Fokus Datenschutz - Datenstrategie der Bundesregierung

Donnerstag, 28. Januar 2021

Datenstrategie der Bundesregierung

Kabinettfassung, 27. Januar 2021
Datenschutzrelevante Aussagen

Analysiert von www.Datenschutz-Dialog.de by www.Tele-Media.de
Fragen? Frage-Datenstrategie-FokusDatenschutz@dadi.de
Version: 210128

Quelle:
https://www.bundesregierung.de/resource/blob/992814/1845634/5bae389896531854c579069f9a699a8f/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1

Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum

Fokus Datenschutz

Chancen ergreifen: Daten zugänglich machen, nutzen und teilen

Seite 6
Es sollen datengestützte Innovationen und Dienste ermöglicht und gleichzeitig bei personenbezogenen Daten der hohe und weltweit angesehene Datenschutzstandard Europas und Deutschlands gehalten werden.

Verantwortung – Chancen nutzen, Risiken begegnen

Seite7
Der Datenschutzstandard in Europa bietet ein starkes Fundament, auf dem diese Strategie aufsetzt. Unter einer verantwortungsvollen Datennutzung verstehen wir dabei aber nicht nur die Einhaltung des Rechtsrahmens, sondern auch die Orientierung an zentralen ethischen Grundsätzen und Prinzipien sowie die Berücksichtigung der nach dem Stand der Technik erarbeiteten Qualitäts- und Sicherheitskriterien.

Ein hohes Datenschutzniveau kann sogar ein Innovationstreiber werden und maßgeblich für den Erfolg einer digitalen Technologie sein, weil es das Vertrauen in diese erhöht.

Weiterentwicklung

Seite9
Wir sind davon überzeugt, dass wir dank der Maßnahmen der Datenstrategie unsere europäischen Werte, unsere Vorstellungen von Datenschutz und Souveränität im Zeitalter von globalem Datenverkehr und Vernetzung durchsetzen können und unsere Art des Umgangs mit Daten so Vorbild werden kann.

I. Das Fundament: Dateninfrastrukturen leistungsfähig und nachhaltig ausgestalten

Seite11
Hinzu kommt, dass Daten nur dann bereitwillig von den Akteurinnen und Akteuren eines → Datenökosystems geteilt und genutzt werden, wenn die Dateninfrastruktur sicher und vertrauenswürdig ist und die Sicherheit der Daten gewährleistet ist, insbesondere dass Datenschutz und IT-Sicherheit von vornherein technisch in Produkte und Prozesse eingebaut werden.

2.1 Regulierung: Verbesserung der Rahmenbedingungen

Seite16
Diese Rechtsunsicherheit gilt es, insbesondere auch durch untergesetzliche Maßnahmen, weiter

abzubauen, um eine einheitliche Datenschutzpraxis zu etablieren.

2.1.1 Rahmenbedingungen bei personenbezogenen Daten

Wo stehen wir?

Die Europäische Union hat daher mit der Datenschutz-Grundverordnung (DSGVO) im Jahr 2016 die datenschutzrechtlichen Vorgaben neu geregelt und einen an die Digitalisierung angepassten hohen EU-weit einheitlichen Datenschutzstandard geschaffen.

Die DSGVO dient mittlerweile auch in Staaten außerhalb der EU als Vorbild für (neue) Datenschutzgesetze. Auf Bundes- und Landesebene wurde die DSGVO durch bereichsspezifische Datenschutzgesetze ergänzt.

Aufgrund der Komplexität des spezifizierenden Datenschutzrechts werden personenbezogene Daten aus Sorge vor Sanktionen in Deutschland jedoch in vielen Fällen nur eingeschränkt verarbeitet und datenbasierte Projekte nicht umgesetzt.

Seite17
Die DSGVO stellt die Verpflichtung zum Datenschutz auch durch Technikgestaltung auf.

Widersprüchlich interpretierte Datenschutzvorgaben können dazu führen, dass das für die Forschung produktive Kombinieren von Daten unterschiedlicher Quellen gehemmt wird.

