beachtung der Grundprinzipien (Art. 5 DSGVO), das Vorliegen eines Erlaubnistatbestands, die Erforderlichkeit und die Zweckbindung. Beleuchtet werden der Drittlandstransfer, die Regelungen zur Auftragsverarbeitung sowie eine vorausschauende Unternehmenspolitik beim Umgang mit Beschäftigtendaten durch Datenschutz by Design (bei der Entwicklung) und by Default (datenschutzfreundliche Voreinstellungen) gemäß Art. 25 DSGVO.

Weitere Faktoren bilden die Themen wie die automatisierte Entscheidungsfindung, die Datenschutzfolgenabschätzung sowie das Gebot der Datensparsamkeit. Komplettiert wird der Qualitätsmaßstab

‚Rechtskonformität' mit einem Themenkomplex zum Datenschutzbeauftragten sowie den Betroffenenrechte und den Meldepflichten.

Abgeleitet sind diese Qualitätsmaßstäbe aus den Vorschriften der Europäischen Datenschutz-Grundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG). Bei Einhaltung dieses Qualitätsmaßstabs können straf- oder bußgeldbewehrte Regelverstöße, Personen- oder Vermögensschäden sowie erhebliche Reputationsrisiken verhindert werden.

Die Kontrolle der Rechtskonformität der Datenverarbeitung stellt eine wesentliche Aufgabe für Betriebs- und Personalräte dar, die darauf zu achten haben, dass …"die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen…" eingehalten werden (§ 80 Abs. 1 Ziffer 1 BetrVG sowie § 68 Abs.1 Ziffer 2 BPersVG). Dieser Qualitätsmaßstab stellt für die Beschäftigten die Basis für eine Überprüfung der Einhaltung der datenschutzrechtlichen Anforderungen dar.

Verantwortung

Im Qualitätsmaßstab Verantwortung werden die richtige Zuordnung sowie die Einhaltung der Transparenz der Verantwortung überprüft. Strategie, Kultur und Organisation beim Datenschutz werden in dem Faktor Datenschutzmanagementsystem sowie Gemeinsame Verantwortungen hinterfragt und Ressourcen bei der Datenschutzorganisation überprüft.

Verantwortliche sind gemäß Artikel 4 Ziffer 7 DSGVO „die … über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden", also die Entscheidungsträger in Behörden, Einrichtungen, Unternehmen (in Unternehmen somit die Geschäftsleitung). Wesentliche Aufgaben des Verantwortlichen ergeben sich aus den Art. 5 (Grundsätze für die Verarbeitung personenbezogener Daten) und Art. 24 DSGVO (Verantwortung des für die Verarbeitung Verantwortlichen).

Transparenz

Durch den Qualitätsmaßstab Transparenz werden die konkreten betrieblichen Datenschutzleitlinien, deren Verständlichkeit und Bekanntheit hinterfragt. Ein wesentlicher Bestandteil sind das Verzeichnis von Verarbeitungstätigkeiten, Verständlichkeit sowie die Meldungen bei Schutzverletzungen.

Art. 5 Abs. 2 DSGVO (Prinzip der Rechenschaftspflicht) verpflichtet den Verantwortlichen, die Einhaltung der Datenschutzgrundsätze nachweisen zu können. Das Betreiben eines Datenschutzmanagementsystems mit den betrieblichen Datenschutzleitlinien kann zur Erfüllung der Rechenschaftspflicht beitragen. Inwieweit die Datenschutzleitlinien bekannt sind und gelebt werden, stellt eine praxisrelevante Frage dar.

Das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO stellt – soweit eine Verpflichtung zur Aufstellung besteht – ein Kernstück einer Datenschutzorganisation dar und kann zweckmäßigerweise bei vielen Faktoren eine Rolle spielen: Festlegung der Verarbeitungszwecke, Rechenschafts- und Dokumentationspflicht, Erfüllung der Betroffenenrechte, geeignete technisch-organisatorische Maßnahmen, Prüfung einer Datenschutz-Folgenabschätzung. Es kann für seine Aufgabenerfüllung vom Datenschutzbeauftragten herangezogen werden.

Transparente Information und Kommunikation mit den Betroffenen fordern Art. 12 ff. DSGVO als Pflicht des Verantwortlichen.

