ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Positionspapier zur zweiten DSGVO-Evaluation (2024)

Mehr Rechtssicherheit für Forschende: Über die Notwendigkeit eines neuen Instruments im Datenschutzrecht

AUTOREN

Dr. iur. Annika Selzer
Fraunhofer SIT | ATHENE

Sarah Stummer, LL.M.
Fraunhofer SIT | ATHENE

Dipl. Jur. Alina Boll
Fraunhofer SIT | ATHENE

Positionspapier zur zweiten DSGVO-Evaluation (2024)

Mehr Rechtssicherheit für Forschende: Über die Notwendigkeit eines neuen Instruments im Datenschutzrecht

Impressum

Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt
© Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Januar 2024

Hinweise
Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Der Beitrag gibt die persönliche Meinung der Autorinnen wieder.

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Autoren

Dr. iur. Annika Selzer
Fraunhofer SIT | ATHENE

Sarah Stummer, LL.M.
Fraunhofer SIT | ATHENE

Dipl. Jur. Alina Boll
Fraunhofer SIT | ATHENE

Zusammenfassung

Bei angewandter Forschung, die sich mit der Aufklärung oder Abwehr von Cyberangriffen beschäftigt, kann es mitunter vorkommen, dass personenbezogene Daten ungeplant verarbeitet werden. Die in der Europäischen Union geltenden Rechtsakte zum Datenschutz sehen für derartige Fälle – in denen also weder planbar ist, ob eine Forschungsaktivität mit einer personenbezogenen Datenverarbeitung verbunden sein wird, noch, welche Kategorien personenbezogener Daten von welchen Gruppen betroffener Personen in welcher Menge verarbeitet werden – keine Möglichkeit vor, diese rechtskonform auszugestalten. Dementsprechend stößt man hier in Bezug auf die Umsetzung geltenden Datenschutzrechts häufig an Grenzen, was die Forschung behindert, so dass Nutzeneffekte nicht erzielt werden können, z.B. zum Schutz Kritischer Infrastrukturen vor Cyberangriffen.

Vor diesem Hintergrund haben ATHENE-Wissenschaftlerinnen im Jahr 2023 das neue Instrument der **Datenschutz-Vorsorge** vorgeschlagen[1] und weiter ausgeführt.[2] Mittels dieses neu vorgeschlagenen Instruments sollen unplanbare und unvorhersehbare, aber hinreichend wahrscheinliche, personenbezogene Datenverarbeitungen rechtssicher ermöglicht werden. Eine ggf. bevorstehende personenbezogene Datenverarbeitung soll mittels des neu vorgeschlagenen Instruments der Datenschutz-Vorsorge vorbereitet werden, indem zunächst Annahmen zu der möglicherweise bevorstehenden personenbezogenen Datenverarbeitung getroffen werden, die als wahrscheinlich anzunehmen sind. Die Annahmen sollen sich hierbei u.a. aus Vorerfahrungen ähnlicher Forschungsaktivitäten ergeben. Auf dieser Basis sollen sodann datenschutzrechtliche Kernaspekte (u.a. die Identifizierung einer einschlägigen Rechtsgrundlage) umgesetzt werden, die in Bezug auf die zuvor getroffenen Annahmen angemessen sind, bevor die geplante Forschungsaktivität aufgenommen wird.

Somit soll die Datenschutz-Vorsorge für eine datenschutzkonforme und rechtssichere Verarbeitung sorgen, falls es im Rahmen der Forschungsaktivität zu einer personenbezogenen Datenverarbeitung kommen sollte. Um die Umsetzung datenschutzrechtlicher Kernaspekte hierbei angemessen zu gestalten, sollen personenbezogene Datenverarbeitungen, deren Eintreten als unwahrscheinlich angenommen wird (nachfolgend kurz „unwahrscheinliche personenbezogene Datenverarbeitungen"), im Rahmen der Datenschutz-Vorsorge unberücksichtigt bleiben.[3] Sollte es dennoch zu einer unwahrscheinlichen, personenbezogenen Datenverarbeitung kommen, soll diese nicht bußgeldbewehrt sein. Perspektivisch ist die Anwendbarkeit der Datenschutz-Vorsorge auch außerhalb der Forschung grundsätzlich denkbar und hierfür sehen wir tatsächlich auch einen realen Bedarf.