Die Datenschutzaufsicht besteht in Deutschland aus dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (zuständig unter anderem für Bundesbehörden, für die Finanzbehörden hinsichtlich der Verarbeitung personenbezogener Daten im Anwendungsbereich der Abgabenordnung und für Telekommunikations- und Postunternehmen) und 17 Landesdatenschutzbeauftragten , die die Einhaltung des Datenschutzrechts im öffentlichen und nicht-öffentlichen Bereich landesspezifisch beaufsichtigen. Zusammen bilden sie die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), die eine Vereinheitlichung der Rechtsauslegung der Aufsichtsbehörden fördern soll.

Dennoch kann die Rechtsauslegung divergieren. Wir werden prüfen, ob und in welcher Form Optimierungen zur Verbesserung bei der Koordinierung der einheitlichen Durchsetzung des Datenschutzrechts notwendig sind.

Das divergierende Datenschutzverständnis verschiedener Aufsichtsbehörden innerhalb der EU kann ebenfalls Herausforderungen für eine harmonisierte Rechtsanwendung und für mehr europäische → Datensouveränität hervorrufen.

Was wollen wir erreichen?

Wir wollen den verantwortungsvollen Umgang mit personenbezogenen Daten in Deutschland stärken und die Durchsetzung des geltenden Datenschutzrechts sicherstellen.

Wir wollen das Regelungsfeld Datenschutzrecht zusammen mit allen Verantwortlichen unter Beibehaltung des bestehenden Datenschutzniveaus einheitlicher und widerspruchsfreier gestalten.

Hierzu gehört u.a. die mögliche Einführung einer federführenden Datenschutzaufsicht für länderübergreifende Forschungsvorhaben analog zu den bestehenden Regelungen des Gesundheitsdatenschutzes.

Seite18
Wir prüfen dazu auch, ob und wie die Datenschutzaufsicht für den nicht-öffentlichen Bereich verbessert werden kann.

Wir werden bei den Ländern dafür werben, das Datenschutzrecht unter Beibehaltung des bestehenden Datenschutzniveaus insbesondere für den Forschungsbereich länderübergreifend einheitlicher zu gestalten. Eine Harmonisierung im europäischen Datenschutz streben wir mit der e-Privacy-Verordnung an, die den besonders wichtigen Schutz der Privatsphäre in der elektronischen Kommunikation verbessern soll.

Es gibt jedoch auch Bereiche, in denen eine Nutzung persönlicher Daten ohne hinreichende datenschutzrechtliche Legitimation erfolgt. Hiergegen wollen wir weitere Lösungen zum Schutz von Verbraucherinnen und Verbrauchern entwickeln.

Eine einheitliche Rechtsauslegungspraxis ist auch für die Sicherstellung des geltenden Sozial- und Beschäftigtendatenschutzes oder, insbesondere in Bezug auf Gesundheitsdaten von Bedeutung. Schließlich werden wir breiter über die datenschutzrechtlichen Gestaltungsrechte informieren und Projektansätze fördern, die dazu hilfreich sein können.

Der Schutz personenbezogener Daten muss von Anfang an, also bereits bei der Entwicklung von Produkten und Dienstleistungen, berücksichtigt werden. Hier können technische Standards bzw. Normen unterstützend wirken. Zudem sind die Beschaffungsrichtlinien für die öffentliche Hand entsprechend anzupassen.

Um das Datenschutzrecht sicherzustellen und die Interessen von Verbraucherinnen und Verbrauchern zu wahren, wollen wir Datenmanagementsysteme bzw. Personal Information Management Systems (PIMS) etablieren (vgl. Kapitel 2.3).

Die Digitalisierung und der zunehmende Einsatz neuer Technologien wie Künstlicher Intelligenz in der Arbeitswelt führen dazu, dass mehr personenbezogene Daten anfallen und verarbeitet werden. Dem Beschäftigtendatenschutz kommt dabei eine grundlegende Rolle zu, die Daten von Arbeitnehmerinnen und Arbeitnehmern zu schützen, ihr Vertrauen in neue Technologien wie Big Data und Künstliche Intelligenz zu stärken und so den Weg in eine Datenökonomie zu ermöglichen. Klare, handhabbare Regelungen zum Beschäftigtendatenschutz sorgen zudem für mehr Rechtssicherheit für die Unternehmen und können damit Wettbewerbsvorteile auf dem internationalen Markt sein.

