Ergebnisse der Anhörung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

vom 28. Juni 2019 bei der IHK Stuttgart

zur

Evaluierung der DS-GVO

-

„Wenn es nicht sinnvoll ist, dann ist es kein Datenschutz.“

- Für einen praxistauglichen Datenschutz in Baden-Württemberg -

Inhalt

Vorwort

Seit dem 25. Mai 2018 ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) gesetzlich dazu verpflichtet, die Einhaltung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, kurz: die Datenschutz-Grundverordnung - DS-GVO in Baden-Württemberg zu beaufsichtigen und die Verantwortlichen im Lande zu beraten.

Art. 97 Abs. 1 DS-GVO sieht vor, dass die EU-Kommission dem EU-Parlament und dem Rat bis zum 25. Mai 2020 einen Bericht über die Bewertung und Überprüfung der DSGVO vorlegt. Art. 97 Abs. 3 DS-GVO gibt der Kommission hierfür das Recht, Informationen unter anderem auch von den Aufsichtsbehörden anzufordern. Hierzu möchte auch der LfDI Baden-Württemberg seine Einschätzungen, welche aus der bisherigen praktischen Erfahrung seiner unabhängigen obersten Landesbehörde resultieren, zur Kenntnis geben und nimmt die Gelegenheit wahr, Anregungen zur Evaluierung der DS-GVO zu unterbreiten.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK) hat sich mit ihrem „Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden“ vom 06. November 2019, welche vom LfDI Baden-Württemberg mitgetragen wurde, bereits mit dem aus ihrer Erfahrung mit der Anwendung der DS-GVO resultierenden Änderungsvorschlägen an den Europäischen Datenschutzausschuss gewandt. Den Vorsitz des eigens hierzu eingesetzten Projekt-Arbeitskreises der DSK hatte der LfDI Baden-Württemberg inne.

Die Sicht der Aufsichtsbehörden ist sicherlich wichtig und für die EU-Kommission hilfreich – nicht wenig wichtig sind aber die Erfahrungen, welche die Verantwortlichen und Anwendenden der DS-GVO in Baden-Württemberg gesammelt haben – buchstäblich am eigenen Leibe. Um diesen Erfahrungen Rechnung zu tragen, hat der LfDI Baden-Württemberg am 28 Juni 2019 eine Anhörung unter dem Banner „#DSGVO wirkt (?) – 1 Jahr DSGVO – Praxiserfahrungen und Evaluation“ in Zusammenarbeit mit der Industrie- und Handelskammer Region Stuttgart veranstaltet. Zu Impulsvorträgen geladen waren Vertretungen aus Aufsicht, Behörden, Wirtschaft, Wissenschaft, Anwaltschaft, Verbänden und Datenverarbeitern. In einem eigens hierzu eingerichteten E-Mail-Postfach wurden außerdem über das ganze Jahr Zuschriften aus allen Bereichen des Landes gesammelt und ausgewertet – auch von dieser „niedrigschwelligen“ Möglichkeit, Kritik und Anregungen zur DS-GVO abzugeben, haben zahlreiche Institutionen wie Verbände und Vereine, aber auch viele Privatpersonen Gebrauch gemacht.

Der Kreis der Verantwortlichen in Baden-Württemberg ist mit dem Bundesdurchschnitt nur teilweise vergleichbar. Laut Ministerium für Wirtschaft und Finanzen Baden-Württemberg erwirtschaften beispielsweise kleine und mittlere Unternehmen jeden zweiten Euro Umsatz im Land und beschäftigen zwei Drittel der sozialversicherungspflichtigen Beschäftigten. Der Mittelstand ist damit das Rückgrat der Wirtschaft in Baden-Württemberg - und trägt in entscheidendem Maße zur wirtschaftlichen Entwicklung bei. Außerdem engagiert sich einem Bericht des Ministeriums für Soziales und Integration Baden-Württembergs zufolge fast jeder zweite Baden-Württemberger in seiner Freizeit ehrenamtlich in Vereinen und Verbände: über 48 Prozent der der Bürgerinnen und

Bürger tun dies. Baden-Württemberg ist damit bundesweit Spitzenreiter. Daraus ergeben sich auch ganz eigene, spezifische Herausforderungen und Anliegen an einen praxistauglichen Datenschutz. Diese landesspezifischen Erkenntnisse sollen - neben dem Erfahrungsbericht der DSK - einen Beitrag zur Evaluation der DS-GVO durch den europäischen Gesetzgeber bieten.

