

Politikbrief Sommer 2024

Liebe Leserinnen und Leser

Europa hat gewählt. Als Vorsitzender des Berufsverbands der Datenschutzbeauftragten Deutschlands und gleichzeitig als Präsident des europäischen Dachverbands European Federation of Data Protection Officers EFDPO beglückwünsche ich alle gewählten Abgeordneten zur Wahl und freue mich auf die Zusammenarbeit. Lassen Sie uns in Brüssel, Straßburg und vor Ort die Weichen für eine erfolgreiche und sichere Digitalisierung Europas stellen.

Ein wichtiges Thema dabei ist der Umgang mit Künstlicher Intelligenz: Um die Chancen der KI für die europäische Wirtschaft zu nutzen und die schutzwürdigen Interessen auf Privatsphäre und Datenschutz der Bürgerinnen und Bürger zu wahren, brauchen wir eine schlagkräftige Aufsicht. Diese muss sowohl personell als auch fachlich gut ausgestattet sein, um mit den rasanten Entwicklungen Schritt halten zu können. Wer im komplexen Zusammenspiel von sektoralen Zuständigkeiten und föderalen Strukturen – gerade in Deutschland – die KI-Governance ausfüllen soll, ist noch ungeklärt.

Es wird Sie nicht überraschen, dass wir als Datenschutzbeauftragte den Schutz personenbezogener Daten, aber auch von Geschäftsgeheimnissen als grundlegenden Bestandteil des europäischen Rechts- und Lebensmodells verstehen. Die DSGVO gilt weiterhin uneingeschränkt – und muss eingehalten werden. Wir wollen Menschen und Unternehmen vor den Risiken unzulässiger Datenverarbeitungen schützen. Dafür stehen wir als Datenschutzbeauftragte. Dazu ist es von kleinen Betrieben bis zu großen Konzernen und in Behörden wichtig, die Datenschutzbeauftragten bei Training, Entwicklung und Nutzung von KI frühzeitig einzubinden.

Für die Unternehmen bedarf es im Umgang mit KI-Produkten Klarheit, rechtlich verbindliche Handlungslinien und Beratung. Dazu brauchen wir voraussichtlich viele talentierte Fachleute – denn es wird gar nicht so leicht sein, tausende neue KI-Beauftragte für Unternehmen und Behörden zu finden. Hier könnten Datenschutzbeauftragte mit ihrem jahrelangen Wissen um die Prozesse in den jeweiligen Organisationen eine wichtige Schnittstelle sein.



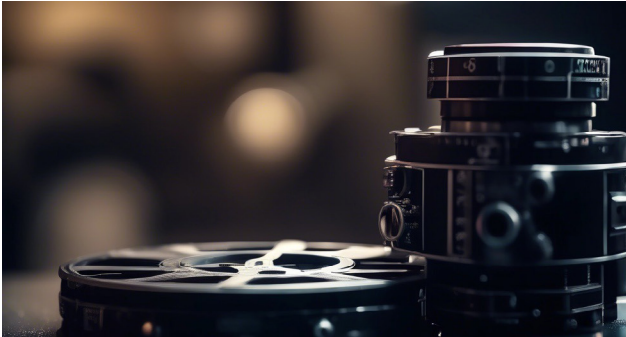
So wie auch die Aufsichtsbehörden in Bund und Land ebenso in die Lage versetzt werden müssen, ihrer Beratungsfunktion gerecht zu werden.

Apropos: An dieser Stelle möchte ich auch dem scheidenden Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Prof. Ulrich Kelber, für die stets inspirierende Arbeit danken und wünsche seiner Nachfolgerin Prof. Dr. Louisa Specht-Riemenschneider alles Gute.

Sehr geehrte Abgeordnete des Europäischen Parlaments und des Bundestages: Lassen Sie uns gemeinsam über diese zentralen Fragen diskutieren und von der praktischen Erfahrung der Datenschutzbeauftragten in vielen tausend Unternehmen profitieren. Wir wünschen Ihnen einen guten Start in Brüssel, einen ebenso schönen Sommer und eine interessante Lektüre.

Ihr Thomas Spaeing
Vorstandsvorsitzender

Compliance und Beratung durch Datenschutzbehörden erweitern



Die Beratungsangebote im Bereich Datenschutz müssen europaweit ausgebaut werden. Diese Forderung basiert auf der Beobachtung, dass die Datenschutzaufsichtsbehörden ihrer gesetzlichen Verpflichtung zur Aufklärung und Sensibilisierung für den richtigen Umgang mit Daten derzeit nicht ausreichend nachkommen können.

Datenschutzaufsichtsbehörden sollen in die Lage versetzt werden, umfassende Beratungsdienste anzubieten. Ein erweitertes Beratungsangebot würde dazu beitragen, die allgemeine Sensibilisierung und Aufklärung im Bereich Datenschutz zu erhöhen und dadurch Unsicherheiten wie auch Risiken abzubauen.

Ein zentrales Anliegen der Datenschutzbeauftragten ist dabei die Bewertung komplexer Datenverarbeitungsmodelle, die insbesondere für Startups eine große Herausforderung darstellt. Viele neue Geschäftsmodelle basieren auf innovativen Datenverarbeitungstechniken, die oft-

mals weitreichende datenschutzrechtliche Implikationen haben. Ohne adäquate Beratung durch die Datenschutzaufsichtsbehörden bleibt diesen Unternehmen häufig nur ein Ansatz des „trial & error“. Dies bedeutet, dass Unternehmen wiederholt Versuche unternehmen müssen, um die Einhaltung der Datenschutz-Grundverordnung (DSGVO) sicherzustellen, was ineffizient und risikoreich ist – und Digitalisierung und Innovation lähmen kann. Sogenannte Regulatory Sandboxes verzerren die Compliance und bereiten nicht auf die datenschutzrechtliche Wirklichkeit vor – und werden deshalb vom BvD abgelehnt.

Aktuell sind viele Unternehmen unsicher, wie sie die gesetzlichen Vorgaben korrekt umsetzen können. Durch gezielte Beratung könnten Missverständnisse ausgeräumt und Fehler vermieden werden, was letztlich zu einer insgesamt höheren Compliance, schnellerer Umsetzung und zu einem besseren Schutz der Daten der Bürgerinnen und Bürger führen würde – auch vor dem Hintergrund des Zusammenspiels unterschiedlicher digitalpolitischer Rechtsakte der letzten Jahre.

Darüber hinaus könnten präventive Beratungsangebote langfristig zu einer Entlastung der Datenschutzaufsichtsbehörden führen. Wenn Unternehmen bereits im Vorfeld datenschutzrechtliche Anforderungen verstehen und umsetzen, reduziert sich das Risiko von Datenschutzverletzungen und damit auch der Bedarf an nachträglichen Prüfungen und Sanktionen. Dies würde Behördenkapazitäten freisetzen, um sich auf besonders kritische Fälle zu konzentrieren und die generelle Effizienz der Datenschutzüberwachung zu steigern.

Zertifizierungen: Europaweite Standards schaffen



Die Ausbildung sowie die beruflichen und fachlichen Kenntnisse der Datenschutzbeauftragten sind sowohl national als auch europaweit sehr heterogen. Dies ist zunächst einmal eher ein Vorteil, denn um beispielsweise dem schnellen digitalen Wandel und der zunehmenden Automatisierung durch KI zu begegnen, braucht es unterschiedliche Fachrichtungen und Kenntnisse aus IT, Recht, Prozessberatung und nicht zuletzt Branchenkenntnis und Kommunikationskompetenz.

Bei aller Vielfalt braucht es aber auch ein gewisses Maß an Einheitlichkeit der Kompetenznachweise. Eine europaweite Zertifizierung mit verbindlichen Standards würde Unternehmen die Auswahl der geeigneten Beratung erleichtern und den Datenschutzbeauftragten eine Leitlinie geben, ihre Weiterbildung zu planen und zu aktualisieren.

Für einen nachvollziehbaren, sicheren und erfolgreichen Umgang mit Daten muss die nächste Legislaturperiode genutzt werden, um europaweite Standards zu entwickeln und zu etablieren. In vielen Fällen gibt es bereits erprobte Verfahren, die nur noch politisch reguliert werden müssten.

In Deutschland hat der BvD mit DPO-Cert ein Konzept für eine Personenzertifizierung von Datenschutzbeauftragten vorgelegt und ermöglicht mit dem Beruflichen Leitbild seit vielen Jahren eine Selbstverpflichtung auf Qualitätsstandards, die aktiv gelebt und nachprüfbar sind. Europaweite Standards sollten sich daran orientieren – der BvD und sein europäischer Dachverband EFDPO sind hier bereits in Gesprächen mit den nationalen Datenschutzverbänden in der EU und jederzeit gesprächsbereit, um das Modell vorzustellen.

Bei Datenpannen den DSB einbinden senkt Risiken und Bürokratie

Die frühzeitige Einbindung des Datenschutzbeauftragten ist immer sinnvoll und reduziert meist die Prozesskosten. Nicht zuletzt, aber vor allem bei der Bewältigung von datenschutzrechtlichen Vergehen. Hier wäre mit einem einfachen Kniff eine deutliche Effizienzsteigerung möglich und Unternehmen sowie Behörden deutlich von Bürokratie zu entlasten.

Ein Beispiel gefällig? Datenpannen sind unverzüglich und innerhalb von 72 Stunden an die zuständige Datenschutzbehörde zu melden. Diese Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzaufsichtsbehörde stellt sowohl die Unternehmen als auch Aufsichtsbehörden vor erhebliche Probleme und Aufwände. Zum überwiegenden Teil geht es hier um

weniger schwerwiegende Fälle wie die Offenlegung von E-Mail-Adressen durch offene Verteiler, Infektionen mit Schadsoftware auf einfachen Arbeitsplätzen oder Adressverwechslungen.

Bei diesen minderschweren Vergehen sollte die Dokumentation der Panne ausreichen und die Meldepflicht an die Behörden entfallen. So könnte man mit einfachen Mitteln sowohl Unternehmen als auch Auf-

sichtsbehörden entlasten, ohne das Schutzniveau zu verringern.

Die in Art. 33 Abs. 5 DSGVO vorgesehene Dokumentation einer jeden Verletzung des Schutzes personenbezogener Daten könnte zur Entlastung des Unternehmens so ausgestaltet werden, dass der DSB dieses Register der „Datenpannen“ führt und die vom Verantwortlichen festgelegten Abhilfemaßnahmen überwacht.

Was muss konkret angepasst werden?

Art. 33 DSGVO muss dahingehend angepasst werden, dass der Datenschutzbeauftragte nach ausführlicher Dokumentation, Zusammenstellung sowie Bewertung des Vorgangs entscheiden kann, ob ein meldepflichtiger Vorfall vorliegt. Dies würde eine zusätzliche Harmonisierung mit § 65 BDSG bringen. Dieser Paragraph sieht vor, dass eine Meldung nur notwendig ist, wenn die Verletzung voraussichtlich eine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat.

BvD-Verbandstage: Ulrich Kelber absolviert letzten öffentlichen Auftritt



Die Eröffnungsreden der BvD-Verbandstagen gehören traditionell der Politik und den großen Leitlinien. Mehr als 250 Teilnehmende erlebten den letzten öffentlichen Auftritt von Prof. Ulrich Kelber als Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Der Schwerpunkt seiner Rede galt dem Datenschutz durch Anonymisierung oder

Pseudonymisierung. Hier seien entscheidende Potenziale noch nicht gehoben. Das Löschen des Personenbezugs, also die Anonymisierung, schafft Freiräume für Forschung und ist ganz entscheidende Schnittstelle zur Verbindung von Datennutzung und Datenschutz. Dem landläufigen Vorurteil, dass der Datenschützer den digitalen Wandel bremsen will, hält Kelber entschieden dagegen: „Wir sind pragmatische Digitalisierungsfans.“ Gerade weil Datenschützer den Prozess zu Ende denken und auf rechtliche Schwachstellen hinweisen würden, unterstützten sie Digitalisierungsprozesse und damit die Unternehmen.