Anonymisierung und technischer Datenschutz
Gerade dieser Herausforderung werden wir uns stellen und datenschutzkonforme Lösungen stärken. Abhilfe können neben rechtlichen Absicherungen vor allem technische Lösungen bieten, die den Datenschutz gewährleisten.

Seite19
Systeme, die Datenschutz durch Technikgestaltung sowie Datenschutz durch Voreinstellungen beinhalten, sollten einen besonders hohen Stellenwert in der Forschungsförderung und beim Zugang zu Daten erhalten.

Wie wollen wir dies erreichen? – Unsere wichtigsten Maßnahmen:

Die einheitliche Rechtsauslegung und -anwendung der Datenschutzvorschriften im nicht-öffentlichen Bereich ist ein entscheidender Faktor für die Wirksamkeit und den Erfolg der Datenschutzreformen der letzten Jahre. Wir setzen uns für eine enge Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder in allen Datenschutzfragen von bundesweiter Bedeutung ein. Wir prüfen Maßnahmen, die hierzu beitragen können. Dies ist aktuell ein Teilaspekt der Evaluation des Bundesdatenschutzgesetzes (BDSG). (BMI)

Wir werden das Datenschutzrecht für Telemedien- und Telekommunikationsdienste in einem Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) angleichen, die Zuständigkeiten der Aufsichtsbehörden in dem Bereich neu regeln und so für mehr Rechtssicherheit sorgen. (BMWi)

Divergierende datenschutzrechtliche Regelungen auf Landesebene erschweren teilweise die Nutzung personenbezogener Daten für die Forschung, etwa im Bildungsbereich. Wir wollen die Möglichkeiten der Datennutzung für Forschungszwecke verbessern. Hierfür werden wir bei den Ländern für eine Harmonisierung der rechtlichen Grundlagen im Landesrecht werben und überprüfen, wo eine Orientierung an der Konzentrationswirkung des § 287a des Fünften Buches Sozialgesetzbuch (SGB V) für die Datenschutzaufsicht auch in anderen Forschungsbereichen sinnvoll ist. (BMBF/BMWi/BMI)

Die Verknüpfbarkeit von Forschungsdaten zu Haushalten und Unternehmen aus unterschiedlichen Quellen wird durch das Zusammenspiel unterschiedlicher gesetzlicher Regelungsbereiche (Sozialrecht, Statistikrecht, Datenschutzrecht) normiert. Hier wollen wir forschungsfreundliche einheitlichere Lösungen finden, ohne datenschutz- und statistikrechtliche Standards zu senken. (BMBF/BMWi)

Mit der Fortsetzung von Datenschutz-Roundtables schaffen wir ein Informations- und Austauschangebot für interessierte Kreise zu aktuellen Datenschutzthemen wie zum internationalen Datenverkehr. (BMI/BMWi)

Wir werden durch technische Lösungen den betroffenen Personen die eigenverantwortliche Wahrnehmung ihrer → Datensouveränität erleichtern. Im Bereich des Datenschutzeinwilligungsmanagements haben wir eine Lösung für ein innovatives Datenschutzeinwilligungsmanagement erforschen lassen. (BMJV)

Seite20
Wir setzen uns auch auf europäischer Ebene für ein einheitliches Datenschutzverständnis ein. Dies gilt insbesondere im Hinblick auf die Durchsetzung des Datenschutzrechts. (BMI)

Anonymisierung und technischer Datenschutz
Zur Förderung des technischen Datenschutzes werden wir ein Forschungsnetzwerk zur Anonymisierung etablieren.

Die Intensivierung des → Datenteilens wollen wir durch eine effizientere Kontrolle des Datenschutzes und der Cybersicherheit flankieren. Öffentliche Prüf- und Zertifizierungslabore, die die technische Prüfung datenbasierter Produkte und Dienste auf ihre Datenschutzkonformität vornehmen, können hier einen wichtigen Beitrag leisten. Wir werden die Errichtung eines Netzwerks aus Prüf- und Zertifizierungslaboren prüfen. (BMI)

Wir werden den Austausch mit Wirtschaftsverbänden und Aufsichtsbehörden zu datenschutzkonformen KI- und Blockchain-Lösungen fortsetzen und damit mehr Sicherheit für innovative Geschäftsmodelle schaffen. (BMWi)

2.1.2 Rahmenbedingungen bei nicht-personenbezogenen Daten

Was wollen wir erreichen?

