Rechtliche Rahmenbedingungen und Handlungsempfehlungen

Im Grünbuch „Digitale Agenda Bodensee – Eine Bestandsaufnahme zum Potenzial der *Digitalisierung* innerhalb KMU in der *Bodenseeregion*“ wurden für *kleine und mittlere Unternehmen (KMU)* relevante Sachverhalte der Digitalisierung jeweils beschrieben und den potenziell einschlägigen Rechtsbereichen zugeordnet, aus deren Anwendung sich Herausforderungen im Umgang mit entsprechenden Phänomenen ergeben können.

Die Befragung aus dem Vorjahr sowie die im Anschluss durchgeführten Workshops belegten zunächst die Praxisrelevanz der untersuchungsgegenständlichen Digitalisierungssachverhalte. Die als „übergeordnete Sachverhalte“ geführten Untersuchungsobjekte wurden hierbei besonders häufig als Teilmengen der *Digitalisierung* erkannt und diskutiert.“

Die Workshop-Gruppen eigneten sich aufgrund ihrer heterogenen Zusammensetzung sehr gut, um die Praxisrelevanz der ausgesuchten Sachverhalte zu bestätigen. So befanden sich unter den Teilnehmenden Repräsentanten von KMU – hierunter auch Geschäftsführung von Start-ups aus dem Bereich Industrie 4.0 und Big Data Analysis, Rechtsabteilungsleitung und Leitung von IT-Abteilungen – sowie Rechtsanwaltskanzleien und Vertreter von Industrie- und Handelskammern.

Neben der Plausibilisierung der untersuchungsgegenständlichen Digitalisierungssachverhalte wurden mit den Teilnehmenden die nachstehenden Thesen diskutiert:

- **These I: Digitalisierung ist nicht schwer**
  „Die rechtlichen Herausforderungen der *Digitalisierung* sind lediglich scheinbar komplex. Durch Aufschlüsselung des weitgefassten Begriffs lassen sich einzelne Phänomene / Sachverhalte identifizieren und eindeutig analysieren.“
- **These II: Digitalisierung braucht nicht mehr Regulierung**
  „Es bedarf keiner weiteren gesetzgeberischen Massnahmen, um rechtlichen Herausforderungen der *Digitalisierung* zu begegnen – bestehende Regelungen reichen aus, um sie zu bewältigen.“
- **These III: Digitalisierung braucht schon gar kein Dateneigentum**
  „... es bedarf insbesondere keiner Normierung eines Dateneigentums.“

Die Teilnehmenden stimmten hierbei insbesondere zu, dass sich Rechtsfragen zu den festgestellten Digitalisierungssachverhalten überwiegend in den bestehenden Rechtsrahmen einordnen und mit diesem beantworten lassen. KMU fehle es hingegen an Zeit, Ressourcen und Kompetenz, um relevante Rechtsfragen frühzeitig zu erkennen und diesen adäquat begegnen zu können. Ausserdem wurde die Forderung nach mehr Fachkräften zur Beurteilung von digitalisierungsspezifischen Rechtsfragen (etwa IT-Anwälte und Richter) sowie nach mehr aufklärenden Informationsveranstaltungen und -materialien vorgebracht. Eine Erweiterung des bestehenden Rechtsrahmens und vor allem die Einführung eines Eigentumsrechts an Daten, traf bei den Workshop-Teilnehmenden eher auf Ablehnung.

Auch ergänzende Experteninterviews, die mit Geschäftsführungen und Rechtsabteilungsleitungen aus KMU geführt wurden, bestätigten die Relevanz der übergeordneten Sachverhalte. Weiterhin zeigte sich, dass sich KMU überwiegend erst bei der Durchführung von Digitalisierungsmassnahmen mit einschlägigen rechtlichen Fragestellungen auseinandersetzen, anstatt diese bereits bei der Planung digitaler Strategien zu antizipieren. Eine Ausnahme bilden hier die Aspekte des Datenschutzes. Einerseits begründeten die Befragten diesen Umstand mit fehlenden Ressourcen und Kompetenzen. Darüber hinaus wurde aber auch ein fehlendes Bewusstsein bezüglich potenzieller Rechtsfragen in den unterschiedlichen Unternehmensfachbereichen als ursächlich befunden – im Vordergrund stünden hierbei vielmehr technische und kommerzielle Aspekte.