Insgesamt hat sich gezeigt, dass die Verantwortlichen in Baden-Württemberg sich in vielen Bereichen alltagstauglichere Lösungen wünschen und einige Vorschriften nur schwer auf datenverarbeitenden Tätigkeiten kleiner Unternehmen oder ehrenamtlicher Arbeit anwendbar sind. Im Vordergrund stehen vor allem Fragen rund um eine mögliche Entlastung bei den Informations-, Transparenz- und Auskunftspflichten, aber auch bei Fragen der Gemeinsamen Verantwortlichkeit und der Auftragsdatenverarbeitung. Trotz zahlreicher Muster und Praxisratgeber meiner Dienststelle und anderen Aufsichtsbehörden scheint hier immer noch eine gewisse Rechtsunsicherheit bei den Verantwortlichen vorhanden zu sein. Wider Erwarten haben sich Sorgen um Sanktionen – zumindest unter der Praxis in Baden-Württemberg – nicht als vorrangig herausgestellt. Dies mag nicht zuletzt daran liegen, dass in Baden-Württemberg immer wieder klargestellt wurde, dass Beratung vor Bestrafung geht – und dass viele Verantwortliche sich auf den Weg zu einer datenschutzkonformen Verarbeitung gemacht haben. Ca. 75% der Unternehmen im Lande gaben nach Umfrage der DIHK an, die DSGVO (zumindest bereits teilweise) umgesetzt zu haben. Meine Erfahrungen sind damit im Großen und Ganzen deckungsgleich.

Die Datenschutzaufsicht in Baden-Württemberg orientiert sich am Leitsatz „Wenn es nicht sinnvoll ist, dann ist es kein Datenschutz“. Unter dieser Zielsetzung soll auch der vorliegende Bericht verstanden werden. Er spiegelt die Stimmen aus dem Land wieder, welche meine Dienststelle bei ihrer täglichen Arbeit und im Laufe des gesamten Evaluierungsprozesses vernommen hat. Dieser Bericht ist eine Zusammenstellung von Erfahrungen und Anregungen der Verantwortlichen und Betroffenen im Land. Als Aufsichtsbehörde sehen wir uns in der Pflicht, der europäischen Ebene auch diese Stimmen zu Gehör zu bringen

Dr. Stefan Brink

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

1. Informations-, Auskunfts- und Transparenzpflichten

Die DS-GVO bringt Verpflichtungen, die kleine Vereine nun ebenso treffen wie Konzerne wie Apple, Amazon, Google, Microsoft oder Facebook. Darunter zahlreiche Pflichten, welche die Bundesgesetzgebung bislang nicht kannte. Der LfDI Baden-Württemberg erhält zahlreiche besorgte Anfragen und Beschwerden aus Vereinen, die sich überfordert fühlen oder Sanktionsandrohungen bei Fehlverhalten fürchten. Beratung alleine reicht den Vereinen im Land nicht aus, es werden tatsächliche Entlastungen gefordert. Vereine und kleine Unternehmen können sich im Gegensatz zu größeren Unternehmen häufig externe Experten nicht leisten.

Viele kleine und mittlere Unternehmen sowie ehrenamtlich Tätige haben in der Praxis erhebliche Schwierigkeiten, die gesetzlich vorgesehenen Informationspflichten umfassend zu erfüllen. Es gilt zu vermeiden, dass gerade das Ehrenamt zu einem haftungsrechtlichen Risiko für die Verantwortlichen wird. Gleichzeitig muss die Einhaltung des Datenschutzniveaus im Sinne aller Bürgerinnen und Bürgern gewährleistet werden. Hier muss mithilfe der im Laufe der Anwendung der DS-GVO gewonnenen Erkenntnisse auf Dauer ein praktikabler und sinnvoller Ausgleich gefunden werden.