Seite23
Verboten wäre demnach beispielsweise die Verweigerung eines angemessenen, datenschutzkonformen und nichtdiskriminierenden Zugangs zu relevanten, ggf. exklusiven Daten, die von Plattformnutzern nicht oder nur unter unverhältnismäßig hohem Aufwand selbst erzeugt oder gesammelt werden können.

Wie wollen wir dies erreichen? – Unsere wichtigsten Maßnahmen:

Seite24
Im Mittelpunkt stehen u.a. Fragen der Akzeptanz, der Mitarbeiterqualifikation, der Datensicherheit und des Datenschutzes für Beschäftigte. (BMBF)

Zur Stärkung der Datenmärkte, Datenkooperationen und Standardsetzung werden wir den Dialog mit allen relevanten Beteiligten weiterführen. Zur Etablierung dieses Dialogs auf europäischer Ebene werden wir uns für das im Koalitionsvertrag vereinbarte Innovationsboard einsetzen. Dieses soll ebenfalls als beratender Ansprechpartner für Datenschutzfragen gegenüber der Wirtschaft (insb. Start-ups und Unternehmen) bei digitalen Innovationen auf EUEbene fungieren. (BMWi)

2.1.3 Stärkung der Daten- und IT-Sicherheit

Wo stehen wir?

Seite25
Die großen außereuropäischen Cloud-Anbieter speichern die Daten ihrer Kunden z.T. in ihren Herkunftsländern. Dies kann mit negativen Folgen für die betroffenen Personen verbunden sein. Zudem widerspricht es nach aktueller Rechtsprechung des EuGHs in manchen Fällen dem europäischen Datenschutzrecht.

Was wollen wir erreichen?

Wir setzen uns weiterhin international für freien Datenverkehr ein, da erzwungene Datenlokalisierung bei Unternehmen unnötige Kosten verursacht. Sofern es um personenbezogene Daten geht, sind allerdings die Vorgaben des europäischen und nationalen Datenschutzrechts zu beachten.

2.2 Schaffung neuer Datenräume

Wo stehen wir?

Seite27
Datenbasierte Innovation kann auch dort, wo Daten über (Wirtschafts-)Sektoren und Forschungsbereiche hinweg geteilt und genutzt werden, entstehen. Daher sollten – wo dies sicher und im Einklang mit dem Datenschutzrecht möglich ist – Datenräume so ausgestaltet sein, dass diese Offenheit über Sektorengrenzen hinweg gewährleistet werden kann.

Was wollen wir erreichen?

Seite28
Es ist daher wichtig, die Nutzung von Gesundheitsdaten zum Wohl der Patientinnen und Patienten und im Einklang mit den geltenden datenschutzrechtlichen Vorgaben in Versorgung und Forschung weiter zu fördern und die Digitalisierung der Gesundheitsversorgung konsequent weiter zu verfolgen.

2.3 Datentreuhänder und neue Kooperationsformen

Wo stehen wir?

Seite34
Datentreuhänder. Diese können durch vielfältige Ausgestaltung das Teilen von Daten vereinfachen und ermöglichen, beispielsweise indem sie Dateninfrastrukturen bereitstellen, sicherstellen, dass das geltende Datenschutzrecht eingehalten wird, bzw. eine Anonymisierung vornehmen.

Diese Datentreuhänder können die Interessen von Verbraucherinnen und Verbrauchern wahrnehmen und diese bei Ausübung und Geltendmachung ihrer datenschutzrechtlichen Gestaltungsrechte und Betroffenenrechte (z.B. Auskunft, Änderungen, Einwilligung, Löschung, Widerspruch) unterstützen.

Was wollen wir erreichen?

Seite35
Wir prüfen die Schaffung eines konkreten Rechtsrahmens für Datenmanagementsysteme bzw. Personal Information Management Systems (PIMS), die das Datenschutzrecht sicherstellen und die Interessen der Verbraucherinnen und Verbraucher wahren.