Zusammenfassend lässt sich an diesen Feststellungen ein dringender Bedarf bei KMU für praxisnahe, rechtliche Orientierungshilfen erkennen. Es scheint wichtig, in den Unternehmen ein Problembewusstsein für rechtliche Herausforderungen zu schaffen. Gleichzeitig soll den Unternehmen ausreichend Informationen an die Hand gegeben werden, um zumindest einen ersten, strukturierten Abgleich zwischen Digitalisierungsbestrebungen und potenziell einschlägigen Rechtsproblemen bewerkstelligen zu können. Der Abgleich soll niederschwellig möglich zugänglich sein, damit dafür keine Spezialisten eingekauft werden müssen (Orientierung). Im Rahmen der durchgeführten Experteninterviews wurden unter anderem nachstehende, auf KMU abgestimmte Massnahmen angeregt, um eine solche Orientierung bereitzustellen:

- Wissensdatenbanken
- Orientierungspapiere
- Workshops und Vorträge
- Zusammenarbeit mit Hochschulen

Mit der rechtlichen Analyse branchenübergreifender und -spezifischer Sachverhalte, leistet dieses Weissbuch einen ersten Beitrag zu dieser Orientierung. Dies findet im Wissen statt, dass darüber hinaus weitere Massnahmen zur Unterstützung von KMU notwendig sind.

Im Weiteren werden rechtliche Fragen zu den folgenden branchenübergreifenden Digitalisierungssachverhalten näher betrachtet:

- Daten mit Personenbezug
- Daten als Asset
- IT-Sicherheit
- Cyber-physische Systeme
- Cloud Computing und digitale Plattformen

Am Ende dieses Kapitels finden Sie einen Link und QR-Code, welcher Sie direkt zu diesen branchenspezifischen Sachverhalten führt.

Daten mit Personenbezug

KMU müssen bei der *Digitalisierung* von Arbeitsprozessen, der Vernetzung von IT-Systemen oder der Nutzung digitaler Dienste, wie z. B. Cloud

Services regelmässig datenschutzrechtliche Vorschriften, wie insbesondere die EU-DSGVO berücksichtigen. Dies kann auf den weiten sachlichen sowie räumlichen Anwendungsbereich zurückgeführt werden. Im Falle von Verstössen gegen den Datenschutz drohen Bussgelder in Höhe von bis zu 20 Millionen Euro oder 4 % des konzernweit erwirtschafteten Jahresumsatzes (sofern höher). Daher sind KMU angehalten, ihre Geschäftstätigkeiten im Einklang mit dem Datenschutzrecht zu gestalten und die dahingehenden individuellen Handlungsbedarfe nicht nur einmalig zu ermitteln, sondern regelmässig erneut zu evaluieren. Dieses Kapitel beschäftigt sich mit der Frage, wann welche datenschutzrechtlichen Vorschriften für KMU einschlägig sein und datenschutzrechtliche Handlungsfelder im Unternehmen organisiert werden können (Datenschutz-Management-System). Zudem wird skizzenhaft aufgezeigt, welche digitalisierungs- und gleichzeitig datenschutzspezifischen Problematiken in Bezug auf die besonders bedeutungsvollen Themen wie Webanalyse und Reichweitenmessung, Cloud Services und vernetzte Systeme entstehen.

1. Abgrenzung personenbezogener von nichtpersonenbezogenen Daten

Unter der Verarbeitung personenbezogener Daten ist gem. Art. 4 Nr. 2 DSGVO jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten gemeint. Personenbezogene Daten beziehen sich anders als sonstige, nicht *personenbezogene Daten*, wie bspw. reine Sensor- / *Maschinendaten*, auf eine identifizierte oder identifizierbare natürliche Person (Art. 4 Nr. 1 DSGVO). Demgegenüber beziehen sich anonyme oder anonymisierte Daten nicht oder nicht mehr auf eine identifizierte oder identifizierbare natürliche Person, weshalb eine Datenverarbeitung im Einklang mit den strengen Vorschriften des Datenschutzrechts nicht mehr zwingend erforderlich ist. Ist eine Anonymisierung nicht möglich, so können Massnahmen zur Erhöhung der Sicherheit der Verarbeitung personenbezogener Daten getroffen werden, wie insbesondere die Pseudonymisierung und Verschlüsselung (vgl. Art. 32 Abs. 1 lit. a DSGVO). Bei der Pseudonymisierung ist die Personenbeziehbarkeit von Informationen weiterhin möglich und damit auch das Datenschutzrecht anwendbar; es handelt sich damit lediglich um eine andere Form der Speicherung, während die Verschlüsselung eine Sicherheitsmassnahme darstellt, durch welche die unbefugte Kenntnisnahme der Daten durch Dritte erschwert werden soll (Klabunde, 2018, s. Erwägungsgrund 26 DSGVO).

