noyb – Europäisches Zentrum für digitale Rechte
Goldschlagstraße 172/4/3/2
1140 Wien
ÖSTERREICH

STELLUNGNAHME zur Öffentlichen Anhörung
„Innovative Datenpolitik: Potenziale und Herausforderungen“

noyb ist fokussiert auf europaweite Fragen der DSGVO, der Durchsetzung von Datenschutzrechten in der EU bzw. im EWR und kann daher zu innerdeutschen Fragestellungen und Fragestellungen außerhalb der DSGVO nur einen begrenzten Beitrag leisten. Wir erlauben uns daher auf Fragen insbesondere aus dem europäischen Blickpunkt zu antworten:

1) **Mit dem Data Act und dem Data Governance Act (und weitern Rechtsakten) wurde ein wegweisender europäischer Datenraum geschaffen. Welche Spielräume hat der deutsche Gesetzgeber bei der Umsetzung der Vorgaben, die er für eine innovative Datenpolitik nutzen sollte und welche Maßnahmen sehen Sie bei der Umsetzung – etwa in der Bündelung der Aufsicht für die digitalpolitischen Dossiers – als besonders wichtig an?**

   noyb hat begrenzte Erfahrungen im Rahmen des Data Act oder des Data Governance Act.

   In den letzten Jahren kann im Bereich der Aufsicht über z.B. die ePrivacy-Richtline 2002/58/EG und die DSGVO festgestellt werden, dass in vielen Mitgliedsstaaten eine Zersplitterung der Zuständigkeiten herrscht, was zu vielen Parallelverfahren und Verzögerungen führt. Beispielsweise sind folgende Situationen bekannt:

   - Parallele Zuständigkeiten bei denen das Setzen von „Cookies“ von Telekomregulierungsbehörden überwacht wird, die Verarbeitung der im Cookie befindlichen personenbezogenen Daten (also etwa einer UserID) von der Aufsichtsbehörde nach der DSGVO zu beurteilen ist.
   - In Deutschland stellt insbesondere in der Datenschutzaufsicht eine föderale und sektorale Zersplitterung und daraus folgende Parallelverfahren ein großes Problem dar. Obwohl Deutschland umfangreiche Ressourcen zur Verfügung stellt (ca. € 104 Millionen von europaweit € 337 Millionen im Jahr 2022)[1] scheint die Schlagkraft und Geschwindigkeit der Datenschutzbehörden nicht im gleichen Maß ausgeprägt zu sein.

[1] https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf (Seite 7)

- In der EU werden mitunter auch innerhalb von Behörden Fälle getrennt bearbeitet – etwa von einer Abteilung, die für Beschwerden zuständig ist und einer getrennten Abteilung, die (im gleichen Fall) für das Verhängen von Bußgeldern verantwortlich ist. Dies wird mitunter mit verschiedenen Verfahrensrechten begründet, ist jedoch nicht sonderlich effektiv. Eine Anpassung von Verfahrensregeln kann hier Abhilfe schaffen.
- Auch Behörden und Gerichte sind vom Fachkräftemangel betroffen. *noyb* muss europaweit regelmäßig feststellen, dass oft banale Sachverhalte nicht verstanden werden. Gerade die deutsche Gerichtsbarkeit fällt auch durch eine stark zersplitterte Rechtsprechung auf. Datenschutzbehörden berichten mitunter von Gerichten, die Entscheidungen willkürlich aufheben aus einer generellen Ablehnungshaltung der Justiz und der Fachwelt heraus. Die Schnelllebigkeit und ständige Innovation von digitalen Produkten bedürfen kontinuierlich geschulte und verständige Mitarbeitende – oft mit Kompetenzen in mehreren Fachbereichen (wie IT und Recht). Die Unterstützung von Innovation, die schnelle Abwicklung von Verfahren aber auch die Bekämpfung von Rechtsbruch scheitern hieran mitunter.

Mögliche nationale Maßnahmen:

- Generell ist zu beobachten, dass viele EU-Mitglieder diese Probleme erkannt haben und die Zuständigkeit möglichst bei einer Stelle bündeln, wie es etwa im Rahmen der Zuständigkeiten nach der ePrivacy-Richtlinie 2002/58/EG und der Zuständigkeit nach der DSGVO oft schon geschehen ist. Dies kann auch auf neue EU-Rechtsakte ausgedehnt werden. Deutschland hat hier bisher eine andere (insb. föderale) Tradition, die bei globalen digitalen Themen nicht hilfreich erscheint.

- Zentrale, kontinuierliche und hochwertige Schulung und Qualitätssicherung von Mitarbeitenden in Behörden und bei Gerichten scheint in der gesamten EU ein Problem zu sein. Die Vermittlung von Fachwissen und Qualifikation ist Sache jedes Mitgliedsstaats und zeichnet gute Verwaltung aus.

- Neben den Behörden ist vor allem auch die Gerichtsbarkeit mitzudenken, die Sachverhalte faktisch und rechtlich korrekt überprüfen und beurteilen muss. Hier haben sich insbesondere (geschulte) Fachsenate und Sonderzuständigkeiten in der Praxis bewährt, weil damit auch der Schulungsaufwand konzentriert werden kann.