Ein wichtiges Kriterium ist hierbei, dass solche Datenmanagementsysteme ausschließlich im Interesse der betroffenen Person tätig sind und entsprechend der Vorgaben des Datenschutzrechts handeln.

Wie wollen wir dies erreichen? – Unsere wichtigsten Maßnahmen:

Seite36
Wir prüfen auf nationaler Ebene die Aufnahme einer Regelung zu Datenmanagementsystemen/„Personal Information Management Systems“ (PIMS), die den Verbrauchern eine erleichterte Wahrnehmung ihrer Datenschutzrechte ermöglichen. (BMWi)

2.4 Teilhabe sichern: Stärkung der Interessen der Bürgerinnen und Bürger in der Datenökonomie

Was wollen wir erreichen?

Seite37
Wichtige Mechanismen zum Schutz von Bürgerinnen und Bürgern bieten das Datenschutzrecht und dessen effiziente Durchsetzung (vgl. hierzu 2.1.1) sowie die Regelungen des Verbraucherschutzes sowie des Kinder- und Jugendmedienschutzes.

III. Datenkompetenz erhöhen und Datenkultur etablieren

3.1 Kompetente Gesellschaft: Selbstbestimmter und informiert

Wo stehen wir?

Seite41
Das Ganze gilt insbesondere im Umgang mit zum Teil sehr unübersichtlichen Ausführungen in Datenschutzerklärungen und Allgemeinen Geschäftsbedingungen.

Wie wollen wir dies erreichen? – Unsere wichtigsten Maßnahmen:

Seite42
Über die Leitinitiative Sichere Digitale Bildungsräume fördern wir die Entwicklung von offenen Standards, Infrastrukturen und Governance-Modellen für einen nutzerinnen- und nutzerzentrierten, selbstbestimmten und datenschutzkonformen Austausch und die Vernetzung von digitalen Lehr- und Lernplattformen sowie digitalen Bildungsnachweisen für alle Bildungsbereiche.

3.2 Erhöhung der Datenkompetenz in Bildung und Ausbildung

Wo stehen wir?

Seite44
In der KMK-Strategie (KultusMinisterKonferenz) zur „Bildung in der digitalen Welt“ sind in dem dort entwickelten Kompetenzrahmen einige Datenkompetenz stärkende Elemente eingebettet, u.a. zum persönlichen Datenschutz und zur Datenanalyse- und -speicherung.

Was wollen wir erreichen?

Seite47
Wir wollen zivilgesellschaftliche Organisationen, Vereine und Verbände beim sicheren und datenschutzkonformen Einsatz datenbasierter Prozesse unterstützen.

4.3 Bessere Datennutzung für eine effizientere und bürgerfreundlichere Verwaltungspraxis

Wo stehen wir?

Seite56
Eine datenschutzkonforme Modernisierung und Digitalisierung sowie Vernetzung der Register bietet Potenzial für Entlastung und Effizienz der Verwaltung und eine effektivere Erbringung von (Verwaltungs-)Leistungen.

Was wollen wir erreichen?

Seite60
Derzeit verfügen zwar alle Behörden über eine(n) behördlichen Datenschutzbeauftragte(n), aber bisher hat kaum eine Behörde eine/n → Chief Data Scientist („Datennutzungsbeauftragte/n“), oder einen Chief Data Officer als verantwortliche Stelle für eine Data Governance, die behördenintern bei der Entwicklung weiterer Nutzungen von Daten unterstützen kann.

Wie wollen wir dies erreichen? – Unsere wichtigsten Maßnahmen:

Der Chief Data Scientist und der Datenschutzbeauftragte arbeiten zusammen.

Seite61
Forschungsdatenzentren.
Diese fungieren als Ansprechpartner für die datenschutzkonforme Nutzung der nicht eingestuften → Rohdaten, die zur Verfügung gestellt werden. Vorreiterbehörden sind BMAS, BMEL, BMG, BMU und BMZ, die sich bei der Setzung von Standards abstimmen.