Zum Ende des Monats wird Ulrich Kelber von Louisa Specht-Riemenschneider abgelöst.

Auch ein anderer langgedienter Vertreter des Datenschutzes gab sich vor seinem Ausscheiden das Stelldichein. „Pirat“ Patrick Breyer, der aus persönlichen Gründen nicht mehr für das Europäische Parlament kandidiert hatte, hielt eine vielbeachtete Keynote.

Kern dessen war ein Bericht über die aktuellen Diskussionspunkte zwischen Europäischem Parlament und Kommission, wie die Chatkontrolle oder den Digitalen Euro. Während Breyer das anlasslose Mitlesen von digitaler Kommunikation nicht nur als groben Eingriff in die Bürgerrechte sieht, zeigte er auch eindrücklich, dass andere Techniken Kriminalität im Netz viel wirkungsvoller verhindern können. Security by Design und das Löschen von Inhalten gehören beispielsweise für den Piratenpolitiker dazu, denn: „Massenüberwachung ist nicht das Modell der Freiheit“. Ebenso forderte er noch einmal eine rasche Einführung der ePrivacy-Verordnung, die mehrere Jahre im Verzug, aber weiterhin bitter notwendig sei, so Breyer.

Am Ende seines Berichts hielt der Digitale Freiheitskämpfer ein flammendes Plädoyer für die digitale Selbstbestimmung eines ganzen Kontinents – und für Europa, auch wenn die politischen Auseinandersetzungen meist ermüdend, manchmal desillusionierend gewesen sind.

Eine ausführliche Eventzusammenfassung sowie die Reden von Thomas Spaeng oder Sergey Lagodinsky in vollem Umfang gibt es [hier](#).

Das waren die BvD-Verbandstage 2024



Das waren unsere BvD-Verbandstage 2024 in Berlin. Weitere Impressionen und Videos von der Veranstaltung finden Sie [hier](#).



Positionspapiere

Papier zur Europawahl

Nach der Wahl 2024 steht Europa an einer entscheidenden Marke für den Umgang mit Bürgerrechten im Zeitalter und der Zukunft des Datenschutzes. Der BvD hat dazu fünf zentrale Forderungen vorgelegt.

► [Download](#)

Benennung von Datenschutzbeauftragten – Unabhängigkeit nur mit Bindung für die Ewigkeit möglich?

In diesem kompakten Positionspapier erläutert der BvD, warum kurze Befristungen der Benennung von Datenschutzbeauftragten in den meisten Fällen für einen effektiven Datenschutz schädlich sind.

► [Download](#)

Europas KI-Dilemma: Digitale Souveränität löst viele Probleme

Der BvD unterstützt den Vorschlag, den deutschen Datenschutzaufsichtsbehörden die Aufgabe als Marktüberwachungsbehörde nach der KI-Verordnung (AI Act) zu übertragen. Um eine Anwendung der Verordnung zu sichern, ist diese Übertragung der Zuständigkeit sinnvoll. Mit der Zuständigkeit der Datenschutzaufsichtsbehörden nach der KI-Verordnung können zudem weitere Parallelstrukturen und damit zusätzlicher Bürokratieaufwand vermieden werden.

► [Download](#)

KONTAKT



Thomas Spaeing
Vorstandsvorsitzender
thomas.spaeing@bvdnet.de



Karsten Füllhaase
Geschäftsführer
karsten.fuellhaase@bvdnet.de

BvD-Geschäftsstelle
Budapester Straße 31
10787 Berlin
T 030 26 36 77 60

@ [@bvd@privacyofficers.social](https://www.instagram.com/bvd@privacyofficers.social)

[linked.com/company/berufsverband-der-datenschutzbeauftragten](https://www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten)

IMPRESSUM

Herausgeber
Berufsverband der
Datenschutzbeauftragten Deutschlands (BvD) e. V.
Budapester Straße 31, 10787 Berlin
www.bvdnet.de
bvd-gs@bvdnet.de

Redaktionsschluss
3. Juli 2024

Redaktion, Produktion, Satz & Layout
KING CONSULT | Kommunikation, Berlin
www.king-consult.de