Gerade bei kleinen Unternehmen, deren Datenverarbeitung hauptsächlich im Rahmen von Kundenbeziehungen stattfindet, scheint die Erfüllung der Informationspflichten oft mit unverhältnismäßig hohem Aufwand verbunden oder schlichtweg nicht realisierbar zu sein. Im Rahmen von Unternehmen-Kunden-Beziehungen sind dem beauftragenden Kunden oft viele der informationspflichtigen Daten bereits bekannt. Hierzu wird jedoch selten zum Beispiel die Rechtsgrundlage der Datenverarbeitung zählen. Fraglich scheint allerdings, ob diese bei jeder Auftragserteilung tatsächlich von Interesse ist. Betroffene klagen an dieser Stelle häufig über eine ungewollte Informationsflut. Zu überlegen wäre, ob unter Berücksichtigung des risikobasierten Ansatzes die Beauftragung beispielsweise eines Handwerksbetriebs mit risikoarmer Datenverarbeitung nur erleichterten Regulierungen unterworfen werden sollte.

Das Prinzip „one size fits all“ funktioniert gerade bei den Informations- und Transparenzpflichten in der Praxis nicht. Eine Überlegung wäre daher, ob für Verantwortliche, deren Kerntätigkeit nicht die Datenverarbeitung ist, Ausnahmen geschaffen werden könnten. Unterschiede sind im Alltag auch dort deutlich erkennbar, wo im Rahmen von geschäftlichen Beziehungen viele Informationen bereits vorhanden sind und eine gewisse Augenhöhe der Beteiligten vorherrscht. Bei vielen vertrags- oder vertragsähnlichen Verhältnissen werden Datenschutzvorgaben oft als bürokratische Belastung ohne Mehrwert gesehen.

Informationspflichten müssen „leicht zugänglich“ sein. Hierdurch sollte jedoch gerade kein Informationsüberschuss entstehen, welcher dazu verleitet, die Informationen gar nicht mehr wahrzunehmen, da die Unterscheidung zwischen essentiellen Informationen und solchen, die nicht vorrangig von Interesse sind, schwer fällt. Dies kann im Einzelfall eher zu einem Mangel an als zur Förderung der Transparenz führen. Dieser Entwicklung ist entgegenzusteuern.

Generelle Ausnahmen von Verantwortlichen-Plichten bergen allerdings immer die Gefahr, dem Ziel der Vorschrift selbst zuwider zulaufen. Bei jeglicher erleichternden Änderung müsste daher darauf geachtet werden, die Grenzen so deutlich zu ziehen, dass die eigentliche Zielgruppe der größeren datenverarbeitenden Unternehmen oder Unternehmen mit datenverarbeitender Kerntätigkeit nicht unter die Ausnahmevorschriften fallen können.

Auch die Auskunftspflicht nach Art. 15 DS-GVO stellt Verantwortliche oft vor große Herausforderungen. Teilweise wurde von einer Pervertierung des Auskunftsrechts als Instrument der „Selbstjustiz“ berichtet. Tatsächlich sind - vor allem im Austausch mit öffentlichen Stellen, aber auch in unserer eigenen Arbeit als auskunftspflichtige Stelle – immer wieder Auslegungsfragen vor allem zum Recht auf Kopie begegnet. Hier ist unklar, wie weit dieses reicht und ob mit dem Begriff der „Kopie“ ein Anspruch auf Aushändigung in Papierform eingehergeht. Die Unterscheidung zwischen der „Auskunft über diese personenbezogenen Daten“ nach Abs. 1 S. 1, der Auskunft über „die Kategorien personenbezogener Daten, die verarbeitet werden“ nach Abs. 1 S. 1 lit. b und der „Kopie der personenbezogenen Daten“ nach Abs. 3 S. 1 fällt Verantwortlichen sowohl im öffentlichen als auch im nichtöffentlichen Bereich gleichermaßen schwer.