Tabelle mit allen Maßnahmen der Datenstrategie
Fokus Datenschutz

II. Innovative und verantwortungsvolle Datennutzung steigern

2.1 Regulierung: Verbesserung der Rahmenbedingungen

2.1.1 Rahmenbedingungen bei personenbezogenen Daten
Rechtssicherheit

Seite66
2.1.1 Zusammenarbeit Datenschutzaufsichtsbehörden
Wir setzen uns für eine enge Zusammenarbeit der Datenschutzaufsichtsbehörden des Bundes und der Länder in allen Datenschutzfragen von bundesweiter Bedeutung ein.

2.1.1 Federführende Datenschutzaufsicht bei länderübergreifenden Vorhaben der Versorgungs- und Gesundheitsforschung
Zur Beschleunigung und Vereinfachung multizentrischer, länderübergreifender Vorhaben der Versorgungs- und Gesundheitsforschung wurde mit § 287a SGB V eine Regelung für die Geltung des Bundesrechts (§ 27 BDSG) und eine federführende Aufsichtsbehörde am Vorbild der DSGVO geschaffen.

2.1.1 Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG)
Wir werden das Datenschutzrecht für Telemedien- und Telekommunikationsdienste in einem

Telekommunikations-Telemedien-Datenschutz-Gesetz angleichen, die Zuständigkeiten der Aufsichtsbehörden in dem Bereich klarer fassen und so für mehr Rechtssicherheit sorgen.

Seite67

2.1.1 Werbung für Harmonisierung der rechtlichen Grundlagen im Landesrecht

Divergierende datenschutzrechtliche Regelungen auf Landesebene erschweren teilweise die Nutzung von personenbezogenen Daten für die Forschung, etwa im Bildungsbereich.

2.1.1 Verknüpfbarkeit von Forschungsdaten – einheitlichere Lösungen

Wir wollen forschungsfreundliche Lösungen für die Verknüpfbarkeit von Forschungsdaten zu Haushalten und Unternehmen finden. Diese verknüpften Daten aus unterschiedlichen Quellen werden durch unterschiedliche Regelungsbereiche (Sozialrecht, Statistikrecht, Datenschutzrecht) normiert

2.1.1 Datenschutz-Roundtable

Mit der Fortsetzung von Datenschutz-Roundtables schaffen wir ein Informations- und Austauschangebot für interessierte Kreise zu aktuellen Datenschutzthemen (z.B. zum internationalen Datenverkehr).

2.1.1 Projekt: „Innovatives Datenschutz-Einwilligungsmanagement“

Das Forschungsprojekt analysiert Einwilligungsmodelle im OnlineKontext und erhebt mit einer repräsentativen Online-Befragung Verbrauchererwartungen. Es werden Empfehlungen zur rechtskonformen und verbraucherfreundlichen Einwilligung in Form eines Best-Practice-Modells entwickelt.

2.1.1 E-Privacy-Verordnung

Wir streben mit der e-Privacy-Verordnung eine Harmonisierung im europäischen Datenschutz an, die den besonders wichtigen Schutz der Privatsphäre in der elektronischen Kommunikation verbessern soll.

2.1.1 Einheitliche Durchsetzung des Datenschutzrechts innerhalb der EU

Auf europäischer Ebene sollte ein einheitliches Datenschutzverständnis entwickelt werden, damit Unternehmen, die in der EU tätig sind, ähnliche Bedingungen in den Ländern vorfinden. Dies gilt insbesondere im Hinblick auf die Durchsetzung des Datenschutzrechts.

Seite68

Anonymisierung und technischer Datenschutz

2.1.1 Prüfauftrag Errichtung eines Netzwerkes aus Prüf- und Zertifizierungslaboren

Prüf- und Zertifizierungslabore, welche die technische Prüfung datenbasierter Produkte und Dienste auf ihre Datenschutzkonformität vornehmen, leisten einen wichtigen Beitrag für die Durchsetzung des Datenschutzrechts. Daher prüfen wir die Errichtung eines solchen Netzwerks.

2.1.1 Austausch mit Wirtschaftsverbänden und Aufsichtsbehörden zu datenschutzkonformen KI- und Blockchain-Lösungen

Wir werden den Austausch mit Wirtschaftsverbänden und Aufsichtsbehörden zu datenschutzkonformen KI- und BlockchainLösungen fortsetzen und damit mehr Sicherheit für innovative Geschäftsmodelle schaffen.

2.1.2 Rahmenbedingungen bei nicht-personenbezogenen Daten

Seite70

2.1.2 Innovationsboard

Wir werden uns für das im Koalitionsvertrag vereinbarte Innovationsboard einsetzen. Dieses soll ebenfalls als beratender Ansprechpartner für Datenschutzfragen gegenüber der Wirtschaft (insb. Start-ups und Unternehmen) bei digitalen Innovationen auf EUEbene fungieren.

Seite72

2.2 Schaffung neuer Datenräume
Förderung innovativer und verantwortungsvoller Initiativen zur Datennutzung

2.2 Datenschutzrechtliche Unterstützungsangebote für die Erprobung von Innovationen in Reallaboren
Wir werden Unterstützungsangebote für die temporäre Erprobung von Innovationen in Reallaboren als Testräume für Innovation und Regulierung schaffen.

Seite80

2.3 Akteure: Datentreuhänder und neue Kooperationsformen

2.3 Personal Information Management Systems (PIMS)
Wir prüfen auf nationaler Ebene eine Regelung zu „Personal Information Management Systems“ (PIMS), die es Verbraucherinnen und Verbrauchern erleichtern, ihrer Datenschutzrechte wahrzunehmen.

2.4 Risiken bekämpfen: Stärkung der Interessen der Bürgerinnen und Bürger in der Datenökonomie

Seite82

2.4 Projekt „Daten-Check für Smartphone-Apps“
Wir fördern das Verbraucherinformationsprojekt „Daten-Check für Smartphone-Apps“. Das zentrale Projektziel ist die Ergänzung der Webseite mobilsicher.de um eine App-Test-Plattform mit Informationen zu Datenschutz und Datensicherheit für Verbraucherinnen und Verbraucher.

2.4 Datensouveränität und Empowerment von Verbraucher:innen – Datenschutz im Umgang mit Sprachassistenten (CheckMyVA)
Das Projekt zielt darauf ab, die Datensouveränität von Nutzerinnen und Nutzern von Sprachassistenten zu verbessern. Hierzu soll eine Plattform erstellt werden, die bei der Wahrnehmung der Verbraucherrechte unterstützt.

III. Datenkompetenz erhöhen und Datenkultur etablieren

3.1 Kompetente Gesellschaft: Selbstbestimmter und informierter Umgang mit Daten in allen Teilen der Bevölkerung

3.1 Leitinitiative Sichere Digitale Bildungsräume
Über die Leitinitiative Sichere Digitale Bildungsräume fördern wir die Entwicklung von offenen Standards, Infrastrukturen und Governance-Modellen für einen nutzerzentrierten und datenschutzkonformen Austausch sowie die Vernetzung von digitalen Lehr- und Lernplattformen.

Glossar zur Datenstrategie
Fokus Datenschutz

Seite109
Der Datenschutz gewährleistet den Schutz der Grundrechte und Grundfreiheiten der Bürgerinnen und Bürger, insb. ihrer informationellen Selbstbestimmung und Privatsphäre im Zusammenhang mit Datenverarbeitungen.

Datenschutzes durch Technikgestaltung. Grundgedanke ist, dass sich Datenschutz am wirksamsten umsetzen lässt, wenn er bereits bei Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert ist. Der wirksame Schutz personenbezogener Daten erfolgt durch das frühzeitige Ergreifen technischer und organisatorischer Maßnahmen im Entwicklungsstadium.

Seite110
Der Begriff Datensouveränität geht über das Datenschutzrecht hinaus und stellt die Autonomie der betroffenen Person, aber auch des Unternehmens über ihre bzw. seine Daten in den Mittelpunkt, welche bzw. welcher souverän und durch technische Mittel und seine Fähigkeiten selbstständig in der Lage ist, sich selbstbestimmt in der Datenwelt zu bewegen.

Datentreuhänder können aber auch datenschutzrechtliche Interessen und Gestaltungsrechte für eine Vielzahl von Verbraucherinnen und Verbrauchern geltend machen.