Sächsischer Landtag
6. Wahlperiode

DRUCKSACHE 6/10629

Antrag

der **Fraktion DIE LINKE.**

Thema: Subsidiaritätsbedenken bezüglich des Vorschlages für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Ratsbeschlusses 2007/533/JI sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011, COM(2017) 352 final

Der Landtag möge beschließen:

I. Der Landtag stellt fest, dass

1. der oben näher bezeichnete Rechtssetzungsvorschlag der Europäischen Union einerseits eine strategische Weichenstellung im Bereich der Entwicklung von IT-Systemen der EU-Mitgliedstaaten und ihrer Regionen im Bereich von Justiz und Sicherheit besonders mit Blick auf Interoperabilität und technische Standards vornimmt und andererseits auch einen Wandel bestehender Konzepte und Praktiken in der Sicherheits- und Justizpolitik zur Folge haben wird;

2. sich der Trend der Digitalisierung im Bereich der Justiz und der Sicherheit auf EU-, Bundes- und Landesebene (z.B. GKDZ, Schnittstellen des Datenaustausches innerhalb der Sicherheitsbehörden und zwischen Polizei und Staatsanwaltschaft bzw. Staatsanwaltschaft und Gericht) und ihre Einbettung in eine elektronische Verwaltung (eGovernance) zukünftig noch erheblich verstärken wird und damit die Voraussetzungen des Artikels 5 EU-Vertrag (besonders das Verhältnismäßigkeitsgebot in Absatz 4) auch aus Sicht der Regionen mit Gesetzgebungsbefugnissen berührt werden;

Dresden, 05.09.2017 - b.w. -

Rico Gebhardt
Fraktionsvorsitzender

Eingegangen am: 05.09.2017 Ausgegeben am: 05.09.2017

3. durch den aus der Digitalisierung hervorgehenden Zwang zu Interoperabilität und Standardisierung der IT- und Datenverarbeitungssysteme eine zentrale Steuerung notwendig ist, die auf EU-Ebene im Bereich von Justiz und Sicherheit wesentlich über die dazu der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (euLISA) zugewiesenen europaweiten Kompetenzen und Befugnisse gesteuert werden soll;

4. im Zuge der Vernetzung der IT-Systeme die mit diesem Rechtssetzungsvorhaben der Europäischen Union angestrebten Veränderungen der Befugnisse und Kompetenzen von euLISA (z.B. bei der nationalen Umsetzung der sog. dezentralen Systeme in den Bundesländern) unausweichlich Bundesrecht aber auch jene Teile des Landesrechtes (angefangen beim Recht auf Datenschutz in Artikel 33 der Verfassung des Freistaates Sachsen, über die Bestimmungen des Sächsischen Datenschutzgesetzes bis hin zum Sächsischen E-Government-Gesetz) berührt sind, die direkt oder indirekt derzeitig in Sachsen die Ausgestaltung der Digitalisierung in diesen Bereichen regeln und daher zwangsläufig deren Anpassung zur Folge haben werden;

5. in dem Verordnungsvorschlag nicht ausreichend begründet wird, warum die Ausweitung der Befugnisse und Kompetenzen von euLISA den Grundsätzen der Subsidiarität und Verhältnismäßigkeit entspricht (S. 17);

6. insbesondere gegen die Einführung eines EU-weiten biometrischen Identitätsmanagements bzw. gegenüber Regelungen zur Dauer der Datenspeicherung verfassungs- und datenschutzrechtliche Bedenken hinsichtlich der Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Regelungen bestehen;

7. die ins Unübersichtliche gestiegene Anzahl von Behörden in den EU-Mitgliedstaaten, die direkt Zugriff auf die von euLISA verwalteten Datensysteme haben sollen bzw. auch die Erlangung von Informationen durch Stellen aus Nicht-EU-Staaten über Mitgliedschaft in anderen Sicherheitsstrukturen wie Interpol indirekt Informationen erlangen können, erhebliche und durchgreifende Zweifel an der Verhältnismäßigkeit der entsprechenden Regelungen in dem Verordnungsentwurf und der Bestimmungen bezüglich der Stellung des Datenschutzes aufkommen lassen;

8. vor dem Hintergrund enormer Investitionen in die IT-Großsysteme und deren Betriebsmanagement durch euLISA (Aufstockung des euLISA-Budgets „um 78 354 Mio. EUR“ [S. 20 des Verordnungsentwurfs]) sowie deren Kompetenzen im Bereich von Pilotprojekten und Forschung, aus denen sich richtungsweisende weitere Vorschläge für zukünftige Entwicklungen ergeben werden und angesichts der Tatsache, dass die demokratische Kontrolle und der Datenschutz nicht annähernd äquivalent ausgestaltet und mitgeregelt werden, sollte dem Europäischen Datenschutzbeauftragten die Teilnahme als Beobachter an den Zusammenkünften der Entscheidungsgremien von euLISA (Verwaltungsrat, Exekutivdirektor) in derselben Weise rechtsverbindlich ermöglicht werden, wie das derzeitig z.B. für Europol und Eurojust vorgesehen ist.