Das vorliegende Positionspapier schlägt deshalb vor, das Instrument der Datenschutz-Vorsorge in der Europäischen Datenschutz-Grundverordnung zu verankern. Nur durch diesen Schritt könnte die Datenschutz-Vorsorge bewirken, dass geltendes Recht und der technische Fortschritt sinnvoll ineinandergreifen und somit einen verbesserten Schutz für die Gesellschaft bewirken. Denn würde die Datenschutz-Vorsorge Teil des europäischen Datenschutzrechtssystems werden, würde sie

- einerseits für datenschutzrechtlich Verantwortliche Klarheit bieten, um unvorhersehbare und unplanbare personenbezogene Datenverarbeitungen rechtssicher umsetzen zu können und
- andererseits einen – wie in der DSGVO vorgesehenen – angemessenen Schutz für die Rechte und Freiheiten der betroffenen Personen bewirken.

[1] Boll/Selzer/Spiecker gen. Döhmann, Tagesspiegel Online.
[2] *Boll/Selzer*, DuD 2024; *Boll/Stummer*, DuD 2024; *Boll/Stummer/Selzer*, DuD 2024; *Boll*, DuD 2024.
[3] Für die drei ersten Absätze *Boll/Selzer*, DuD 2024.

1. Einleitung

Die Datenschutz-Grundverordnung – kurz: DSGVO – wird im Jahr 2024 zum zweiten Mal evaluiert. Im Rahmen dieser Evaluation legt die Europäische Kommission dem Europäischen Parlament und dem Rat der Europäischen Union einen Bericht über die Überprüfung der DSGVO vor, in dem u.a. geeignete Vorschläge zur Änderung, Anpassung und/oder Ergänzung der DSGVO unterbreitet werden, welche u.a. die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft berücksichtigen (Art. 97 DSGVO).

Wir möchten diese Evaluation zum Anlass nehmen, auf einen aus unserer Sicht bestehenden Ergänzungsbedarf der DSGVO aufmerksam zu machen.

2. Problemstellung

Der Europäische Verordnungsgeber gibt durch die DSGVO einen Regelungsrahmen für fast jede denkbare Form der Verarbeitung personenbezogener Daten – also der Verarbeitung von persönlichen Informationen von Menschen, wie z.B. dem Namen, der Anschrift oder dem Beruf eines Menschen – vor. Hierbei geht der Europäische Verordnungsgeber davon aus, dass jede personenbezogene Datenverarbeitung vor deren Beginn vorhersehbar und im Detail planbar ist. Dies entspricht jedoch – insbesondere in der Cybersicherheitsforschung – vielfach nicht mehr den tatsächlichen Gegebenheiten, weil eine personenbezogene Datenverarbeitung im Rahmen der hier betrachteten Forschung häufig nicht beabsichtigt wird, jedoch das Eintreten einer solchen Datenverarbeitung nicht gänzlich ausgeschlossen werden kann und somit nicht immer planbar ist.[4]

Der treibende Gedanke, sich mit diesem Thema zu beschäftigen, kam aus der Betrachtung eines Beispiels, bei dem ein Cybersicherheitsforschender im Darknet zu neuen Angriffsmethoden recherchiert, um ggf. Gegenmaßnahmen zu entwickeln. Hierbei kann es vorkommen, dass der Cybersicherheitsforschende bei seiner Recherche ungeplant Listen mit gestohlenen personenbezogenen Daten aus Cyberangriffen auffindet. Um Schlimmeres zu vermeiden, informiert er die in der Liste enthaltenen Personen, damit diese ggf. Gegenmaßnahmen ergreifen können (z.B. Zurücksetzen des Passworts).