2. Räumlicher Anwendungsbereich der EU-DSGVO

KMU des Bodenseeraums mit Sitz in den Ländern Deutschland und Österreich unterliegen in Bezug auf die Verarbeitung personenbezogener Daten neben den jeweiligen nationalen datenschutzrechtlichen Vorschriften auch den europäischen Vorschriften der DSGVO. Die Anwendbarkeit der DSGVO für KMU mit Sitz in der Schweiz und eine Angleichung der nationalen Schweizer Datenschutznormen an das europäische Recht sind bis zum Jahr 2020 beabsichtigt (Schweizerische Bundesamt für Justiz, 2019). Nachstehend werden daher die Grundlagen des Datenschutzrechts mit dem Fokus auf das europäische Datenschutzrecht erläutert.

Bezogen auf eine identifizierte natürliche Person	Bezogen auf eine identifizierbare natürliche Person	Besondere Kategorien pbD („sensible Daten“ gem. Art. 9 Abs. 1 DSGVO)	Kein Personenbezug
· Name · Geburtsdatum · Adresse · E-Mail-Adresse · Telefonnummer · …	· Ermittlung der Identität einer Person durch Verwendung ergänzender Informationen wie zum Beispiel: · IP-Adresse (EuGH „Breyer“) · Geräte-IDs · Cookies zum Zweck der Identifizerung · Device Fingerprints · Kfz-Kennzeichen · Personalnummer · Ausweisnummer · Kontonummer · Berufliche Aktivitäten · weitere nicht ausreichend anonymisierte (oder pseudonymisierte) Daten	· Daten bezogen auf Rasse / ethnische Herkunft · politische Gesinnung · Religion / philosophische Überzeugung · Gewerkschaftszugehörigkeit · genetische / biometrische Daten, z. B. Fingerabdrücke zur Entsperrung von Apps · Gesundheit · sexuelle Orientierung	· Anonyme Informationen · Daten ohne Bezug auf eine identifizierte oder identifizierbare natürliche Person · anonym erhaltene Daten deren Ursprung nicht oder nicht mehr ermittelbar sind · reine Maschinendaten / Sensordaten ohne Personenbezug

Abbildung 12: Abgrenzung personenbezogener Daten von nicht-personenbezogenen Daten

Auch für in der Schweiz ansässige KMU kann neben dem nationalen Schweizer Datenschutzgesetz (DSG) die EU-DSGVO Anwendung finden, vor allem dann, wenn

a. nach dem sog. Niederlassungsprinzip gem. Art. 3 Abs. 1 DSGVO eine Niederlassung eines in der Schweiz ansässigen Unternehmens *personenbezogene Daten* innerhalb der EU verarbeitet oder
b. nach dem sog. Marktortprinzip gem. Art. 3 Abs. 2 DSGVO ein in der Schweiz ansässiges Unternehmen Waren und Dienstleistungen für EU-Bürgerinnen und Bürger anbietet (z. B. auf Websites) oder wenn dieses auf Websites Webtracking betreibt, durch welches sich das Surfverhalten von EU- Bürgern beobachten lässt.

3. Allgemeine datenschutzrechtliche Pflichten und nationale Besonderheiten sowie Ausnahmen für KMU

Grundsätzlich ist im Falle der Anwendbarkeit der DSGVO regelmässig insbesondere auf die Umsetzung folgender Pflichten zu achten:

- Einhaltung der datenschutzrechtlichen Grundsätze nach Art. 5 DSGVO (Grundsätze der Richtigkeit, Zweckbindung, der Rechtmässigkeit und der Verarbeitung nach Treu und Glauben, der Speicherbegrenzung und der Integrität und Vertraulichkeit) und damit v. a. die Verarbeitung personenbezogener Daten nur auf Basis einschlägiger Rechtsgrundlagen (Art. 6 DSGVO); hierbei ist die Besonderheit der Möglichkeit einer Einwilligung 14-Jähriger in Österreich zu beachten (§ 4 Abs. 4 DSG)