Kontrollfähigkeit

Die Kontrollfähigkeit wird durch den Umgang mit den Informations- und Auskunftsrechten, der Berichtigung, dem Löschungsrecht und der Portabilität von Daten überprüft, der Revision (Überprüfung) des Schutzes der Privatsphäre, der Vertraulichkeit der Kommunikation sowie Regelungen zur Leistungs- oder Verhaltenskontrolle festgestellt. Des Weiteren werden die Überprüfung von Löschroutinen sowie der Prozess zu den Meldungen von Sicherheitsvorfällen (Schutzverletzungen, Art. 33 f. DSGVO) herangezogen. Die Steuerbarkeit von Prozessen und Systemen der personenbezogenen Datenverarbeitung stellt ein weiteres Prüfkriterium dar.

Informations- und Auskunftsrechte sind gesetzlich normierte Ansprüche (Art. 12 ff DSGVO), ebenso wie das Recht auf Berichtigung (Art. 16 DSGVO) und das Recht auf Löschung (Art. 17). Die Mitnahme von Personaldaten bei einem Arbeitgeberwechsel (Portabilität von Daten) ergibt sich aus Art. 20 DSGVO – Recht auf Datenübertragbarkeit.

Qualitätssicherung

Die Überprüfung der Qualitätssicherung bezieht sich auf die Datensicherheit und die entsprechende Dokumentation. Ein Überprüfungsschwerpunkt liegt auf der Beachtung der erforderlichen technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO

Die Vorgaben für die Sicherheit der Verarbeitung finden sich hauptsächlich in Art. 5 Abs. 1 lit. f DSGVO sowie in Art. 32 DSGVO. Zudem normieren weitere Bestimmungen wie z.B. Art. 24, 25, 36 DSGVO Anforderungen an die Datensicherheit. Darüber hinaus ist Datensicherheit Teil der Compliance in einem Unternehmen und wird üblicherweise durch Nutzung entsprechender Managementsysteme realisiert. Solche Systeme erleichtern die Qualitätssicherung, Vergleichbarkeit und Auditierbarkeit. Zu nennen sind hier die ISO/IEC 27701 (IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen), ISO 29100 (Informationstechnik – Sicherheitsverfahren – Rahmenwerk für Datenschutz) oder IDW PH 9.860.1 (Prüfungsstandard 980 des Instituts der Deutschen Wirtschaftsprüfer). Die Indikatoren für die technisch-organisatorischen Maßnahmen werden aus dem Standard-Datenschutzmodell (Version 2.0b) abgeleitet. Art. 25 DSGVO fordert Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Risikoangemessenheit

Die Risikoangemessenheit beurteilt das Risikomanagement anhand von Risikoanalysen und der Robustheit der Systeme.

Der Risikobegriff findet sich an zahlreichen Stellen in der DSGVO. So soll etwa bei der Auswahl der technischen und organisatorischen Maßnahmen die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden, Art. 32 DSGVO. Die DSGVO ordnet außerdem die Durchführung von bestimmten, besonderen Maßnahmen bei einem „voraussichtlich hohen Risiko“ für die persönlichen Rechte und Freiheiten natürlicher Personen an. Beispiele dafür sind die Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO, die Meldepflicht nach Art. 33 DSGVO und die Benachrichtigung des Betroffenen bei Datenschutzverletzungen gem. Art. 34 DSGVO.

Art. 32 Abs. 1 lit. b DSGVO verlangt bzgl. der Maßnahmen zur Sicherheit der Verarbeitung „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zu-

sammenhang mit der Verarbeitung auf Dauer sicherzustellen;“ Also IT-Systeme, die ausreichend widerstandsfähig sind, um auch trotz Störung und Fehlern funktionsfähig bleiben. Mit Blick auf die Verarbeitung personenbezogener Daten, Sicherheit garantiert werden kann. In diesem Sinne meint Belastbarkeit Robustheit der Systeme.

In der Praxis können Unternehmen bei der Risikobewertung unterstützend auf entsprechende DIN-Normen zurückgreifen: ISO/IEC 27005 (Management von Informationssicherheitsrisiken) sowie ISO 3100 (Risikomanagement).

Kompetenz

Abschließend können über den Qualitätsmaßstab Kompetenz der Stand der Qualifizierung zum Datenschutz der Beschäftigten, die Kompetenz des Datenschutzbeauftragten sowie die Praxisrelevanz der Vorgaben geprüft werden. Ein Aspekt dabei ist die Fähigkeit für die Betroffenen zu einem Selbstdatenschutz.

Aus Beschäftigtensicht sind Sensibilisierungs- und Schulungstätigkeiten von großer Bedeutung, die sich nicht nur allein auf die Informationspflicht aus der DSGVO ableiten. Denn nur mit Beschäftigten, die ausreichend für den richtigen Umgang mit personenbezogenen Daten sensibilisiert und geschult sind, können Datenschutzrisiken in Betrieben und in der Verwaltung reduziert werden. Eine wichtige Funktion hat dabei der Datenschutzbeauftragte. Die DSGVO stellt hohe Anforderungen an Datenschutzbeauftragte mit umfassenden Unterrichtungs-, Beratungs- und Kontrollaufgaben (Art. 39 DSGVO).

3.2 Die Elemente des BeDaX im Überblick

Die folgende Tabelle gibt einen Überblick über die Qualitätsmaßstäbe und den ihnen jeweils zugeordneten Faktoren. Die Faktoren werden über Fragen operationalisiert. Diese sogenannten „Indikatoren" fungieren als Anzeiger für die untersuchten Sachverhalte oder Eigenschaften. Sie sind Aspekte des jeweiligen Faktors und stellen die konkreten Fragestellungen dar.

Qualitätsmaßstäbe	Faktoren
Ethik	Schutz, Fairness, Würde, Gleichbehandlung, Teilhabe
Rechtskonformität	Zulässigkeit, insbesondere Erlaubnistatbestand, Erforderlichkeit und Zweckbindung, Drittlandstransfer, Auftragsdatenverarbeitung, Datenschutz by Design und by Default, Automatisierte Entscheidungen, Datenschutzfolgenabschätzung, Datensparsamkeit, Datenschutzbeauftragter, Betroffenenrechte, Meldepflichten
Verantwortung	Zuordnung funktionaler Verantwortung, Transparenz der Verantwortung, Datenschutzmanagementsystem, Gemeinsame Verantwortung, Ressourcen
Transparenz	DS-Leitlinien, Verständlichkeit, Verzeichnis von Verarbeitungstätigkeiten, Informationspflichten, Meldung der Schutzverletzung,
Kontrollfähigkeit	Informations- und Auskunftsrechte, Berichtigung, Löschungsrecht, Portabilität, Revision, Löschroutine, Meldungen von Sicherheitsvorfällen, Steuerbarkeit
Qualitätssicherung	Datensicherheit, technische und organisatorische Maßnahmen, Dokumentation
Risikoangemessenheit	Risikoanalyse und Robustheit der Systeme,
Kompetenz	Qualifizierung, Praxisrelevanz der Vorgaben, Selbstdatenschutz, Datenschutzbeauftragte

4. Bewertungsmodell

Der Index Beschäftigtendatenschutz ist ein gewichteter additiver Index. Für jede Antwort wird ein Wert zwischen 0 und 100 Punkten vergeben. Die Werte werden über die Faktoren summiert und anschließend gemittelt (vgl. Kapitel 3.1). Gleichzeitig werden Gewichtungen sowohl für die einzelnen Indikatoren (Fragen) als auch für die Faktoren und Qualitätsmaßstäbe vorgenommen (vgl. Kapitel 3.2), die die unterschiedlichen Relevanzen der Merkmalsdimensionen widerspiegeln. Die Gewichtungen sind theoretisch-inhaltlich begründet. Sie wurden auf der Grundlage einschlägiger Fachliteratur und von Expertengesprächen bestimmt (vgl. Kapitel 1.2) und erlauben so die Berücksichtigung von unterschiedlichen Relevanzen der einzelnen Elemente.

(Das ausführliche Dokument „BeDaX-Fragebogen inklusive Wertzuweisung und Gewichtungen" kann beim Projetleiter BeDaX angefordert werden.)

4.1 Grundprinzip der Wertezuweisung

Die Bewertung des betrieblichen Beschäftigtendatenschutzniveaus erfolgt auf der Grundlage eines umfangreichen Fragebogens, der die wichtigsten Aspekte rund um den Beschäftigtendatenschutz abfragt. Dabei sind die meisten Fragen nicht wertneutral, d.h. die Antworten sind im Sinne des betrieblichen Beschäftigtendatenschutzes als positiv oder negativ zu bewerten. Jede Merkmalsausprägung, d.h. jede Antwort, ist mit einem Wert zwischen 0 und 100 unterlegt, wobei 0 den niedrigsten und 100 den höchsten Wert darstellt. Die Werte werden entsprechend der Anzahl der Antworten gleichmäßig abgestuft. Demgegenüber dienen neutrale Fragen lediglich als Filter („Trichterfrage“) und fließen nicht in die Bewertung ein. Daher werden die Antworten hier jeweils mit dem Wert 0 belegt.

Folgende Tabelle zeigt eine ***Übersicht*** der zugewiesenen Werte abhängig vom Skalenniveau der Fragen:

Skalenniveau des Merkmals	**Merkmalsausprägungen**	**Zugewiesener Wert**
Dichotom (positiv*)	Positive Ausprägung	100
	Negative Ausprägung	0
Dichotom (negativ*)	Positive Ausprägung	0
	Negative Ausprägung	100
Ordinal (positiv*)	Ja	100
	Eher ja	75
	Teils, teils	50
	Eher nein	25
	Nein	0
Ordinal (negativ**)	Ja	0
	Eher ja	25
	Teils, teils	50
	Eher nein	75
	Nein	100
Aufzählungen*** (ordinal)	Je Item	Anzahl der Items dividiert durch 100
Trichterfragen (wertneutral, nominal)	Ja	0
	Nein	0

Erläuterungen:
*positiv = Zustimmung wird im Sinne des Beschäftigtendatenschutzes als positiv gewertet
**negativ = Ablehnung wird im Sinne des Beschäftigtendatenschutzes als positiv gewertet
*** Aufzählung = Je mehr Items ausgewählt werden, desto besser im Sinne des Beschäftigtendatenschutzes

Zur besseren Verständlichkeit zeigt folgende Tabelle ausgewählte ***Beispiele***:

Frage	**Merkmalsausprägungen**	**Zugewiesener Wert**
Gibt es ein Konzept für den Beschäftigtendatenschutz, das die Einhaltung des Datenschutzrechts für die Beschäftigten sicherstellt? (Skalenniveau: dichotom, positiv)	Ja	100
	Nein	0
Gibt es eine Auftragsverarbeitung von Beschäftigtendaten (z.B. Clouddienste, externe	Ja	0
	Nein	100

Lohnbuchhaltung)? (Skalenniveau: dichotom, negativ)		
Weiß die Interessenvertretung grundsätzlich, welche Daten zu welchen Zwecken über die Beschäftigten im Unternehmen erhoben und gespeichert sind? (Skalenniveau: ordinal, positiv)	Ja	100
	Eher ja	75
	Teils, teils	50
	Eher nein	25
	Nein	0
Entstehen bei einer Verweigerung einer erbetenen Einwilligung in die Datenverarbeitung Nachteile für die Beschäftigten? (Skalenniveau: ordinal, negativ)	Ja	0
	Eher ja	25
	Teils, teils	50
	Eher nein	75
	Nein	100
Welche Aufgaben des Datenschutzbeauftragten sind geregelt? (Aufzählung)	Beratungs- und Unterstützungsaufgaben	jeweils 25
	Schulung, Unterweisung	
	Führung der Datenschutzdokumentation	
	Zusammenarbeit mit der Aufsichtsbehörde	
	Sonstige	0
Erfüllt Ihr Unternehmen bzw. Ihre Verwaltung die Voraussetzungen zur Pflicht, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen? (Trichterfrage, nominal)	Ja	0
	Nein	0

4.2 Besonderheiten der Wertezuweisung

Filterführung

Die Besonderheiten der Wertezuweisung bei der Filterführung des BeDaX resultieren aus der unterschiedlichen Behandlung der Folgefragen in Abhängigkeit von den jeweiligen Filterfragen.

Trichterfragen

Im BeDaX-Tool gibt es zwei Trichterfragen: eine zum Verzeichnis aller Verarbeitungstätigkeiten und eine zur Bestellung einer Datenschutzbeauftragten. Trichterfragen sortieren diejenigen Befragten aus, die keine Antwort auf die eigentliche Testfrage geben können. Trichterfragen werden nicht gewertet.

Beispiel – Trichterfrage:

„Erfüllt Ihr Unternehmen bzw. Ihre Verwaltung die Voraussetzungen zur Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen?“

□ Ja -> 0
□ Nein -> 0

Folgefrage, wenn Antwort „ja“: „Gibt es ein Verzeichnis von Verarbeitungstätigkeiten in Ihrem Unternehmen gemäß der DSGVO?“

□ Ja -> 100
□ Nein -> 0

Lautet die Antwort auf die Trichterfrage „nein“, werden die Folgefragen ausgeblendet und ebenfalls nicht gewertet.

Filterfragen #1 und #2

Bei Filterfragen des Typs #1 und #2 handelt es sich um nicht wertneutrale Filterfragen, d.h. auch die Filterfrage wird gewertet. Diese Filterfragen sind immer dichotom und werden mit „ja“ oder „nein“ beantwortet.

Die beiden Typen #1 und #2 unterscheiden sich dabei wie folgt:

Bei *Filterfragen #1* wird die Antwort „ja“ mit 100 bewertet, die Antwort „nein“ mit 0. Demnach ist es im Sinne des Beschäftigtenschutzes gut, wenn die Frage mit „ja“ beantwortet wird, wie beispielsweise bei der Frage, ob es ein betriebliches Datenschutzkonzept oder ein Berechtigungs- und Rollenkonzept gibt. Die Wertezuordnung bei den Folgefragen erfolgt, wie in Kapitel 3.1 beschrieben. Bei „nein“ werden die Folgefragen ausgeblendet und nicht bewertet.

Beispiel – Filterfrage #1

„Sind im Unternehmen Grundsätze zur Leistungs- und Verhaltenskontrolle geregelt?“

□ Ja -> 100
□ Nein -> 0

Bei Filterfragen #2 wird die Antwort „nein“ mit 100 bewertet, die Antwort „ja“ mit 0. Im Unterschied zu den Filterfragen #1 ist es im Sinne des Beschäftigtendatenschutzes bei diesen Fragen demnach besser, wenn es den abgefragten Tatbestand nicht gibt, wie beispielsweise eine Beschäftigtendatenverarbeitung auf der Basis von Einwilligungen, oder eine Weitergabe von Beschäftigtendaten an Unternehmen in Drittländer. Die hier abgefragten Tatbestände sind zwar im rechtlichen Sinne nicht unzulässig, erhöhen jedoch das Risiko, gegen den Beschäftigtendatenschutz zu verstoßen. Bei guter Ausgestaltung kann im BeDaX bei diesen Fragen dennoch die volle Punktzahl erreicht werden. Die Wertezuordnung bei den Folgefragen erfolgt, wie in Kapitel 3.1 beschrieben. Bei „nein“ werden die Folgefragen ausgeblendet und nicht bewertet.

Beispiel – Filterfrage #2

„Gibt es eine Auftragsverarbeitung von Beschäftigtendaten (z.B. Clouddienste, externe Lohnbuchhaltung)?“

□ nein -> 100
□ ja -> 0

4.3 Gewichtungen

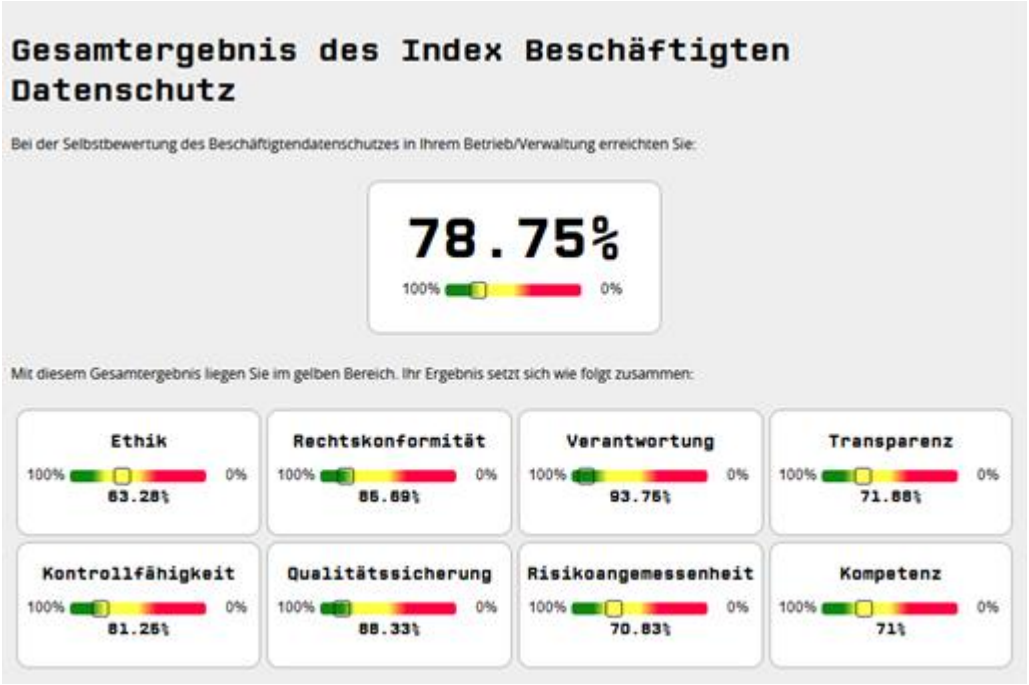
Da sich die Qualitätsmaßstäbe hinsichtlich ihrer Bedeutung für die Einschätzung des Datenschutzniveaus in den Unternehmen bzw. Verwaltungen unterscheiden, wurden auf der Basis der Experteninterviews die jeweiligen Gewichtungen festgelegt. Rechtskonformität und Transparenz bilden dabei die wichtigsten Qualitätsmaßstäbe und wurden deshalb mit 30 % plus 25 % über 50 % gewichtet. Die weiteren 6 Qualitätsmaßstäbe sind mit 8 % bzw. 7 % relativ gleich bewertet.

Ethik	8 %
Rechtskonformität	30 %
Verantwortung	8 %
Transparenz	25 %
Kontrollfähigkeit	7 %
Qualitätssicherung	7 %
Risikoangemessenheit	7 %
Kompetenz	8 %

Ähnlich wie bei den Qualitätsmaßstäben finden auch die Faktoren innerhalb der Qualitätsmaßstäbe sowie die Einzelfragengewichtung in unterschiedlicher Gewichtung Eingang in die Bewertung. Die detaillierten Gewichtungen der Faktoren und Fragen können beim Projektleiter BeDaX angefordert werden.

5. Ergebnisdarstellung

Das über den Index Beschäftigtendatenschutz ermittelte Datenschutzniveau im Betrieb bzw. in der Verwaltung wird als Wert zwischen 0 (niedrigster Wert) und 100 (höchster Wert) ausgegeben. Zusätzlich wird das Ergebnis auf einer Farbskala von grün (100 bis 80 Punkte), über gelb (unter 80 bis 50 Punkte) bis rot (unter 50 Punkte) farblich unterlegt. So können auf einen Blick das Gesamtergebnis und die Ergebnisse entlang der Qualitätsmaßstäbe erfasst werden. Um die „Schwachstellen“ im Datenschutzniveau besser lokalisieren zu können, erfolgt im Anschluss an den Ergebnisüberblick eine detaillierte Ausgabe der Werte pro Einzelfrage.



Warnhinweise

Legt die Antwort einen klaren Rechtsverstoß nahe, der möglicherweise ein Bußgeld gemäß DSGVO nach sich ziehen könnte, wird direkt ein Warnhinweis ausgegeben. Diese Warnhinweise finden sich zusätzlich bei der Auswertung zu der jeweiligen Frage wieder. Hier ein Beispiel für einen Warnhinweis:

Bei der Frage, ob eine Einwilligung nachvollziehbar dokumentiert wurde, wird bei der Antwort Nein oder eher Nein folgender Warnhinweis ausgegeben:

> **Keine nachvollziehbaren Einwilligungen?**
> Die grundsätzlichen Anforderungen an die Wirksamkeit einer rechtswirksamen Einwilligung sind in Art. 4 Nr. 11 und 7 DSGVO festgehalten und in Erwägungsgrund 32 weiter spezifiziert. Diese muss freiwillig, für einen konkreten Fall, nach ausreichender Information des Betroffenen und unmissverständlich abgegeben werden.
> Eine Einwilligung, die nicht den dargestellten Anforderungen genügt, ist unwirksam und kann nicht als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden. Bei Verstößen gegen die Grundsätze der Verarbeitung, einschließlich der Bedingungen für die Einwilligung, kann von der zuständigen Aufsichtsbehörde nach Maßgabe von Art. 83 Abs. 5 lit. a DSGVO eine Geldbuße verhängt werden. Außerdem kommen je nach den Umständen des Einzelfalls auch Schadensersatzansprüche der betroffenen Person in Betracht.

(Das entsprechende Dokument mit allen Warnhinweisen zum BeDaX-Tool kann beim Projektleiter BeDaX angefordert werden.)