Da für den Cybersicherheitsforschenden in solchen Fällen vor Verarbeitungsbeginn weder ersichtlich ist, ob personenbezogene Daten verarbeitet werden, noch wie viele personenbezogene Daten welcher Art und welcher betroffenen Personen (und somit der Schutzbedarf) sicher feststellbar ist, ist auch die Umsetzung datenschutzrechtlicher Anforderungen im Vorfeld grundsätzlich nicht konkret planbar. Sofern eine personenbezogene Datenverarbeitung jedoch nicht vorhersehbar und planbar ist, ist sie nach geltendem Recht nicht rechtskonform umsetzbar. Insofern stehen Forschende in derartigen Fällen vor einem Dilemma, im Rahmen ihrer Forschung ggf. gegen geltendes Datenschutzrecht zu verstoßen.

Trotz des hohen Nutzens, den der Cybersicherheitsforschende durch derartige Arbeiten erzielen kann, bewegt er sich in einer rechtlichen Grauzone. Das Wissen über diese rechtliche Grauzone kann dazu führen, dass derartige Forschungsaktivitäten – auch wenn sie Mehrwerte erzeugen – aus Angst vor rechtlichen Konsequenzen unterbleiben.[5]

Um derartige Forschung auch in Zukunft zu ermöglichen, ist es somit notwendig, das geltende Recht an tatsächliche Gegebenheiten der Forschung anzupassen und auf ihre Bedürfnisse zu reagieren. Konkret besteht der dringende Bedarf, einen eindeutigen und rechtsicheren Rahmen für unvorhersehbare und unplanbare personenbezogene Datenverarbeitungen zu schaffen, der diese Datenverarbeitungen einerseits rechtskonform umsetzbar macht, ohne hierbei andererseits in unangemessener Weise die Rechte und Freiheiten betroffener Personen einzuschränken.

[4] *Boll/Selzer*, DuD 2024.
[5] Boll/Selzer/Spiecker gen. Döhmann, Tagesspiegel Online.

Auch wenn der Bedarf – wie hier beschrieben – aus einem Beispiel der Cybersicherheitsforschung abgeleitet wurde, ist es wichtig zu betonen, dass ein Bedarf, unvorhersehbare und unplanbare Datenverarbeitungen rechtskonform zu ermöglichen, auch außerhalb dieser und anderer Forschung besteht.

3. Lösungsvorschlag

Vor diesem Hintergrund bedarf es aus unserer Sicht im europäischen Datenschutzrechtssystem eines neuen Instruments, mit dessen Hilfe unvorhersehbare und unplanbare personenbezogene Datenverarbeitungen ermöglicht werden sollen, ohne die Rechte und Freiheiten betroffener Personen hierbei unangemessen einzuschränken. Dieses Instrument bezeichnen wir als „Datenschutz-Vorsorge" oder kurz „DS-V".

Mittels der DS-V soll eine ggf. bevorstehende – unvorhersehbare und unplanbare – personenbezogene Datenverarbeitung vorbereitet werden, indem zunächst Annahmen zu der möglicherweise bevorstehenden personenbezogenen Datenverarbeitung getroffen werden, die als hinreichend wahrscheinlich anzunehmen sind. Im Falle der Forschung können sich Annahmen hierbei u.a. aus Vorerfahrungen ähnlicher Forschungsaktivitäten oder aufgrund der Kenntnisse des Mediums, das zur Forschungsaktivität eingesetzt wird („welche Daten welcher betroffenen Personen könnten gewöhnlich im Darknet in Folge eines Datendiebstahls zu finden sein?"), ergeben. Auf dieser Basis sollen sodann datenschutzrechtliche Kernaspekte umgesetzt werden (u.a. bedarf es der Identifizierung einer einschlägigen Rechtsgrundlage, der Umsetzung technischer und organisatorischer Maßnahmen sowie der Umsetzung von Informationspflichten), die in Bezug auf die zuvor getroffenen Annahmen angemessen sind, bevor die personenbezogene Datenverarbeitung eventuell erfolgt.