Lösungsansätze

- Gleichgang der Ausnahmenregelungen der Art. 13 und 14 DS-GVO
- Anhebung oder Differenzierung der Risikostufe in Art. 13 und 14 DS-GVO
- Ausnahmen bei Informationspflichten beispielsweise für die Datenverarbeitung zu privilegierten Zwecken, zugunsten von Unternehmen, deren Datenverarbeitung nicht Zweck der Geschäftstätigkeit ist oder zugunsten der Geheimhaltungsinteressen des Verantwortlichen
- Einführung einer 250-Personen-Grenze (ähnlich Art. 30 Abs. 5 DS-GVO) für Informationspflichten
- Einführung von Definitionen und Differenzierung der Pflichten von Kleinstunternehmen und Kleinen und Mittleren Unternehmen (KMU),
  beispielsweise nach Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Az. K(2003) 1422)
- Streichung des Entstehens der Informationspflichten „zum Zeitpunkt der Erhebung“ für bestimmte Fallkonstellationen
- Zulassung des sog. Medienbruchs für risikoarme Fallkonstellationen und gesetzliche Normierung der notwendigen Informationen im zweistufigen Verfahren
- Änderung der Fristen für die Bereitstellung von Informationen in Alltagsgeschäften unter Berücksichtigung des Zwecks der Regelungen zu Informationspflichten
- Standardisierung von Datenschutzerklärungen auf Internetseiten
- Die „Notwendigkeit“ bei den Informationspflichten von den „jeweiligen Umständen“ abhängig machen, um auf Alltagssituationen eingehen zu können
- Klarstellung, dass eine Angabe einer Kategorie von Empfängern auch ausreichend ist, wenn der Verantwortliche den Empfänger konkret kennt
- Klarstellung des Verhältnisses von Transparenzpflichten und Betriebs- und Geschäftsgeheimnissen
- Begrenzung des Auskunftsanspruchs beispielsweise über eine Verhältnismäßigkeitseinrede, weitere Schärfung der Missbrauchseinrede Art. 12 Abs. 5 S. 2 „bei offenkundig unbegründeten Anträgen“, begriffliche Klarstellung oder Streichung Rechts auf „Kopie“

2. Verarbeitungsverzeichnis

Die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten stellt für kleine und mittlere Unternehmen häufig eine schwer zu bewältigende Herausforderung dar.

Zwar hält die DS-GVO mit Art. 30 Abs. 5 DS-GVO eine Ausnahmevorschrift von der Verpflichtung für Unternehmen oder Einrichtungen bereit, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 DS-GVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO einschließt.

Diese Ausnahmereglung ist für kleine und mittlere Unternehmen allerdings in der Praxis so gut wie nie einschlägig. Die Gegenausnahmen hierzu sind so weitreichend, dass kaum ein Unternehmen von dieser Ausnahme profitiert. Bei der Beschäftigung von etwas weniger als 250 Mitarbeitern ist eine lediglich gelegentliche Verarbeitung personenbezogener Daten kaum möglich. Jeder Betrieb, der Arbeitnehmer beschäftigt, verarbeitet zwangsläufig zumindest deren Daten zur Durchführung des Beschäftigungsverhältnisses - auch Gesundheitsdaten im Rahmen der Fehltageverwaltung oder die Religionszugehörigkeit im Rahmen der Steuerverwaltung. Die Ausnahme scheitert spätestens an der „gelegentlichen“ Verarbeitung im Sinne von „Häufigkeit“. Dies dürfte nicht das gesetzgeberische Ziel gewesen sein. Die einzige Möglichkeit, dieser unerwünschten Folge entgegenzutreten, ist die Einschränkung der Gegenausnahme des Art. 30 Abs. 5 DS-GVO. Bei dieser „missglückten Rückausnahmeregelung“ wird dringend Anpassungsbedarf gesehen.

Der eigentlich vorgesehene risikobasierte Ansatz greift hier nicht durch. „One size fits all“ scheint auch hier nicht zu funktionieren. Für Verantwortliche wäre es nachzuvollziehen, wenn beispielsweise stärker auf eine datenverarbeitende Kerntätigkeit abgestellt würde und für andere Verantwortliche geringere Anforderungen gelten würden, z.B. bei Geschäftsbeziehungen. Hier würde eine Differenzierung anhand der Kerntätigkeit dem eigentlichen Ziel der Vorschrift mehr Rechnung tragen. Im Gegenzug könnte die Schwelle der Mitarbeiterzahl gesenkt werden.