- Nicht zu vernachlässigen ist die Auswirkung von nationalen Zuständigkeiten und Regelungen auf europäische Verfahren. So sind etwa die europäischen Kooperationsmechanismen je nach EU-Rechtsakt unterschiedlich. Nationale Zuständigkeiten (insbesondere in der deutschen föderalen Struktur) sind hier mitunter inkompatibel oder bedürfen zusätzlicher nationaler Kooperation.

- Soweit diese Stellen auch für die Belange des Datenschutzes zuständig sind, ist aufgrund von Artikel 16(2) AEUV und Artikel 8(3) GRCh die Unabhängigkeit der gesamten Behörde sicherzustellen.

2) **Für eine innovative Datenpolitik bedarf es einer innovativen, modernen aber auch sicheren und vertrauenswürdigen Infrastruktur. Was sind zentrale Elemente dieser Infrastruktur, wie muss diese ausgestaltet sein, um eine innovative Datenpolitik zu ermöglichen und wie weit sind wir beim Aufbau einer solchen Infrastruktur und welche Bedeutung kommt hier einer souveränen europäischen Cloudinfrastruktur zu?**

Die Frage einer souveränen europäischen Cloudinfrastruktur ist primär eine wirtschaftspolitische und sicherheitspolitische Frage. *noyb* hat hierzu keine Expertise.

Zur Frage des Zugriffs auf Daten durch Drittstaaten siehe unter Frage 15.

Generell denken wir, dass wir uns in der zweiten von drei Phasen befinden:

- Initial wurden digitale Dienste nicht reguliert.

- In den letzten 10-20 Jahren sehen wir nun massive weltweite Anstrengungen, die Digitalisierung zu regulieren (wie etwa US-Überwachungsgesetze, EU-Marktregularien oder chinesische Abschottungsgesetze). Naturgemäß widersprechen sich diese nationalen und regionalen Regelungen mitunter, was zu einer rechtlichen Zersplitterung führen kann und insbesondere den Handel, Zugriff auf Wissen und die Interoperabilität stören kann. Teile dieser Zersplitterung sind das natürliche Resultat von regulativen Entscheidungen in verschiedenen Systemen und Kulturen und wird – wie auch in anderen Bereichen – nicht vermeidbar sein bzw. explizit gewollt sein (wie etwa „souveräne Infrastrukturen").

- Trotzdem sehen wir mittelfristig großes Potential, dass diese Unterschiede und Hemmnisse mittels internationaler Verträge (zumindest innerhalb der demokratischen Staaten) minimiert werden können, wie etwa durch „No Spy"-Abkommen im Bereich des staatlichen Zugriffs.

3) **Oft wird Datenschutz als Hemmnis für innovative Datenpolitik vorgeschoben oder werden Datenpolitik und Datenschutz gegeneinander in Stellung gebracht. Wie sehen Sie die Rolle des Datenschutzes für eine innovative Datenpolitik, welche Instrumente wie beispielsweise Datentreuhänder können welchen Beitrag leisten, um Datenschutz und innovative Datenpolitik zusammenzudenken und sehen Sie es auch als Wettbewerbsvorteil an, innovative Datenpolitik unter Wahrung des Datenschutzes made in EU sicherzustellen?**

Folgende Elemente können den Rahmen der (nationalen) politischen Spielräume etwas genauer beschreiben:

- Die wenigen „harten roten Linien" der DSGVO (insbesondere in Artikel 5 und 6 DSGVO) basieren auf Artikel 8 und 52 der GRCh und sind – ohne Änderung der EU-Verträge – jedenfalls Basis für jede weiter politische Gestaltung. Spielraum besteht eher bei Dokumentationspflichten und ähnlichem.

- Nach Artikel 6(1) DSGVO ist auch ohne Einwilligung beinahe jede übliche Verarbeitung zulässig (z.B. im Rahmen von Verträgen, gesetzlichen Pflichten oder überwiegenden Interessen, wie etwa für notwendige Beweise). In der Praxis gibt es hier wenig Fälle die nicht sachgerecht abgedeckt werden.
- Lediglich wenn ein Unternehmen auch noch über diesen Rahmen hinausgehen möchte (z.B. für Werbetracking oder für Datenhandel), müssen sie Betroffene um ihre Einwilligung nach Artikel 6(1)(a) fragen. Betroffene können dann ihre Rechte nach der DSGVO freiwillig aufgeben oder auf ihre Rechte bestehen.
- Artikel 23 und 85 DSGVO erlaubt darüber hinaus umfangreiche Ausnahmen für Sicherheit, Forschung, Meinungs- und Informationsfreiheit oder Journalismus.

Der angebliche Konflikt zwischen Datenschutz und „Innovation" stammt nach unserer Praxiserfahrung viel mehr aus banalem „Framing", bei der jegliche (auch problematische) Nutzung von personenbezogenen Daten jedenfalls als „*innovativ*" und jegliche (beabsichtigte, technikneutrale) Regelung als „*innovationsfeindlich*" dargestellt wird.