Sollte eine personenbezogene Datenverarbeitung erfolgen, die im Rahmen der vorbereitenden Datenschutz-Vorsorge nicht als hinreichend wahrscheinlich angesehen wurde, dann soll der Umstand, dass diese konkrete Datenverarbeitung ohne eine vorbereitende Datenschutz-Vorsorge erfolgte, nicht bußgeldbewehrt sein.

Die DSGVO besteht aus derzeit insgesamt 99 einzelnen Artikeln, wobei jeder Artikel einen eigenen Themenbereich (z.B. die Bedingungen an eine Einwilligung) regelt. Konkret schlagen wir eine Ergänzung der DSGVO durch einen neuen Artikel vor, der das neue Instrument der DS-V rechtsverbindlich festschreiben würde. Da die einzelnen Artikel der DSGVO in übergeordnete Kapitel unterteilt werden (z.B. werden die Bedingungen an eine Einwilligung in dem Kapitel „Grundsätze" geregelt), sollte ein solcher neuer Artikel nicht als neuer Artikel 100 eingefügt werden. Stattdessen sollte ein solcher neuer Artikel, mit „a" hinter einer Artikelnummer versehen, in einem passenden Kapitel als neuer Artikel ergänzt werden, und zwar so, dass eine möglichst passende, logische Reihenfolge der Artikel innerhalb dieses Kapitels entsteht. Vor diesem Hintergrund schlagen wir eine Regelung der DS-V als neuen Artikel 36a[6] DSGVO vor.

Der hier vorgeschlagene Artikel 36a DSGVO verfolgt zwei gleichwertig wichtige Ziele:

1) Er soll datenschutzrechtlich Verantwortlichen Klarheit darüber verschaffen, dass unvorhersehbare und unplanbare personenbezogene Datenverarbeitungen rechtssicher umsetzbar sind.
2) Er soll den datenschutzrechtlich Verantwortlichen im Rahmen unvorhersehbarer und unplanbarer personenbezogener Datenverarbeitungen zur Umsetzung von Maßnahmen verpflichten, die einen angemessenen Schutz der Rechte und Freiheiten der von einer ggf. erfolgenden personenbezogenen Datenverarbeitung betroffenen Personen bewirken sollen.

Hierfür müsste in dem Artikel 36a DSGVO zunächst geregelt werden, wann eine Organisation, die für eine personenbezogene Datenverarbeitung verantwortlich ist (aus datenschutzrechtlicher Sicht „der Verantwortliche"), eine DS-V verpflichtend durchzuführen hat. Dies soll insbesondere dann der Fall sein, wenn eine personenbezogene Datenverarbeitung nicht vorhersehbar, nicht planbar, aber hinreichend wahrscheinlich ist.

[6] Diese Verortung erscheint ideal, da die DS-V somit auf das Instrument der Datenschutz-Folgenabschätzung folgen würde – einem Instrument, das gewisse Ähnlichkeiten mit der DS-V aufweist.

In absoluten Ausnahmefällen, in denen eine personenbezogene Datenverarbeitung einen sehr großen Schaden für betroffene Personen bedeuten könnte (z.B. bei einer potenziellen Verarbeitung von Informationen über Personen im Zeugenschutz), soll eine Datenschutz-Vorsorge auch durchgeführt werden, wenn die Datenverarbeitung unwahrscheinlich ist.

Dies könnte in der DSGVO wie folgt normiert werden:[7]

Vorschlag eines Artikels 36a Absatz 1 DSGVO
(1) Ist eine personenbezogene Datenverarbeitung
a) nicht vorhersehbar und
b) nicht planbar und
c) hinreichend wahrscheinlich
hat der Verantwortliche eine Datenschutz-Vorsorge durchzuführen.
In Ausnahmefällen hat der Verantwortliche eine Datenschutz-Vorsorge auch durchzuführen, wenn die personenbezogene Datenverarbeitung nicht vorhersehbar und nicht planbar sowie unwahrscheinlich ist, jedoch voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte. Für mehrere ähnliche Verarbeitungsvorgänge mit gleichen Zwecken kann eine einzige Datenschutz-Vorsorge umgesetzt werden.