Lösungsansätze

- Ersatz der Häufigkeitsvoraussetzung des Art. 30 Abs. 5 DS-GVO durch Abstellen auf Datenverarbeitung als Kerntätigkeit des Unternehmens (beispielsweise ähnlich Art. 37 Abs. 1 lit. b DS-GVO)
- Schaffung privilegierter Verarbeitungskategorien beispielsweise für Geschäftsbeziehungen
- Sensible Kategorien personenbezogener Daten nach Art. 9 DS-GVO als einzige Rückausnahme
- Erhöhung der Risikostufe

3. Benennungspflicht von Datenschutzbeauftragten

Der Ruf nach der Abschaffung der Benennungspflicht für Datenschutzbeauftragte ist wohl landesweit am häufigsten zu hören. Der Nutzen der Benennungspflicht insgesamt und der Meldepflicht an die Datenschutzaufsichtsbehörden wird häufig in Frage gestellt, vor allem wenn es um kleinere Vereine oder Unternehmen geht.

Das Ziel der Harmonisierung des Rechts auf europäische Ebene wird hier oft als nicht erreicht angesehen. Weite Öffnungsklauseln stehen in der Kritik, unterschiedliche Rechtsanwendung kann bis hin zu Wettbewerbsnachteilen führen. Häufig wird auch hier eine Stärkung des risikobasierten Ansatzes, die Erleichterung für risikoarme Datenverarbeitungen und die Fokussierung auf Qualität und Quantität der Datenverarbeitungen gefordert.

Seit der nationale Gesetzgeber die Anhebung der Personengrenze im Bundesdatenschutzgesetz von zehn auf zwanzig umgesetzt hat, ist es zunächst ruhiger um das Thema geworden. Allerdings werden die Verantwortlichen bald feststellen, dass eine fehlende Benennungs- oder Meldepflicht sie nicht von ihren Aufgaben als datenschutzrechtlich Verantwortliche befreit.

Bei dieser Diskussion ist zu bedenken, dass die Datenschutzbeauftragten für eine kompetente datenschutzrechtliche Beratung sorgen, um Datenschutzverstöße schon im Vorfeld zu vermeiden und nicht zuletzt das Sanktionsrisiko gering zu halten. Oft wird vergessen, dass auch beim Wegfall der Benennungspflicht die Pflichten des Datenschutzrechts bestehen bleiben, die interne Beratung und der angelernte Sachverstand jedoch wegfällt. Ein Wegfall würde kurzfristig als Entlastung empfunden werden, allerdings würde beim Aufkommen der nächsten datenschutzrechtlichen Fragestellung eine interne Rückgriffsmöglichkeit entfallen und der LfDI könnte die Einzelfall-Betreuung sämtlicher Vereine in Baden-Württemberg auch mit massiven Personalaufstockungen nicht gewährleisten.

Die Meldepflicht an die Aufsichtsbehörde ist ebenso kein Selbstzweck. Die grundlegende Abschaffung der Meldepflicht der Datenschutzbeauftragten würde die Kontrolle der Aufsichtsbehörden in diesem Bereich erschweren. Der Meldepflicht kommt zudem eine Selbstkontroll-Funktion - auch hinsichtlich des Aufbaus einer Datenschutzorganisation - zu. Ein Datenschutzbeauftragter stellt die Wahrung der Rechte von Beschäftigten und Bürgern sicher, deren Daten verarbeitet werden. Datenschutzbeauftrage bieten die Chance, Knowhow zu verbreiten, ohne auf eher pauschal arbeitende Dienstleister angewiesen zu sein.

Nach dem auch den Regelungen der Art. 37 ff. DS-GVO zugrunde gelegten risikobasierten Ansatz muss ein Datenschutzbeauftragter nur dann benannt werden, wenn dies wegen des Risikos erforderlich ist. Die Feststellung des Risikos wird allerdings von eher starren Voraussetzungen abhängig gemacht. Dem risikobasierten Ansatz könnte hier durchaus größeres Gewicht verliehen werden.

Bayern hat die Meldepflicht für Amateursportvereine, Musikkapellen und sonstige vor allem durch ehrenamtliches Engagement getragene Vereine aufgehoben. Sollte sich dies als vereinbar mit deutschem und europäischem Datenschutzrecht erweisen, wäre darüber nachzudenken, hier eine gesetzliche Klarstellung solcher Möglichkeiten in den Gesetzestext aufzunehmen, um eine europaweite Erleichterung herbeizuführen. Allerdings müssten Möglichkeiten gefunden werden, wie die Beratung zur Einhaltung der bestehenden Pflichten trotzdem gewährleistet werden könnten, beispielsweise durch Einrichtung einer zentralen Beratungsstelle mit entsprechender Ausrüstung.

Lösungsansätze

- Ausnahmeregelungen für ausschließlich ehrenamtlich tätige, nicht wirtschaftliche Vereine
- Ausnahmeregelungen für Kleinstunternehmen, verbunden mit einer entsprechenden Legaldefinition
- Angleichung der Bestellpflicht im öffentlichen und nichtöffentlichen Bereich, stattdessen Differenzierung der Pflichten anhand von Unternehmensgröße oder Branche
- Einrichtung einer zentralen Beratungsstelle für von der Bestellpflicht befreite Verantwortliche

5. Herstellerhaftung - „privacy by design“

Die DS-GVO stellt mit Privacy by Design / Privacy by Default Grundsätze auf, die sich an Hersteller richten, nimmt Hersteller aber nicht als solche in die Pflicht. Es sollten auch Hersteller, Lieferanten, Importeure, Verkäufer usw. in die Pflicht genommen werden, so wie dies im Produkthaftungsrecht (ProdHaftG bzw. RL 85/374/EWG) bereits der Fall ist.

Beim Begriff „Datenschutz durch Technikgestaltung“ (Privacy by Design), der im Artikel 25 Abs. 1 DS-GVO für den Verantwortlichen vorgeschrieben ist, stellt sich in der Praxis der Adressatenkreis als nicht weitreichend genug heraus. Da Verantwortliche in der Regel nicht selbst Software entwickeln und in weiten Teilen Standard- und Anwendungssoftware von Herstellern bzw. Anbietern, zum Teil sogar von solchen mit globaler, nationaler oder regionaler Monopol- oder zumindest marktbeherrschender Stellung, beziehen und nutzen müssen, läuft diese Forderung häufig ins Leere. Sie sollte daher auch die Hersteller von Software zur Einhaltung dieses datenschutzfördernden Designprinzips verpflichten. In der Praxis trifft dies insb. auf Hersteller von komplexer Software wie z. B. Betriebssystemen, Datenbankmanagementsystemen, Standard-Office-Paketen oder sehr speziellen Fachanwendungen, zu.

Betriebssysteme etwa sind auf dem Markt nur in begrenzter Anzahl vorhanden, sodass Verantwortliche, die Server, Desktop-Computer, Notebooks, Tablets, Smartphones oder ähnliche Geräte betreiben, auf eines derjenigen zurückgreifen müssen. In der Regel sind diese beim Kauf durch den Anwender schon vorinstalliert. Nach derzeitiger Rechtslage ist es die Pflicht der Verantwortlichen, etwaige datenschutzrechtlich relevante Schwachstellen, Fehlkonfigurationen, aus ihrer Sicht unerwünschte Funktionen, etc. zu finden und abzustellen. Den Hersteller trifft keine Pflicht, seine Produkte ohne diese Fehler auszuliefern. Ähnlich verhält es sich in Alltagssituationen, etwa bei haustür-Schließsystemen via Smartphone-App oder anderen „smart home“ Anwendungen. Zwischen der dafür zuständigen App und de m möglicherweise in einem Drittland ohne angemessenes Datenschutz-Niveau befindlichen) Hersteller findet Datenverkehr statt. Setzt ein Unternehmen derartige Systeme ein, ist es selbst Verantwortlicher und muss Datenverarbeitungen verantworten, die es nicht durchschauen kann. Der Hersteller ist nicht effektiv greifbar. Setzt eine Privatperson im Rahmen privat-familiärer Tätigkeit derartige Systeme ein, ist ein Verantwortlicher i.S.d. DS-GVO schon nicht vorhanden. Die Pflichten der DS-GVO treffen niemanden, gehen also ins Leere.

Die bisherige Rechtslage widerspricht dem Ansatz von „data protection by design“ bzw. „by default“. Entgegen Erwägungsgrund 78 S. 4 DS-GVO werden Hersteller in keiner Weise ermutigt, „das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“. Damit bestehen nicht nur erhebliche Lücken im Bereich des Schutzes personenbezogener Daten, sondern es kommt zu einer Potenzierung von technischem und bürokratischem Aufwand bei dem Versuch, dezentral Mängel zu beseitigen, die zentral verursacht werden. Dies belastet alle Verantwortlichen und Auftragsverarbeiter, wobei KMU überproportional belastet werden.

Die Rechtslage widerspricht so auch dem über die RL 85/374/EWG harmonisierten Produkthaftungsrecht. Danach haften Hersteller, Importeure, Lieferanten, etc. für Schäden, die durch ihre Produkte entstehen. Diese bereits harmonisierte Rechtslage müsste in den Bereich des Schutzes personenbezogener Daten zu übertragen werden. Für datenschutzrechtlich relevante Produkte muss daher auch der Hersteller in die Verantwortung genommen werden.

Über die Position der DSK hinausgehend vertritt der LfDI Baden-Württemberg die Auffassung, dass die Durchsetzung einer wie beschrieben angepassten Rechtslage nur dann möglich wäre, wenn die Datenschutz-Aufsichtsbehörden auch zur Kontrolle der Einhaltung des Datenschutzes bei Herstellern, Importeure, Lieferanten, etc. befugt wären.

Lösungsansätze

- Einfügen einer an der Produkthaftungs-Richtlinie orientierten Hersteller-Definition in den allgemeinen Begriffsbestimmungen und Aufnahme in sämtliche Verantwortlichen-Pflichten sowie
- in die Verpflichtungen zur Zusammenarbeit mit den Aufsichtsbehörden und in die Zuständigkeits-, Aufgaben- und Befugnis- Normen der Aufsichtsbehörden sowie in die Sanktionsmöglichkeiten zum Zwecke der wirksamen Rechtsdurchsetzung

5. Unklarheiten bei der Gemeinsamen Verantwortlichkeit, insbesondere im „social media“-Bereich

Das Inkrafttreten der DS-GVO hat insbesondere beim Betrieb von Internetseiten und der Benutzung von sozialen Medien für massive Verunsicherung gesorgt.

Fragen rund um die Gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO sowie der Abgrenzung zur Auftragsdatenverarbeitung nach Art. 28 DS-GVO sind die Folge. Häufig wird im Falle der Ablehnung einer Verarbeitung im Auftrag eine Gemeinsame Verantwortlichkeit unterstellt, die aber regelmäßig nicht vorliegt.

Eine Umfrage meiner Behörde bei den Gemeinden in Baden-Württemberg hat zum Thema „Weitergabe von Online-Nutzungsdaten“ ergeben, dass fast jede Gemeinde eine Website hat und über die Hälfte davon Inhalte oder Elemente von Dritten (z.B. Google/Facebook) in die Seite einbindet. Dies hat oftmals zur Folge, dass das gesamte Nutzungsverhalten von Website-Besuchern an Dritte ohne ersichtliche Rechtsgrundlage weitergegeben wird.

In anderen Konstellationen wird mit der Einwilligung als Rechtsgrundlage gearbeitet. Das eigentliche Ziel des Nutzerschutzes scheint in der Praxis durch Einwilligungs-Buttons und Banner nicht erreicht zu werden, sondern führt im Gegenteil eher zu Abwehrreaktionen. Bei sogenanntem „Tracking“ oder „Targeting“ auf Websites durch Drittanbieterwerkzeuge oder Webanalysetools stellt sich oft die Frage nach der Rechtsgrundlage und der Erfüllung der Informationspflichten.