Wir sehen jedoch mehr „innovative" Unternehmen, die Datenschutz als Teil des Produkts sehen. Beispielsweise können gutes UI/UX-Design etwa mit „*Inline Consent*" (z.B. Schiebereglern an der relevanten Stelle und zum relevanten Zeitpunkt in einer App) Betroffenen eine offene und transparente Wahl geben. Ein proaktives Umsetzen der rechtlichen Regelungen kann nicht nur die Zufriedenheit der Kunden steigern, sondern auch Recht und Produkt in Einklang bringt.

Bisher besteht unseres Wissens zu wenig Evidenz wie diese Ansätze auch wirtschaftliche Vorteile (Vertrauen, positives Image) bieten. Anekdotisch wird dieser Ansatz jedoch regelmäßig als hilfreich bestätigt.

Zu Datentreuhänderschaften haben wir keine Evidenz in der Praxis. Im Rahmen der Prinzipien nach Artikel 5 oder 25 DSGVO scheinen derartige Konstrukte jedoch schon nach dem aktuellen gesetzlichen Rahmen mitunter notwendig.

4) Welche Elemente fehlen in Deutschland auf dem Weg zu innovativer Datenpolitik, wie können weitere Anreize für das Teilen von Daten in wechselseitigem Interesse weiter ausgebaut werden und welche Bedeutung – Stichwort Open Data, Datenlabore und Transparenzgesetz – kommen dem Staat und der öffentlichen Verwaltung zu und werden diese dieser gerecht?

noyb hat zu diesem Thema keine spezifische Expertise.

Generell unterstützt *noyb* das Teilen und Nutzen von öffentlichen Daten. Insbesondere bei Daten, die an sich keinen Personenbezug haben oder (korrekt) anonymisiert sind, verwundern viel mehr regelmäßige Begründungen, dass es datenschutzrechtliche Bedenken gäbe.

In unserer Erfahrung fehlen mitunter landes- und europaweit einheitliche offene Formate, zentrale Portale und Schnittstellen um vorhandenes Potential zu nutzen.

5) **Haben Forschung, Zivilgesellschaft und öffentliche Stellen ausreichend Datenzugang zu den Daten sehr großer Online-Plattformen (VLOPs) und anderen datenhaltenden Unternehmen, um gemeinwohlorientierte Fragestellungen zu Themen wie beispielsweise Klimaschutz, sozialer Gerechtigkeit oder effizienter Verwaltung zu bearbeiten bzw. gibt es weitere Ansatzpunkte im nationalen und EU-Recht, um einen solchen Datenzugang zu gewährleisten und welchen Regelungsbedarf sehen Sie insoweit für die Zukunft?**

noyb hat keine direkten Erfahrungen hierzu, jedoch kann wohl auch hier von der Praxis unter der DSGVO gelernt werden:

- Zugriffsrechte von Betroffenen nach der DSGVO werden in der Praxis weder flächendeckend eingehalten noch durchgesetzt:
  - Intern schätzen wir die Häufigkeit von vollständigen Auskünften nach Artikel 15 auf maximal 5%. Bei etwa 50% aller Anfragen gibt es überhaupt keine substanzielle Antwort, der Rest sind Teilantworten. Problematische oder kritische Punkte (z.B. die Datenquellen oder die Empfänger von Daten, ebenso wie die Logik bei Entscheidungen über Einzelpersonen) werden dabei üblicherweise nicht beantwortet.
  - Die Datenübertragbarkeit nach 20 DSGVO ist in der Praxis nach unserer Erfahrung überhaupt totes Recht.
  - Oft erhält man als zahlender Geschäftskunde von Unternehmen (etwa über Portale oder APIs) mehr Daten zu Betroffenen als über das Auskunftsrecht.
  - Wir haben seit 2018 europaweit keinen einzigen Fall erlebt, bei dem eine Datenschutzbehörde (durch Nachschau) die Einhaltung dieser Rechte effektiv überprüft hat. Bisher beschränken sich Behörden hier auf reine Aktenverfahren (also den Behauptungen der Parteien ob Daten vorliegen oder nicht).

- Wir stellen auch fest, dass sogar im B2B-Bereich die Rechte von Kunden großer Cloudanbieter im Rahmen von Artikel 28 und 20 DSGVO (wonach dem verantwortlichen Endkunden und Cloud-Anbietern als Auftragsverarbeiter) umfangreiche Rechte zustehen, dies in der Praxis mitunter ignoriert werden oder faktisch verunmöglicht werden.

Auf Basis dieser Erfahrung bezweifeln wir, dass VLOPs Zugriffsrechte in anderen Bereichen effektiv umsetzten und diese Umsetzung von den Behörden überprüft wird.

Zu Fragen 6 bis 10:

noyb hat hierzu keine Fachexpertise, bzw. gehen wir davon aus, dass andere Sachverständige hierzu besser berufen sind.

11) Wie sollte, vorangestellt die Zielparameter einer verbesserten Datenverfügbarkeit- und Nutzbarkeit, eine grundlegende Neuordnung der Datenschutzaufsicht in Deutschland aussehen, wo genau sollte eine Reform der DSGVO ansetzen und welche möglichen Restriktionen sehen Sie hierbei?

Zur Reform der Datenschutzaufsicht in Deutschland:

Wir verweisen zur Frage der Bündelung und Schulung auf die Beantwortung von Frage 1.

Darüber hinaus scheinen folgende Elemente im europäischen Kontext reformbedürftig:

- Die Bestellung von Mitgliedern der Datenschutzaufsicht erfolgt in Deutschland zumeist (entgegen Artikel 53(1) DSGVO) nicht „*im Wege eines transparenten Verfahrens*". Zumeist gibt es keine Ausschreibung oder Bewerbungsprozesse – die Stellen werde oft als rein politisches Amt besetzt. Dies scheint mit der Unabhängigkeit der Behörden (von der Politik) nicht in Einklang zu bringen zu sein und ist auch in der Praxis für uns spürbar, da Verfahren nicht nüchtern und neutral abgehandelt werden, sondern stark politisch gedacht wird. Eine Entpolitisierung der Datenschutzaufsicht über transparente und leistungsabhängige Bestellungen wäre leicht zu verankern und ist auch im Rest der EU zumindest formell zumeist gegeben.
- Wir stellen weiterhin fest, dass deutsche Datenschutzbehörden oft eine (europarechtlich nicht vorgesehene) Doppelrolle einnehmen und gleichzeitige „Richter" in Beschwerdeverfahren sind und Unternehmen beraten. Man kann jedoch nicht „Anwalt" und „Richter" zugleich sein. Regelmäßig müssen wir feststellen, dass deutsche Behörden Unternehmen vorab zum von uns beanstandeten Rechtsbruch „beraten" haben und damit befangen sind. In Einzelfällen haben deutsche Behörden Unternehmen sogar zu fraglichem Vorgehen proaktiv aufgerufen. Artikel 57(1)(b) und (d) DSGVO sieht explizit nur eine generelle „Sensibilisierung" oder „Aufklärung" durch Behörden vor, jedoch keine individuelle Beratung. Hier werden umfangreichte öffentliche Ressourcen für Beratung aufgewandt, die an sich Aufgabe des Privatsektors ist. Eine Klarstellung, dass Behörden keine individuelle Beratungsfunktion haben, wäre wünschenswert.
- Ebenso fällt auf, dass die deutsche Datenschutzaufsicht fast durchgängig ihre Entscheidungen nicht veröffentlicht. Für rechtsunterworfene Unternehmen ist es damit schwierig, die Interpretation der Gesetze vorauszusehen, was extreme Rechtsunsicherheit schafft. In Deutschland entstand damit ein „Halbwissen" von Unternehmen und Beratern, die Zugang zu den (eigenen) Entscheidungen haben und das mitunter als Wissensvorteil nutzen. Artikel 65(6) DSGVO verlangt zumindest für Entscheidungen des EDSA die Veröffentlichung. Auch fast alle anderen Mitgliedsstaaten veröffentlichen alle oder alle relevanten Entscheidungen. Deutschland fällt hier aus dem europäischen Rahmen. Eine Veröffentlichungspflicht von Entscheidungen wäre im BDSG leicht zu verankern und würde die Rechtsklarheit deutlich erhöhen.

- Weiters stellen wir fest, dass trotz der Pflicht nach Artikel 83(1) DSGVO „*wirksame, verhältnismäßige und abschreckende*“ Strafen zu verhängen, nach allen bekannten Informationen die Straftätigkeit der deutschen Behörden vernachlässigbar scheint. Ebenso sieht *noyb* für fast alle eingebrachten Fälle in Deutschland „*informelle*“ Lösungen statt einer rechtlich bindenden Entscheidung. Die bisher bestehende Evidenz zeigt,[2] dass genau dieses Vorgehen zu weniger Rechtstreue und damit wieder zu mehr Arbeitsbelastung bei den Behörden führt (ein „Kreislauf des Rechtsbruchs“).
- Wir verweisen auch auf europäische Bestrebungen im Rahmen einer DSGVO-Verfahrensverordnung (siehe Gesetzgebungsverfahren 2023/0202(COD)) und der laufenden europäischen Debatte, ob Konzerne mit Relevanz für die gesamte EU durch eine zentrale EU-Datenschutzbehörde überwacht werden sollen. Damit soll das bestehende Schlupfloch der untätigen Aufsichtsbehörde in Irland geschlossen werden. Auch wenn es bisher hierzu keinen Vorstoß der Europäischen Kommission gibt, scheint diese Debatte weiter zu laufen und mitunter die sachgerechte Lösung zu sein.

Zur Reform der DSGVO und Problemen, die primär in Deutschland gesehen werden:

Die Verfügbarkeit und Nutzbarkeit scheinen in Artikel 5 und 6 DSGVO schon fast deckungsgleich mit den Grenzen von Artikel 8 und 52 GRCh, womit der politische Spielraum (ohne einstimmige Änderung der EU-Verträge) überschaubar bleibt. Die Restriktionen ergeben sich damit schon aus dem EU-Primärrecht.