Innerhalb einer verantwortlichen Organisation wird die Umsetzung datenschutzrechtlicher Anforderungen häufig an diejenigen Mitarbeitenden delegiert, die mit der Ausführung der konkreten personenbezogenen Datenverarbeitung betraut wurden. So wird z.B. häufig die Umsetzung datenschutzrechtlicher Anforderungen im Rahmen des Bewerbungsprozesses an die Mitarbeitenden der Personalabteilung delegiert. Jedoch kennen sich diese Mitarbeitenden nicht immer tiefgreifend mit dem datenschutzrechtlichen Rahmen aus.

Da sowohl die Entscheidung über die Durchführungspflicht einer DS-V als auch die Durchführung der DS-V fundierte datenschutzrechtliche Kenntnisse voraussetzt, ist darüber hinaus zu regeln, dass der Datenschutzbeauftragte – also der Mitarbeitende, der innerhalb der verantwortlichen Organisation u.a. Empfehlungen zur Datenschutzumsetzung gibt und datenschutzrechtliche Vorgaben intern überwacht – in diese Schritte einzubinden ist.

Dies könnte in der DSGVO wie folgt normiert werden:

Vorschlag eines Artikels 36a Absatz 2 DSGVO
(2) Der Verantwortliche holt sowohl bei der Frage nach der Durchführungspflicht als auch bei der Durchführung der Datenschutz-Vorsorge den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

Datenschutzaufsichtsbehörden kommt u.a. die Aufgabe zu, für bestimmte Pflichten der DSGVO zu konkretisieren, in welchen Fällen (bzw. bei welchen Vorgängen, bei denen es zu einer personenbezogenen Datenverarbeitung kommt) die jeweilige Pflicht der DSGVO besteht. Dies ist insbesondere dann wichtig, wenn die Entscheidung über die Durchführungspflicht komplex ist und die verantwortlichen Organisationen somit ggf. vor (zu große) Schwierigkeiten stellt.[8] Dies kann auch bei einer DS-V angenommen werden, sodass die jeweils zuständige Datenschutzaufsichtsbehörde die verantwortlichen Organisationen mit einer Liste unterstützen soll, die typische Vorgänge beinhaltet, für die eine Pflicht zur Umsetzung einer DS-V besteht.

Da es innerhalb Europas mehr als eine Datenschutzaufsichtsbehörde gibt, haben diese auf die einheitliche Anwendung der DSGVO – und somit auch auf eine einheitliche Anwendung der Pflicht zur Umsetzung einer DS-V – hinzuwirken. Dies geschieht im sogenannten Kohärenzverfahren.

[7] Um den Wortlaut der DSGVO im Rahmen des Formulierungsvorschlags möglichst getreu zu übernehmen, lehnt sich der vorliegende Formulierungsvorschlag an den vorhandenen Formulierungen des Art. 35 DSGVO an und übernimmt diese teilweise wörtlich, sofern diese im Einzelnen auch auf die DS-V übertragen werden können.
[8] Vor diesem Hintergrund veröffentlichten Datenschutzaufsichtsbehörden bereits Listen mit Verarbeitungsvorgängen, für die eine Pflicht zur Umsetzung einer sogenannten Datenschutz-Folgenabschätzung besteht. Bei der Datenschutz-Folgenabschätzung handelt es sich um ein bereits in der DSGVO geregelten Instruments des Datenschutzrechts für besonders risikoreiche personenbezogene Datenverarbeitungen.

In der DSGVO könnten diese Inhalte wie folgt normiert werden:

Vorschlag eines Artikels 36a Absatz 3 DSGVO
(3) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Vorsorge durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Liste dem in Artikel 68 genannten Ausschuss. Sofern einschlägig, hat dies im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 zu erfolgen.