Gerade beim Betrieb von Seiten auf sozialen Medien stellt sich nach den neusten Entscheidungen des EuGH zur Kategorisierung als Gemeinsame Verantwortlichkeit für die Seitenbetreiber die Frage, wie sie die daraus entspringenden Pflichten realisieren sollen. Oft besteht in der Praxis für die Profil-Inhaber nicht die Möglichkeit, auf die gemeinsame Datenverarbeitung Einfluss zu nehmen und Zweck und Mittel festzulegen, geschweige denn dies transparent zu machen. Selbst wenn die Möglichkeit besteht, ist den gemeinsam Verantwortlichen im Rahmen des Art. 26 ohne weitere Hilfestellung der Aufsichtsbehörde - wie beispielsweise durch unser „Vertragsmuster für eine Vereinbarung nach Art. 26 DS-GVO“ - nicht klar, welche wesentlichen Inhalte festzulegen sind, sodass eine Vielzahl ungenügender Vereinbarungen besteht und Betroffenen die Klarheit über den korrekten Ansprechpartner fehlt. Die Regelung des Art. 26 DS-GVO wird häufig als defizitär beschrieben. Es wird Präzisierungsbedarf auch bezüglich der Transparenzanforderungen sowie des Rechtsverhältnisses der Verantwortlichen untereinander gesehen.

Lösungsansätze

- Klarere Abgrenzungskriterien zwischen Gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO und Auftragsdatenverarbeitung nach Art. 28 DS-GVO
- Klarstellung dahingehend, dass der erfüllte Tatbestand einer Gemeinsamen Verantwortlichkeit keine Rechtsgrundlage für den Datenaustausch zwischen den beteiligten Verantwortlichen darstellt
- Orientierung des Betroffenenrechts anhand der Organisationspflicht und Beschränkung der Reichweite der gemeinsamen Haftung auf ein adäquates Maß

- Klarstellung, dass eine Gemeinsame Verantwortlichkeit für eine gesamte Anwendung oder auch für ein gesamtes Projekt bestehen, daneben aber auch nur einen Teilbereich des gesamten Verarbeitungssystems betreffen kann
- Klarstellung, wann eine Gemeinsame Verantwortlichkeit vorliegen kann, beispielsweise
    - wenn zwei oder mehr Verantwortliche darüber entscheiden, welche Personen an der Datenverarbeitung beteiligt sind und Zugang zu den Daten haben,
    - welche Kategorien von personenbezogenen Daten erhoben werden sollen,
    - wie die personenbezogene Daten erhoben werden sollen,
    - aufgrund welcher Rechtsgrundlage die Datenverarbeitung vorgenommen werden soll,
    - welche technischen und organisatorischen Maßnahmen ergriffen werden sollen,
    - wann personenbezogenen Daten gelöscht werden;
    - den Anlass für eine Datenerhebung geben, oder
    - bei einer gemeinsamen Verarbeitung personenbezogener Daten eigene individuelle Ziele verfolgen
- Klarstellung, dass Gemeinsam Verantwortliche die regelmäßige Überprüfung ihrer gegenseitigen Pflichten vereinbaren können
- Normierung einer der Auftragsverarbeitung ähnlichen Regelung zu den wesentlichen Inhalten einer Vereinbarung zur gemeinsamen Verantwortlichkeit
- Förderung weiterer Guidelines auf europäischer Ebene

Fazit

Bei aller Kritik darf man nicht vergessen, welche Vorteile das neue Datenschutzrecht bietet. Man hat nun, vor allem auch gegenüber anderen Wirtschaftsräumen, ein einheitliches europäisches Instrument. Die Bürgerrechte sind dadurch eindeutig gestärkt worden. Die DS-GVO ist also ein Erfolgsmodell - mit Verbesserungspotenzial.

Die Europäische Kommission braucht für ihre Aufgabe der Fortentwicklung des Datenschutzrechts alle Erfahrungen aus der Anwendung der DS-GVO; nicht nur aus aufsichtsbehördlicher Sicht, sondern umfassend. Hierzu leisten wir einen Beitrag.

Der LfDI ist sich des Umstandes bewusst, dass die Chancen auf tatsächliche Gesetzesänderungen auf EU-Ebene nach den langen Verhandlungen beim Zustandekommen der DS-GVO und den aktuellen Erfahrungen aus den Verhandlungen zur ePrivacy-Verordnung eher begrenzt sind. Nichts desto trotz sehen wir es als unsere Aufgabe, die Anwendung der DS-GVO vor Ort weiterhin zu beobachten und ein offenes Ohr für die Anliegen und Probleme der Verantwortlichen in Baden-Württemberg zu haben - und die so gewonnen Erkenntnisse an die Gesetzgeber im Land, im Bund und in Europa weiter zu tragen.