II. Der Landtag fordert die Staatsregierung auf,

1. die in Antragspunkt I. dargestellten (und ihre ggf. eigenen weiteren) Bedenken bei der Behandlung des EU-Rechtssetzungsvorschlages im Plenum des Bundesrates am 22. September 2017 einzubringen;

2. alle Möglichkeiten auf Bundes- und EU-Ebene zu nutzen, die vorgetragenen Bedenken einzubringen und auf eine dementsprechende Änderung dieses EU-Rechtssetzungsvorhabens zu drängen.

Begründung:

Bereits die Verordnung zur Errichtung der Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts[1] war vom Bundesrat mit einem Beschluss[2] ganz grundsätzlich mit Blick auf Subsidiarität und Verhältnismäßigkeit in Frage gestellt worden. Insbesondere wurden in dem Bundesratsbeschluss die mangelnde Begründung der zwingenden Notwendigkeit der Einrichtung einer solchen Agentur, die Kosten-Nutzen-Relation (Verhältnismäßigkeit) und die unzureichende Beachtung des Schutzes von Grund- und Menschenrechten sowie des Datenschutzes hervorgehoben.

So sehr nachvollziehbar ist, dass in Zeiten terroristischer Bedrohungen EU-Sicherheitskonzepte überdacht werden und die sich aus den Fortschritten von Digitalisierung und Informationstechnologie im Bereich von Justiz und Sicherheit ergebende Möglichkeiten zu neuen Ansätzen bei Gefahrenabwehr und Strafverfolgung führen können, kann sich aus dieser neuen Situation von Bedrohungslagen und technischen Möglichkeiten keine Carte blanche für die automatische Umsetzung aller denkbaren technischen Möglichkeiten ergeben nach dem Motto „Was technisch machbar ist, wird umgesetzt."

Eine solche Perspektive stellt sicher die Lobby der IT-Industrie zufrieden, die infolge der immensen Kosten für Hard- und Software und deren Erhaltung den größten Anteil der enormen Investitionssummen erhalten wird (Gesamtkostenrahmen 2018-20 726,488 Mio. Euro). Die Frage bleibt jedoch, ob dieser Investitionsaufwand in einem vertretbaren Verhältnis zu dem erwarteten Sicherheitsgewinn steht. Dem gigantischen Netzwerk von EU-weiten Datenverarbeitungssystemen im Bereich von Sicherheit und Justiz steht derzeit kein auch nur annähernd gleichwertig effektiv funktionierendes System demokratischer, parlamentarisch-öffentlicher Kontrolle entgegen. Stattdessen wird offenbar hauptsächlich auf das Vertrauen in die Agentur euLISA gesetzt.

Hinsichtlich des Datenschutzes ist es notwendig, darauf zu drängen, dass die Kontrolle der Datenverbundsysteme in der Praxis kontinuierlich im Prozess der Entscheidungsfindung in den dafür zuständigen Gremien erfolgt, die erforderliche Transparenz insbesondere zu den kritischen Bereichen (mögliche Fehlerfassung, Nichteinhalten von Löschfristen, mangelnde Kontrolle der Zugriffsberechtigten oder unberechtigte Zugriffe) für die Öffentlichkeit hergestellt wird und die Rolle der Datenschutzbeauftragten und der parlamentarischen Kontrolle dieses exekutiven Handelns von Sicherheitsbehörden bzw. von anderen Stellen,

[1] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung einer Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht
KOM(2009) 293 endg.; Ratsdok. 11722/09.
[2] Drucksache 648/09 (Beschluss) vom 18.09.09.

die mit Daten aus dem Datenverbund arbeiten, effektiv gestärkt wird. Dies könnte z.B. durch die rechtsverbindliche Einrichtung eines Beobachterstatus für den Europäischen Datenschutzbeauftragten in den Entscheidungsgremien von euLISA vergleichbar zu den Befugnissen von Europol und Eurojust erfolgen.