Die eben dargestellte Herausforderung hinsichtlich der Entscheidung über die Durchführungspflicht einer DS-V seitens der verantwortlichen Organisation könnte des Weiteren durch eine Liste der zuständigen Datenschutzaufsichtsbehörde unterstützt werden, die typische Vorgänge beinhaltet, für die keine Pflicht zur Umsetzung einer DS-V besteht.[9]

Dies könnte in der DSGVO wie folgt normiert werden:

Vorschlag eines Artikels 36a Absatz 4 DSGVO
(4) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Vorsorge erforderlich ist. Die Aufsichtsbehörde übermittelt diese Liste dem in Artikel 68 genannten Ausschuss. Sofern einschlägig, hat dies im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 zu erfolgen.

Darüber hinaus müsste geregelt werden, welche Pflichten im Rahmen der Durchführung einer DS-V konkret bestehen. Wie bereits in Art. 36a Abs. 1 DSGVO erläutert, sollen im Rahmen einer DS-V i.d.R. nur solche personenbezogenen Datenverarbeitungen berücksichtigt werden, die zwar unplanbar und unvorhersehbar, aber dennoch hinreichend wahrscheinlich sind. Insofern sollte im Rahmen einer DS-V zunächst beschrieben werden, im Rahmen welcher Tätigkeiten eine personenbezogene Datenverarbeitung ggf. zu erwarten ist und warum diese ggf. zu erwarten ist (z.B. weil es in vergleichbaren Forschungsaktivitäten bereits in der Vergangenheit zu ähnlichen personenbezogenen Datenverarbeitungen kam). Sodann sind für diese wahrscheinlichen Datenverarbeitungen wichtige Kernaspekte des Datenschutzrechts vorbereitend umzusetzen, um aus datenschutzrechtlicher Sicht darauf vorbereitet zu sein, dass es später ggf. zu einer personenbezogenen Datenverarbeitung kommen wird.

Die Umsetzung erfolgt auf Basis von Annahmen, die sich u.a. aus Vorerfahrungen mit ähnlichen Kontexten ergeben können. So wären auf Basis dieser Annahmen u.a. angemessene technische und organisatorische Maßnahmen zu implementieren.

Dies könnte in der DSGVO wie folgt normiert werden:

Vorschlag eines Artikels 36a Absatz 5 DSGVO
(5) Die Datenschutz-Vorsorge enthält zumindest Folgendes:
a) eine umfassende und systematische Beschreibung der geplanten Tätigkeit, insbesondere hinsichtlich des Zwecks der Tätigkeit sowie ihrer Notwendigkeit;
b) die Identifizierung von einschlägigen Rechtsgrundlagen gemäß Artikel 6 bis 10 sowie gegebenenfalls die Umsetzung von Verträgen gemäß Artikel 26 Absatz 1 und Artikel 28 Absatz 3 und die Umsetzung der Voraussetzungen der Artikel 44 bis 50;
c) die Identifizierung und gegebenenfalls die Umsetzung von Informationspflichten gemäß Artikel 13 oder 14;
d) die Identifizierung und gegebenenfalls die Umsetzung technischer und organisatorischer Maßnahmen gemäß Artikel 25 und 32;
e) erforderlichenfalls die Datenschutzbetreuung im Wirkbetrieb, welche insbesondere
- die Überwachung der tatsächlichen Datenerhebung, den Abgleich mit der prognostizierten Datenerhebung und gegebenenfalls die Dokumentation unerwarteter Datenverarbeitungen gemäß Artikel 5 Absatz 2,

[9] Auch diese Listen werden bereits im Rahmen der Datenschutz-Folgenabschätzung geregelt (siehe Fußnote 8). Im Gegensatz zu den Listen, die typische Vorgänge beinhalten, für die eine Pflicht zur Umsetzung einer Datenschutz-Folgenabschätzung besteht, ist die Veröffentlichung einer Liste mit Vorgängen, für die keine Pflicht zur Umsetzung besteht, nicht verpflichtend. Insofern liegt es im Ermessen der Aufsichtsbehörden, ob sie eine derartige Liste veröffentlichen möchten. Diesem Vorgehen folgen wir im Rahmen unseres Vorschlags zur Regelung des Instruments der DS-V.