Wie unter Frage 3 dargestellt, scheint in der deutschen Praxis viel mehr ein Problem des Verständnisses dieser Spielräume vorzuliegen. Hierzu beobachten wir in Deutschland folgende Phänomene:

- Deutschland hat eine ausgeprägte Beratungs- und Rechtsindustrie. Diese scheint oft mehr damit beschäftigt zu sein, vermeintliche Probleme zu finden - um dann hierfür wieder „Lösungen“ anzubieten, als Gesetze mit Augenmaß zu interpretieren. Deutschland sticht hier europaweit mit einer „Liebe zum Problem“ hervor, die uns in der Praxis sonst nirgendwo begegnet. Mit anderen Worten: Erst extreme Auslegungen oder Gedankenspiele führen oft zu den „Problemen“ die dann wieder „gelöst“ werden müssen. Wir denken nicht, dass dies eine Grundlage für Reformwünsche sein sollte.

- Gerichte (und mitunter auch Aufsichtsbehörden) bemächtigen sich der Produkte dieser Gedankenspiele mitunter, um Verfahren fälschlich abzuweisen (so etwa mittels der deutschen Erfindung einer „Erheblichkeitsschwelle“ beim Schadenersatz, die vom EuGH nun als unrechtmäßiger nationaler Alleingang erkannt wurde) oder auch mitunter überschießende Entscheidungen zu treffen. Oft wird im direkten Gespräch klar, dass politische Ansichten (für oder gegen die DSGVO) ausschlaggebend sind und nicht unbedingt nüchterne, rechtliche Analyse (siehe oben zur politischen Bestellung von Entscheidungsträgern).

[2] https://noyb.eu/de/data-protection-day-74-insiders-see-relevant-violations-most-companies

Zu vorhandenen Spielräumen:

Gleichzeitig sehen wir die Möglichkeit für Reformen um sachgerecht zwischen „Big Tech", Mittelstand und Kleinunternehmen zu differenzieren. Schon im Rahmen der DSGVO-Verhandlungen wurde diese Differenzierung diskutiert, aber leider von Unternehmensvertretern blockiert. Gerade Vertreter von Großkonzernen hatten kein Interesse daran, dass die Gesetze für sie strenger wären als für ein EPU. Kenngrößen für eine mögliche Differenzierung müssten hier jedoch etwa die Anzahl der Betroffenen oder die Art der verarbeiteten Daten liefern, nicht die Größe des Unternehmens anhand von Mitarbeitenden oder Finanzzahlen.

Während die Kernbestimmungen der DSGVO durch Artikel 8 und 52 GRCh gedeckt sind und es somit keinen wirklich Spielraum für Abänderungen gibt, sind folgende Bereiche sicherlich reformierbar und würden auch den Großteil der tatsächlichen Belastung für KMUs verringern:

- Eine Verschiebung von Pflichten von KMUs hin zu Anbietern von Cloud- und Softwareprodukten (die tatsächliche Entscheidungsmacht haben),
- eine Limitierung vom internen Dokumentationspflichten,
- erhöhte Rechtssicherheit bei klar legaler Verarbeitung durch europäische Standards und Musterdokumente oder
- eine externe privatwirtschaftliche Datenschutzprüfung statt durch interne Datenschutzbeauftragte

Politisch scheint dies primär über Spezialgesetze (*lex specialis*) möglich, die juristisch unterhalb der DSGVO angesiedelt sind, wie etwa die (geplante) ePrivacy-VO oder die DSGVO-Verfahrensverordnung.

12) Wie kann die Umsetzung von Data Act und AI Act, gerade was die Ermöglichung von KI angeht, durch Standardisierungsarbeiten, Codes of Conducts und Codes of Practices erleichtert werden, insbesondere mit Bedeutung von Transparenz und Kontrolle über Daten?

noyb hat hierzu keine Fachexpertise, bzw. gehen wir davon aus, dass andere Sachverständige hierzu besser berufen sind.

13) Welche Maßnahmen sind aus Ihrer Sicht prioritär, um eine starke Datenökonomie und ein innovatives Daten-Ökosystem mit Rechen- und Datenzentren in Deutschland und Europa aufzubauen und die Ansiedlung von datengetriebenen Unternehmen zu erleichtern?

noyb geht davon aus, dass die Ansiedelung dieser Unternehmen primär von wirtschaftlichen Entscheidungen bestimmt wird, die außerhalb des Datenschutzes liegen (wie z.B. Stromkosten, Bauverfahren, Steuern, Fachkräfteangebot, Gehaltskosten). Immerhin ist die DSGVO europaweit gültig und derartige Investitionen sind europaweit durchaus vorhanden und beachtlich. Zu den wirtschaftlichen Faktoren, welche diese Entscheidungen beeinflussen, hat *noyb* jedoch keine Expertise.

Im Rahmen der DSGVO scheinen vor allem „Pull-Faktoren“ internationale Unternehmen anzuziehen. Fast alle unserer Beschwerden sind gegen Unternehmen, die ihren Hauptsitz in Irland oder Luxemburg haben. Hier liegt die Vermutung nahe, dass Deutschland primär der Konkurrenz („regulatorisches und steuerrechtliches Dumping“) von zwei (kleinen) Mitgliedsstaaten ausgesetzt ist, die EU-Gesetzte nicht durchsetzen und extreme Steuervorteile bieten.

Die prioritäre Maßnahme scheint daher (gemeinsam mit anderen EU-Mitgliedsstaaten) gegen derartige „Schlupflöcher“ in der EU vorzugehen.

14) Wie müssten ideale Leitlinien für die rechtssichere Anonymisierung von Daten im Rahmen der DSGVO und des Data Acts aus Ihrer Sicht ausgestaltet sein? Wie wird die Anonymisierung in anderen EU-Mitgliedsstaaten gehandhabt, und welche Maßnahmen sind erforderlich, damit Deutschland in diesem Bereich endlich Fortschritte erzielt?

Die (korrekte) Anonymisierung ist eine technische Fragestellung, bei der zuvor personenbezogene Daten nicht mehr auf eine Person zurückgeführt werden können und die Person somit nicht mehr „identifizierbar“ ist. Während dies in vielen Fällen einfach möglich ist, bedarf dieser Vorgang besonders bei großen Datenmengen einer guten technischen und organisatorischen Umsetzung.

Während etwa im akademischen Bereich oder bei Forschungsdaten hierzu solide Prozesse bekannt sind, müssen wir in der Praxis feststellen, dass viele Unternehmen diese Möglichkeiten entweder gar nicht nutzen – oder aber nur vermeintlich anonymisierte Daten verarbeiten. Ein typisches Beispiel betrifft internationale Anbieter, die das reine „Hashen“ von Daten als Anonymisierung bewerben und damit auch EU-Geschäftskunden täuschen oder reine Pseudonymisierung mit Anonymisierung verwechseln.

Europaweit ist damit eine (korrekte) Anonymisierung sicherlich ein Bereich, in dem klare technische Vorgaben und „Best Practice“ vielen Unternehmen und staatlichen Stellen eine bessere Nutzung und Weitergabe von Daten erlauben würde.

15) Inwiefern sind die Zweifel an der Rechtssicherheit des Data Protection Agreements zwischen den USA und der EU, das auf zwei vorhergehend aufgehobene Agreements nach dem Schrems I- und Schrems II-Urteil des EuGH folgte, berechtigt und außerdem eine Bremse für Innovationen in Europa und welche Regulierung bräuchte es, um nachhaltig für Rechtssicherheit zu sorgen?

Basis der so-genannten „Schrems I- und II“-Urteile sind die Aufdeckungen von Edward Snowden zu FISA 702 und EO 12.333. Seit 2013 lässt sich (in Bezug auf EU-Bürger und EU-Unternehmen) keine relevante Veränderung beobachten, welche die US-Massenüberwachung nennenswert eingeschränkt hätte.

Wichtig ist, anzumerken, dass FISA 702 für die Anwendung lediglich breit definierte „*Foreign Intelligence Information*“ bei einem US-Cloud oder Telekomanbieter benötigt. Es kann sich hier auch um Geschäftsdaten oder Behördeninformationen handeln. Es handelt sich also insbesondere auch um Informationen die zur Spionage gegen Ziele in der EU genutzt werden können. Ein hinreichender Verdacht auf eine Straftat oder eine richterliche Überprüfung im Einzelfall ist nicht vorgesehen. Durch die besondere Vormachtstellung der USA am EU-Markt ist damit ein extrem tiefgreifender Einblick in europäische Datenbestände möglich.

Konsequenz der (wiederholt) rechtswidrigen Angemessenheitsentscheidungen:

Da die Entscheidungen des EuGH in Schrems I und II *ex tunc* wirken, gab es zumindest zwischen 2000 und Juli 2023 keine Möglichkeit personenbezogene Daten durch eine Angemessenheitsentscheidung in die USA zu übermitteln. Gleiches gilt *de facto* auch für viele Fälle in denen Unternehmen, die unter FISA 702 der US-Massenüberwachung zuarbeiten müssen, sogenannte „Standardvertragsklauseln“ nutzen.

Rechtmäßig dürften nur Übermittlungen gewesen sein, die zwingend notwendig und etwa unter Artikel 49 DSGVO erlaubt waren, Übermittlungen zu Unternehmen in den USA die nicht unter FISA 702 fallen, sowie technisch gesicherte Übermittlungen, wie etwa Durchleitungen bei Ende-zu-Ende-Verschlüsselung.

In der Praxis ergibt sich für den Bereich massive Rechtsunsicherheit, da sich Unternehmen und Betroffene nicht mehr auf den Rechtsbestand des Europarechts verlassen können. Grund hierfür sind weniger die Urteile des EuGH, als die politischen Entscheidungen der EU-Kommission – auch entgegen der Warnungen von Fachbeamten.

Die Rechtsunsicherheit wurde auch dadurch verstärkt, dass Datenschutzbehörden in der gesamten EU die Entscheidungen des EuGH praktisch nicht durchgesetzt haben. Bei Unternehmen entstand damit eine weitere Unsicherheit zwischen Rechtsbestand (der die Übermittlung zumeist illegal machte) und Rechtspraxis (in der der Rechtsbruch von den Behörden toleriert wurde).

Zu den möglichen nachhaltigen Lösungen:

Festzuhalten ist, dass sich die EU und die USA im Bereich des Schutzniveaus gegenüber staatlicher Überwachung (siehe 4. Verfassungszusatz in den USA und Artikel 7 und 8 GRCh) sehr ähnlich sind. Teilweise geht der 4. Verfassungszusatz sogar über das Schutzniveau der GRCh hinaus. Der Konflikt zwischen den Systemen besteht darin, dass EU-Recht als Menschenrecht alle Menschen schützt, während das US-System nur US-Staatsbürger schützt. Der Konflikt besteht also nicht bezüglich des Schutzniveaus, sondern bezüglich der geschützten Menschen.

Eine dauerhafte Lösung kann daher nur darin bestehen, dass beidseitig unabhängig von der Staatsbürgerschaft das Grundrecht auf Privatsphäre geschützt wird. Gelegentlich wird ein solches Vorgehen als „No Spy"-Abkommen beschrieben. Dabei sichern sich Staaten mit ähnlichen Grundwerten (z.B. liberale Demokratien) gegenseitig Schutz ihrer Daten zu – auch um einen freien Datenfluss zu ermöglichen. Erste Ansätze hierfür bestehen in den USA in EO 14086 und auch in Artikel 45 DSGVO. Ein stimmiges System für gegenseitige Garantien fehlt hier jedoch bisher – auch zwischen EU-Mitgliedsstaaten.

Hierfür wäre ein deutlicher innenpolitischer Druck in den USA notwendig. Realistisch scheint dieser nur aus wirtschaftlichen Gründen – etwa bei einer tatsächlichen Durchsetzung der EuGH-Entscheidungen in Schrems I und Schrems II durch die Aufsichtsbehörden, was für US-Unternehmen deutliche wirtschaftliche Nachteile zur Folge hätte, da für US-Cloud-Produkte damit ein großer Markt wegbrechen würde. Die USA verfolgen aktuell ähnliche Strategien gegenüber TikTok oder Huawei, insofern Daten von US-Bürgern von einem möglichen Zugriff durch chinesische Behörden betroffen sind.

16) Wie können Innovationen sowohl im Bereich digitaler Dienste als auch im Bereich Regulierung für mehr Datenschutz und Einhaltung der Grundrechte sorgen und welche guten Beispiele kennen Sie dafür?

Im Bereich der Regulierung stellen wir fest, dass Aufsichtsbehörden im digitalen Bereich selbst oft noch analoge und manuelle Verfahren nutzen und etwa digitale Beweismittel nicht auswerten können und Verfahren nicht automatisiert sind.

In anderen Bereichen (egal ob Finanzverwaltung, Parkraumbewirtschaftung oder Gesundheitsverwaltung) sind in vielen Mitgliedsstaaten deutlich progressivere und modernere Verfahren vorzufinden als etwa vor Datenschutzaufsichtsbehörden, weswegen ein Vergleich mit anderen Rechtsbereichen mitunter sinnvoller scheint.

Im Bereich der Datenschutzaufsichtsbehörden scheinen sich europaweit zumindest eine standardisierte Einbringung (z.B. mittels Beschwerdeformulare), eine moderne Aktenverwaltung und die Nutzung von Textblöcken in wiederkehrenden Entscheidungen durchzusetzen. Die Verknüpfung dieser nationalen Systeme scheitert jedoch aktuell noch. Auch wenn das zwischen den Behörden genutzte europäische „IMI-System" theoretisch Schnittstellen zur Verfügung stellen würde, werden Akten manuell hoch und runtergeladen und gehen regemäßig verloren, auch weil Aktenteile im IMI nach wenigen Monaten gelöscht werden, obwohl Verfahren mitunter Jahre lang dauern. Das EU-Parlament schlägt im Gesetzgebungsverfahren zum DSGVO-Verfahrensrecht[3] nun einen „Joint Case File" vor um bei grenzüberschreitenden Fällen eine zentrale Aktenverwaltung durch die federführende Aufsichtsbehörde zu ermöglichen.

Außerhalb der Behörden scheinen in Kanzleien und NGOs (langsam und schrittweise) „Legal Tech"-Systeme genutzt werden. *noyb* hat selbst etwa über 600 Beschwerde zu rechtswidrigen „Cookie-Bannern" damit effizient betrieben und die entsprechende Software auch Behörden vorgestellt. Trotz großem Interesse gibt es bisher unseres Wissens keine derartigen Anwendungen in den Behörden.

[3] Siehe EU-Verfahren 2023/0202(COD)

Mittelfristig wären eine europaweite Beschaffung und Bereitstellung von spezifischer Software für die Erkennung von Rechtsverletzungen und die Durchsetzung von neuen digitalen Gesetzen wohl sinnvoll. Ein Budget oder eine Zuständigkeit hierfür ist uns jedoch nicht bekannt.

17) **Was kann und sollte Ihrer Auffassung nach der Staat tun, damit die Datenbestände, über die er selbst auf Bundes-, Landes- und kommunaler Ebene verfügt, nicht weiterhin unberührt in Silos schlummern, sondern von der Gesellschaft insgesamt besser genutzt werden können, etwa zum Bürokratieabbau, zu mehr Sicherheit und Komfort beim Nutzen staatlicher Leistungen? Wäre vor diesem Hintergrund das Zusammenlegen einzelner Datenbanken zu einem großen Register ein vernünftiger Weg, und falls ja, wie ließe sich dieser verfassungsfest im Sinne des Föderalismus beschreiten?**

noyb hat zu Fragen des deutschen Föderalismus und Verfassungsrechts keine Fachexpertise. Generell scheinen kleinteilige Strukturen in Deutschland, mangelnde Standardisierung über diese Strukturen hinweg, ein fehlen eine zentralen Beschaffung und aber wohl auch ein Investitionsstau im Bereich der (Verwaltungs-)Digitalisierung nur langfristig und durch grundsätzliche Reformen lösbar.

Die Zusammenlegung aller Daten zu „*einem großen Register*" scheint dabei weder technisch noch organisatorisch sinnvoll. In anderen EU-Staaten sind vor allem folgende Elemente zu sehen:

- Verwaltungsdigitalisierung braucht Mut zur Veränderung von Zuständigkeiten und Verfahrensabläufen, sowie gute Planung um Umsetzung. Es ist nicht sinnvoll ein Papierverfahren zu digital nachzubilden. Hier ergeben sich oft auch Möglichkeiten zur Verwaltungsvereinfachung.
- Interoperabilität, Schnittstellen und einheitliche (Open Source) Software erlaubt auch verschiedenen Rechtsträgern zusammenzuarbeiten, Kosten zu sparen und (notwendige) Daten auszutauschen.
- Gerade Unternehmen, berufsmäßige Vertreter und ähnliche Gruppen werde oft zur digitalen Kommunikation verpflichtet, um Medienbrüche zu vermeiden.
- Die eigene Hoheit über Kernanwendungen muss jedenfalls gegeben bleiben um „Lock-In"-Effekte zu vermeiden und sich von globalen Anbietern nicht erpressbar zu machen (wie aktuell z.B. im Rahmen der „Pflicht" zu Microsoft 365 oder gewissen Konferenz-Lösungen von Behörden oft beklagt).
- Für all das ist eine starke IT-Kompetenz in den öffentlichen Körperschaften nötig.

18) **Die großen Digitalkonzerne zeigen es: Maschinenlesbare Daten haben einen Wert, mit ihrer Monetarisierung werden die zahlreichen Dienste, die unseren Alltag prägen, finanziert. Sollten Ihrer Auffassung nach digitale Daten, die die Menschen alltäglich erzeugen und die gleichsam als Blut der Gesellschaft zirkulieren, auch offiziell einen Wert und damit einen Preis bekommen, und wenn ja, wie ließe sich eine solche Datenökonomie im Wortsinn aufbauen und regulieren? Wie ließe sich die griffige Formel vom „Eigentum an den eigenen Daten" real umsetzen?**

> Die Frage des „*Eigentums an Daten*“ ist zwar oft plakativ proklamiert worden, aber aus gutem Grund global nie umgesetzt worden. Privatsphäre ist ein Grundrecht und Grundrechte sind (mit wenigen Ausnahmen) dem Markt entzogen. Es gibt daher auch kein „*Eigentum am Wahlrecht*“ oder kein „*Eigentum an der Meinungsfreiheit*“.

An einem Datum selbst kann man (je nach anwendbarem Recht) verschiedene Rechte haben. Bei einem einfachen Bild, das mehrerer Personen abbildet, gibt es das „Eigentum“ am Datenträger, verschiedene Immaterialgüterrechte (Urheberrecht an einer Datenbank, Urheberrecht an einem Bild oder Text), klassische Persönlichkeitsrechte (in Deutschland etwa das „APR“) und schlussendlich das Recht der Betroffenen auf Datenschutz. Alle diese Rechte haben aber andere Schutzbereiche und (begründet) differenzierte Einschränkungen.

So sehr ein „*Recht auf Eigentum*“ Betroffenen wohl verständlicher wäre, trägt gerade ein wirtschaftliches Recht wenig zum Schutz der Privatsphäre bei, da es dem Eigentumsrecht (als typisch wirtschaftsliberales Grundrecht) inhärent ist, dass man es fast unbegrenzt verschenken, verwirken oder verkaufen kann – schon im Kleingedruckten von AGB. Das Problem wäre damit ebenso wenig gelöst, wie wenn das Wahlrecht in AGB als Eigentum „*verkauft*“ oder „*überlassen*“ werden könnte. Bei einem solchen System, hätte Meta oder Google schon bald mehrere Millionen Stimmen zum Deutschen Bundestag „*überlassen*“ bekommen.