- Einhaltung der Transparenz- / Informationspflichten (Artikel 13 und 14 DSGVO)
- Gewährleistung der Wahrnehmung der Betroffenenrechte (Art. 16 – 22 DSGVO)
- Einhaltung der Benachrichtigungs- und Meldepflichten bei Datenschutzverstössen (Art. 33 und 34 DSGVO), jedoch bestehen bislang keine expliziten Meldepflichten für Datenschutzverstösse in der Schweiz[1]
- Führen eines Verzeichnisses für Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Abschluss von Verträgen zur Auftragsverarbeitung gem. Art. 28 DSGVO (s. Kapitel „Cloud-Computing und digitale Plattformen“)
- Sicherstellung eines angemessenen Datenschutzniveaus im Falle einer Übermittlung personenbezogener Daten in sog. Drittländer (Art. 44 DSGVO)
- Ggf. Benennung eines Beauftragten für den Datenschutz (Art. 37 DSGVO), wobei die Konkretisierung der Anforderungen an die Bestellpflicht eines Datenschutzbeauftragten in Deutschland (§ 38 Abs. 1 BDSG) als auch die Besonderheit des Zeugnisverweigerungsrechts und der Verschwiegenheitspflicht des Datenschutzbeauftragten in Österreich (§ 5 DSG) zu beachten ist
- Umsetzung technisch-organisatorischer Massnahmen (TOMs) (Art. 32 DSGVO)

Neben den bereits genannten Besonderheiten der nationalen Datenschutzgesetze im Vergleich zur EU-DSGVO ist auch die jeweilige Konkretisierung des Beschäftigtendatenschutzes in Deutschland und Österreich (§ 26 BDSG, § 11 DSG) hervorzuheben.

Die besondere Situation, welche sich für KMU namentlich in personeller und wirtschaftlicher Hinsicht ergibt, sollte in der DSGVO zwar berücksichtigt werden (Erwägungsgrund 13 zur DSGVO), jedoch halten sich die dahingehenden praktischen Erleichterungen in Grenzen. Dies zeigt sich an den beiden folgenden Beispielen: Art. 30 Abs. 5 DSGVO sieht die Pflicht zum Führen eines Verfahrensverzeichnisses zwar dann nicht vor, wenn eine Einrichtung weniger als 250 Mitarbeitende beschäftigt. Allerdings besteht für KMU diese Pflicht bei risikoträchtigen, nicht nur gelegentlichen Verarbeitungen oder bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 bzw. 10 DSGVO trotzdem. Dadurch ist der Anwendungsbereich dieser Ausnahme nicht allzu gross. In Bezug auf die Umsetzung der TOMs können nach Art. 24 Abs. 1 und 2 DSGVO aufgrund des Verhältnismässigkeitsprinzips dahingehende Erleichterungen, Flexibilität und wirtschaftlich vertretbare Lösungen für KMU bedeuten (Sydow, 2018). Hier sollte eine Abwägung jedoch nicht zulasten der Wahrung der Rechte und Freiheiten der Betroffenen stattfinden. Risikoaverse KMU werden daher im Zweifel eher bestrebt sein, den höheren datenschutzrechtlichen Anforderungen nachzukommen. Wesentliche Erleichterungen in Bezug auf die Umsetzung datenschutzrechtlicher Pflichten können KMU im Verhältnis zu Grosskonzernen damit im Wesentlichen durch die Abwägung von Risiken bzw. das Eingehen verbleibender Risiken erreichen.

[1] Künftig sollen diese nach einem Entwurf des revidierten Schweizer DSG jedoch „so rasch als möglich“ stattfinden (vgl. den Entwurf der Schweizerischen Eidgenossenschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz unter: https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf (Stand: 09.03.2019).

4. Implementierung eines Datenschutz-Managementsystems

Für die Umsetzung der einzelnen datenschutzrechtlichen Anforderungen kann sich die, ggf. auch gesetzlich verpflichtende, Etablierung eines Datenschutz-Management-Systems (DMS) eignen. Sie sollte sich an die sieben Grundelemente (Abbildung 13) eines *Compliance*-Management-Systems (CMS) nach dem Prüfungsstandard 980 des Instituts der Wirtschaftsprüfer (IDW) als Grundgerüst anlehnen (Institut der Wirtschaftsprüfer, 2011; Auer-Reinsdorff & Conrad, 2016) (siehe Abbildung 13).

Datenschutz-Kultur	Die Schaffung einer Datenschutz-Kultur, insb. Schärfung des Bewusstseins der Mitarbeitenden für datenschutzrelevante Sachverhalte
Datenschutz-Ziele	Festlegung von Datenschutz-Zielen als Teil allgemeiner Unternehmensziele
Datenschutz-Organisation	Entwicklung einer Datenschutz-Organisation, wozu feste Prozesse, Rollen, Verantwortlichkeiten und Berichtswege zählen.
Datenschutz-Risiken	Frühzeitige Ermittlung von Datenschutz-Risiken und Berichterstattung hierzu
Datenschutz-Programm	Massnahmen zur Begrenzung und Vermeidung von Datenschutzverstössen und deren Dokumentation
Datenschutz-Kommunikation	Informierung der Mitarbeitenden und Etablierung eines Prozesses zum Umgang mit Schwachstellen
Überwachung + Verbesserung des DMS	Fortlaufende Prüfung des DMS im Hinblick auf die Angemessenheit und Wirksamkeit auf Basis der Dokumentation des DMS

Abbildung 13: Bestandteile eines Datenschutz-Management-Systems

Um der Bindung einer Grosszahl interner Ressourcen für die Bearbeitung von Datenschutzthemen vorzubeugen, kann es für KMU sinnvoll sein, ein DMS zusammen mit einem externen Datenschutzbeauftragten zu entwickeln. Es kann auch dann ein solcher externer Datenschutzbeauftragter bestellt werden, wenn hierzu keine Verpflichtung besteht (z. B. aufgrund der nicht einschlägigen Beispielfälle aus Art. 37 Abs. 1 DSGVO oder der nicht erreichten Mindestanzahl von Mitarbeitenden, welche die Bestellpflicht auslösen).

5. Digitalisierungsspezifische Problembereiche und Handlungsempfehlungen

Aus datenschutzrechtlicher Sicht kommt insbesondere den digitalisierungsspezifischen Themengebieten der Webanalyse bzw. des Webtrackings und der Reichweitenmessung, des Cloud-Computing sowie der Vernetzung von Systemen besondere Bedeutung zu. Durch den Transfer personenbezogener Daten zwischen Geschäftspartnern und Dienstleistern bei vernetzten Systemen stellt sich zuallererst oftmals die Frage, welche Partei welche datenschutzrechtlichen Verantwortlichkeiten übernimmt. Nachstehend werden die Besonderheiten der datenschutzrechtlichen Verantwortlichkeit bei digitalisierungsspezifischen Sachverhalten sowie anschliessend jene der Webanalyse, des Cloud-Computing sowie der Vernetzung von Systemen dargestellt.

5.1 Datenschutzrechtliche Verantwortlichkeit bei digitalisierungsspezifischen Sachverhalten

Werden *personenbezogene Daten* zwischen Unternehmen transferiert, so bestimmen sich die datenschutzrechtliche Verantwortlichkeit und der damit einhergehende Handlungsbedarf danach, wer Mittel und Zwecke der Datenverarbeitung festlegt. Geschieht dies gemeinsam durch zwei oder mehrere Verantwortliche (z. B. aufgrund des gemeinsamen Betriebes einer Datenbank), so ist von einer gemeinsamen Verantwortlichkeit („Joint Controllership“) gem. Art. 26 DSGVO auszugehen. Es ist dann ein entsprechender Joint-Controllership-Vertrag abzuschliessen. Darin sind die jeweiligen Verantwortlichkeiten der einzelnen Parteien zu konkretisieren, insbesondere im Hinblick auf die Wahrnehmung der Betroffenenrechte und die Informationspflichten nach den Artikeln 13 und 14 DSGVO (Schneider, 2019). Zusätzlich sind vor allem beim Betrieb gemeinsamer Datenbanken die jeweiligen Datensphären und die TOMs in Abhängigkeit der konkreten Verarbeitungstätigkeiten und der damit einhergehenden individuellen Risiken je Partei zu definieren. Daneben bedarf die Datenübermittlung in diesem, aber auch in jenem Fall, in welchem anstelle der gemeinsamen eine eigene Verantwortlichkeit vorliegt, einer gesonderten Rechtsgrundlage nach Art. 6 DSGVO, da Joint Controller nach Art. 4 Nr. 10 DSGVO sogenannte „Dritte“ sind (Dovas, 2016, S. 512). Eine gemeinsame Verantwortlichkeit kann z. B. bei Big Data-Anwendungen, im Bereich des Affiliate-Marketings oder bei der sukzessiven oder gleichzeitigen Verarbeitung bzw. Übermittlung von Daten zwischen Internetplattformen vorliegen (Dovas, 2016, S. 512).

Wird ein Unternehmen lediglich weisungsgebunden und ohne eigene Entscheidungsbefugnis für und im Auftrag einer verantwortlichen Stelle (den Auftraggeber) tätig (z. B. im Rahmen von IT-Support und Wartungsdienstleistungen), so handelt dieses selbst als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO (Auftragnehmer) und ein Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO ist abzuschliessen. Beauftragt ein Auftragsverarbeiter z. B. im Rahmen des Softwarehostings seinerseits selbst einen Auftragsverarbeiter (z. B. einen Cloudanbieter), so ist auch zwischen diesen beiden Parteien ein entsprechender Vertrag unter Berücksichtigung der Besonderheiten der Unterbeauftragung abzuschliessen. Der Auftraggeber sollte sich im Rahmen seiner Weisungsbefugnis also stets vertraglich zusichern lassen, dass Unterauftragnehmer / Subdienstleister nur mit seiner vorherigen Genehmigung vom Auftragnehmer eingesetzt werden.

5.2 Datenschutzrechtliche Besonderheiten der Webanalyse, des Cloud-Computing sowie der Vernetzung von Systemen

Der Einsatz von Webtracking-Tools (z. B. Google Analytics, Matomo), die Nutzung von Cloudangeboten (z. B. durch Speicherplatz) sowie die Vernetzung von Systemen ziehen jeweils datenschutzrechtliche Besonderheiten nach sich. Dazu sind in Abbildung 14 die jeweiligen grundlegenden Handlungsempfehlungen beispielhaft zusammengefasst. Dabei wird davon ausgegangen, dass *personenbezogene Daten* verarbeitet werden.

Daten als Asset

1. Paradigmenwechsel im Umgang mit Daten ohne Personenbezug

Daten und ihre Verwertung durch Analysemethoden tragen nicht nur zur Realisierung von Effizienzpotenzialen beim Einsatz von Ressourcen bei. Sie eröffnen auch die Weiterentwicklung bestehender und die Einführung neuer Geschäftsmodelle (Geissbauer, Schrauf, Berttram, & Cheraghi, 2017, S. 26). Damit stossen Daten bzw. die hieraus gewonnene Information sukzessive in das Zentrum erfolgsrelevanter Wertschöpfungsfaktoren vor. Das könnte sie zukünftig auf eine Ebene mit Arbeitskraft, Technologie und Kapital als Kernfaktoren der Wertschöpfung heben (Porter & Happelmann, 2015, S. 3; Otto, et al., 2016, S. 10). In Unterscheidung zu den vorgenannten Produktionsfaktoren ist ausserdem zu

Webtracking-Tools (z. B. Google Analytics, Matomo)	Cloud Computing, z. B. in Form von Speicherplatz	Vernetzung von Systemen
· Sicherstes Vorgehen auf Basis einer expliziten Einwilligung · Information der Website-Besucher über Tracking-Methoden in Datenschutzhinweisen · Wahl der jeweils möglichen datenschutzfreundlichen Voreinstellungen	· in der Regel Abschluss einer Vereinbarung zur Auftragsverarbeitung erforderlich · Zusicherung von Serverstandorten in der EU / des EWR empfehlenswert · Anonymisierung der Daten, Einsatz von adäquaten Verschlüsselungstechnologien	· Klärung der datenschutzrechtlichen Verantwortlichkeiten für die Systeme / Systemkomponenten · Wahrung des Grundsatzes der Zweckbindung, Vorsicht bei der Verknüpfung von Datensätzen · Wahrung der Transparenzpflichten gegenüber Betroffenen

Abbildung 14: Handlungsempfehlungen für Webtracking-Tools, Cloud-Computing und der Vernetzung von Systemen