- die Überwachung des Bestehens und gegebenenfalls die Umsetzung von Rechten der betroffenen Person gemäß Artikel 12 und 15-22,
- die Überwachung der Umsetzung von Informationspflichten gemäß Artikel 13 oder 14, der Umsetzung von Löschfristen sowie der Umsetzung und gegebenenfalls Anpassung technischer und organisatorischer Maßnahmen gemäß Artikel 25 und 32 sowie
- die Überwachung des Bestehens und gegebenenfalls den Umgang mit einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 und 34 umfasst;
f) eine Dokumentation der in Absatz 5 Buchstabe a-e genannten Schritte gemäß Artikel 5 Absatz 2.

Um den Risiken für die Rechte und Freiheiten der von einer personenbezogenen Datenverarbeitung (potenziell) betroffenen Personen angemessen begegnen zu können, sollte wann immer möglich eine kleine Anzahl potenziell betroffener Personen (oder ihrer Vertreter) in die DS-V eingebunden werden, um ihren Standpunkt zur ggf. bevorstehenden Datenverarbeitung einzuholen und im weiteren Verlauf der Umsetzung einer DS-V berücksichtigen zu können. Dies ist jedoch regelmäßig nur sinnvoll möglich, wenn sich der Kreis potenzieller betroffener Personen eingrenzen lässt. Dies wäre z.B. der Fall, wenn eine unplanbare und unvorhersehbare Datenverarbeitung grundsätzlich nur die Nutzer eines bestimmten sozialen Netzwerkes betreffen könnte. In diesem Fall ließe sich der Standpunkt einiger Nutzer des sozialen Netzwerkes einholen.

Dies könnte in der DSGVO wie folgt normiert werden:

Vorschlag eines Artikels 36a Absatz 6 DSGVO
(6) Sofern sich der Kreis potenzieller betroffener Personen eingrenzen lässt, holt der Verantwortliche gegebenenfalls den Standpunkt von potenziell betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

Die DSGVO regelt in Art. 30 eine Pflicht zur Umsetzung einer umfangreichen Dokumentation, die bei unplanbaren und unvorhersehbaren Datenverarbeitungen i.d.R. nicht oder nur unvollständig umgesetzt werden könnte. Insofern bedarf es für unplanbare und unvorhersehbare Datenverarbeitungen einer Ausnahmeregelung dieser Pflicht.

Dies könnte in der DSGVO wie folgt normiert werden:

Vorschlag eines Artikels 36a Absatz 7 DSGVO
(7) Artikel 30 Absatz 1 und Absatz 2 findet mit der Maßgabe Anwendung, dass die in dem Verzeichnis von Verarbeitungstätigkeiten enthaltenen Angaben durch den Verantwortlichen und gegebenenfalls durch den Auftragsverarbeiter nur im bereits bekannten Umfang aufzuführen sind.

Mit der vorgeschlagenen Ergänzung eines Artikels 36a DSGVO gingen weitere, geringfügige Änderungsbedarfe der DSGVO einher, u.a. müsste Art. 83 Abs. 5 DSGVO, der den Bußgeldrahmen gegen bestimmte Verstöße gegen die DSGVO umfasst, um Verstöße gegen den neuen Art. 36a DSGVO ergänzt werden, so dass im Ergebnis Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden könnten, wenn eine DS-V (bei Einschlägigkeit der neuen Vorschrift) nicht durchgeführt würde. Hierbei ist zu beachten, dass für nicht vorhersehbare, nicht planbare und nicht hinreichend wahrscheinliche personenbezogene Datenverarbeitungen keine Pflicht zur Durchführung einer DS-V bestehen soll. Sollte eine derartige Verarbeitung unerwarteterweise doch erfolgen, so soll dies nicht bußgeldbewehrt sein.

Weiterer Ergänzungsbedarf besteht u.a. für eine Legaldefinition für unvorhersehbare und unplanbare Datenverarbeitungen (Art. 4 DSGVO), die Ergänzung der Aufgaben des Datenschutzbeauftragten (Art. 39 Abs. 1 lit. c DSGVO) und die Ergänzung der Aufgaben der Aufsichtsbehörden (Art. 57 Abs. 1 lit. k DSGVO).[10]

[10] Siehe hierzu und zu dem Vorschlag des Art. 36a DSGVO im Detail *Boll/Stummer/Selzer*, DuD 2024.