Grundsätzlich handelt es sich bei der zukünftigen Ausgestaltung von euLISA um die Frage demokratischer Grundverfasstheit der EU im Justiz- und Sicherheitsbereich, die oft im Spannungsfeld von Freiheit und Sicherheit verortet wird. Die damit verbundenen Richtungsentscheidungen sind politisch-rechtlicher Natur und dürfen nicht durch Entscheidungen über (dann präjudizierende) technische Entwicklungen ersetzt werden.

Insofern sind die bereits frühzeitig bei der Gründung der Agentur vom Bundesrat im Jahre 2009 zu Recht aufgeworfenen grundsätzlichen Bedenken nach wie vor gültig, insbesondere auch vor dem Hintergrund der Tatsache, dass der Europäische Datenschutzbeauftragte (EDSB) mit seinen in der auf den 2. Mai 2017 (also kurze Zeit vor Übermittlung dieses Verordnungsentwurfes) datierten Stellungnahme zum Schengener Informationssystem vorgetragenen Bedenken ähnlich kritische Fragen aufwirft und den europäischen Gesetzgeber aufgefordert,

> „sich über die derzeitigen Vorschläge hinaus Gedanken über einen kohärenteren, schlüssigen und umfassenden Rechtsrahmen für die IT-Großsysteme der EU für Grenzmanagement und Sicherheit zu machen, der voll und ganz im Einklang mit den Grundsätzen des Datenschutzes steht.“[3]

Als in besonderer Weise bedenklich wird die Entwicklung eines integrierten biometrischen Identitätsmanagements für die gesamte Europäische Union hervorgehoben, die das Schengener Informationssystem (SIS), die Fingerabdruckdatei (Eurodac), die Visumdatenbank (VIS), das dezentrale Europäische Strafregisterinformationssystem (ECRIS) und das (noch nicht beschlossene) Ein-/Ausreisesystem (EES) in einem biometrischen Kerndatensystem verschmelzen soll.

Auch die vom EDSB geäußerten Bedenken hinsichtlich der deutlich angestiegenen Zahl von Behörden, die Zugriff auf die IT-Großsysteme besitzen und deren (fragliche) durchsetzbare Verantwortung und Rechenschaftspflicht für die Verarbeitung personenbezogener Daten nicht ausreichend geklärt ist, treffen auf den vorliegenden Verordnungsvorschlag in gleicher Weise zu.

Die Brisanz dieser kritischen Bedenken wird gerade angesichts der jüngsten Erfahrungen des Missbrauchs supranationaler Sicherheitsinstrumente für die politische Verfolgung missliebiger Personen durch die Türkei im Fall der Vollstreckung eines internationalen Haftbefehls durch Interpol gegen einen betroffenen deutschen Staatsbürger deutlich.

Mit dem beabsichtigten weiteren Ausbau von euLISA wird voraussichtlich auch eCODEX, das IT-Großsystem zum Datenaustausch zwischen Justizbehörden der EU, in die Verantwortung dieser Agentur übergeben (S. 9f.). Es wäre notwendigerweise zu erörtern, inwieweit dabei Fragen der Gewaltenteilung und des nach Bundesrecht wie sächsischem

[3] Stellungnahme 7/2017 Stellungnahme des EDSB zur neuen Rechtsgrundlage für das Schengener Informationssystem vom 2. Mai 2017, veröffentlicht im Amtsblatt der Europäischen Union am 23. Juni 2017.

Landesrecht geltenden Trennungsverbots bei der Datenübermittlung zu beachten sind bzw. eine Datenübermittlung nicht zulässig ist.

Die hier dargestellten Bedenken zum Regelungsinhalt des EU-Rechtssetzungsvorschlages beziehen sich nicht abstrakt auf die EU-Ebene oder das Funktionieren einer Agentur der EU, sondern sie berühren die Interessen Sachsens und geltendes Landesrecht unmittelbar infolge der engen Verflechtung der Sicherheitsstrukturen auf den verschiedenen Ebenen der EU-Governance über zentralisierte und dezentralisierte IT-Systemen im Sinne der Information des Rates der Europäischen Union (vgl. General Secretariat of the Council (2017). Overview of the information exchange environment in the justice and home affairs area. No. prev. doc.: 9368/1/16 REV 1, Brussels, 15 February 2017.) (siehe Anhang).

So ist z.B. das komplexe Vorgangsbearbeitungssystem der sächsischen Polizei, IVO, auch eine Schnittstelle mit Zugriff auf SIS II und damit auf den Großverbund von IT-Systemen unter Kontrolle von euLISA, dessen Interoperabilität und Abgleich von Daten zwischen den Systemen gerade Ziel des vorliegenden Verordnungsentwurfs ist.

Die Entwicklung dieser Software (eine sächsische Eigenentwicklung) in Sachsen unterliegt z.B. notwendigerweise dem Sächsischen Datenschutzgesetz, soweit es um die Übermittlung von Daten geht. Die Datenübermittlung wiederum ist Teil des von euLISA unterhaltenen Systems der IT-Großsysteme, zu dem auch SIS II gehört, auf das sächsische Behörden über IVO zugreifen. Die Regelungen des Verordnungsvorschlages (mindestens) auf den Datenaustausch (Übermittlung von Daten) bezogen, haben offenkundig direkte Bedeutung für das Handeln sächsischer Behörden, deren diesbezüglichen Befugnisse jedoch durch das geltende Landesrecht bestimmt sind (Gesetzmäßigkeit der Verwaltung). Denn

„IVO ist darüber hinaus nicht nur ein komplexes Vorgangsbearbeitungssystem, sondern zugleich die zentrale Datenbank und Täterlichtbilddatei sowie die Schnittstelle zu INPOL und zum Schengener Informationssystem.“ (https://www.polizei.sachsen.de/de/9826.htm)

Damit ist die Übermittlung personenbezogener Daten berührt, die im Sächsischen Datenschutzgesetz im Detail geregelt ist (vgl. § 14 SächsDSG) und dem Schutz des in Artikel 33 der Sächsischen Verfassung verankerten Grundrechts auf Datenschutz dient.

Die Regelungen des Verordnungsentwurfs sind demgegenüber eher vage und unbestimmt. So heißt es in Artikel 7 Absatz 3:

„Die Agentur beschließt geeignete Maßnahmen, darunter auch Sicherheitspläne, unter anderem um das unbefugte Lesen, Kopieren, Ändern oder Löschen personenbezogener Daten während der Übermittlung personenbezogener Daten oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken.“

Auch bevorstehende notwendige Anpassungen des Datenschutzrechts im Zuge der Umsetzung der EU-Datenschutzgrundverordnung werden die sächsischen Standards nicht in der Weise absenken, dass sie es einer EU-Behörde überlassen, Festlegungen zu „geeigneten Maßnahmen“ ohne rechtlich verbindlichen Charakter zu treffen. Eine Aufgabe sächsischer Standards zu Gunsten weniger bestimmter europäischer Standards käme einer Verletzung des Subsidiaritätsprinzips gleich. Auch die Bestimmungen der Artikel 31, 32 und 37 des Verordnungsvorschlages vermögen diese Bedenken nicht auszuräumen.

Im Übrigen wird an dem Regelungsvorschlag in dessen Artikel 7 auch das technokratische Herangehen von euLISA und der Kommission sichtbar: Während eine an Unbestimmtheit nicht zu überbietende allgemeine Regelung „geeignete Maßnahmen“ zum Schutz zu ergreifen in alleiniger Verantwortung von euLISA festlegt, wird in der Verschlüsselung der zu verarbeitenden Daten das technische Heil gesucht. Die Verschlüsselung dient dem Schutz vor nicht autorisiertem Zugriff, also in diesem Sinne vor externen Angriffen. Mindestens ebenso gefährlich sind jedoch die Angriffe von Innen, die mit Verschlüsselungen nicht zu verhindern sind.

Auch Regelungen des Sächsischen E-Government-Gesetzes können von den hier mit Subsidiaritätsbedenken begegneten Regelungen des Verordnungsentwurfs betroffen sein (vgl. §§ 6, 10 SächsEGovG).

Angesichts dieser Ungleichgewichte zwischen enormer technologischer Aufrüstung einerseits und marginalisierter Kontrolle durch Datenschutzbeauftragte und Parlamente und ein unzureichend geregelter Grund- und Menschenrechtsschutz andererseits sowie der erkennbaren direkten Betroffenheit des Freistaates Sachsens muss von der Staatsregierung erwartet werden, diese Bedenken in geeigneter Weise in nationale und europäische Entscheidungen zu diesem Verordnungsentwurf einzubringen.

Anhang:

General Secretariat of the Council (2017). Overview of the information exchange environment in the justice and home affairs area. No. prev. doc.: 9368/1/16 REV 1, Brussels, 15 February 2017.