4. Relevanz jenseits der Forschung

Nur durch ein wie hier beschriebenes Umdenken im Datenschutzrecht hin zur DS-V kann letztlich sichergestellt werden, dass (einschlägige) Forschung rechtssicher durchgeführt werden und unsere Gesellschaft langfristig von den Vorteilen dieser Forschung profitieren kann.

Doch – wie bereits skizziert – ist die Cybersicherheitsforschung zwar der Impulsgeber der DS-V, jedoch kann das Instrument der DS-V zukünftig auch darüber hinaus relevant werden; so sind entsprechende Anwendungsmöglichkeiten – insbesondere vor dem Hintergrund des technischen Fortschritts – u.a. im Zusammenhang mit anonymisierten Datensätzen, die bereits teilweise de-anonymisiert wurden denkbar.

5. Fazit

Das in der Europäischen Union geltende Datenschutzrechtssystem sieht derzeit keine Möglichkeit vor, unvorhersehbare und unplanbare, jedoch hinreichend wahrscheinliche personenbezogene Datenverarbeitungen rechtssicher auszuführen. Dies wäre jedoch dringend nötig, um u.a. Arbeiten zur Cybersicherheitsforschung rechtssicher durchführen zu können und somit den hohen gesellschaftlichen Nutzen dieser Forschung aufrechterhalten zu können.

Die Datenschutz-Vorsorge würde hierbei Abhilfe schaffen: Durch die rechtsverbindliche Regelung der Datenschutz-Vorsorge in der DSGVO wäre es möglich, für derartige Datenverarbeitungen die rechtliche Grauzone aufzulösen und Rechtssicherheit zu schaffen. Gleichzeitig wären die Rechte und Freiheiten der betroffenen Personen angemessen geschützt.

6. Zum Weiterlesen

Für einen detaillierten Überblick über das vorgeschlagene Instrument wird auf folgende Beiträge verwiesen (in chronologischer Reihenfolge):

Alina Boll, Annika Selzer, Indra Spiecker gen. Döhmann: Datenschutz in der offensiven Cybersicherheitsforschung, über: https://background.tagesspiegel.de/cybersecurity/datenschutz-in-der-offensiven-cybersicherheitsforschung.

Annika Selzer: Umbruch im Datenschutz – Datenschutzvorsorge in der Cybersicherheitsforschung, Verifizierung von Anonymität und Berücksichtigung der Nutzerbedürfnisse, GI Informatik 2023, S. 705-713.

Annika Selzer, Indra Spiecker gen. Döhmann, Alina Boll: Datenschutzvorsorge in der offensiven Cybersicherheitsforschung – Datenschutzkonforme Verarbeitung in Fällen unvorhersehbarer Datenverarbeitungen, DuD 2023, S. 785–789.

Alina Boll und Annika Selzer: Die Datenschutz-Vorsorge (DS-V) – Systematisierung eines neuen Instruments für das Datenschutzrecht, DuD 2024, S. 44-48.

Alina Boll, Sarah Stummer: Erste Schritte im Rahmen der Datenschutz-Vorsorge – Beschreibung und Rechtsgrundlagen, DuD 2024, S. 118-124.

Alina Boll, Sarah Stummer, Annika Selzer: Datenschutz-Vorsorge – Anwendbarkeit jenseits der Forschung und Einbettung in das geltende Datenschutzrecht, DuD 2024 (in print).

Alina Boll: Weitere Schritte im Rahmen der Datenschutz-Vorsorge – Informationspflichten, TOMs, Dokumentation und Betreuung (Schritte 3-6 der DS-V), DuD 2024 (in print).

Alina Boll: Die Datenschutz-Vorsorge in der offensiven Cybersicherheitsforschung – Eine erste exemplarische Umsetzung in Form eines Planspiels (under review).

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit