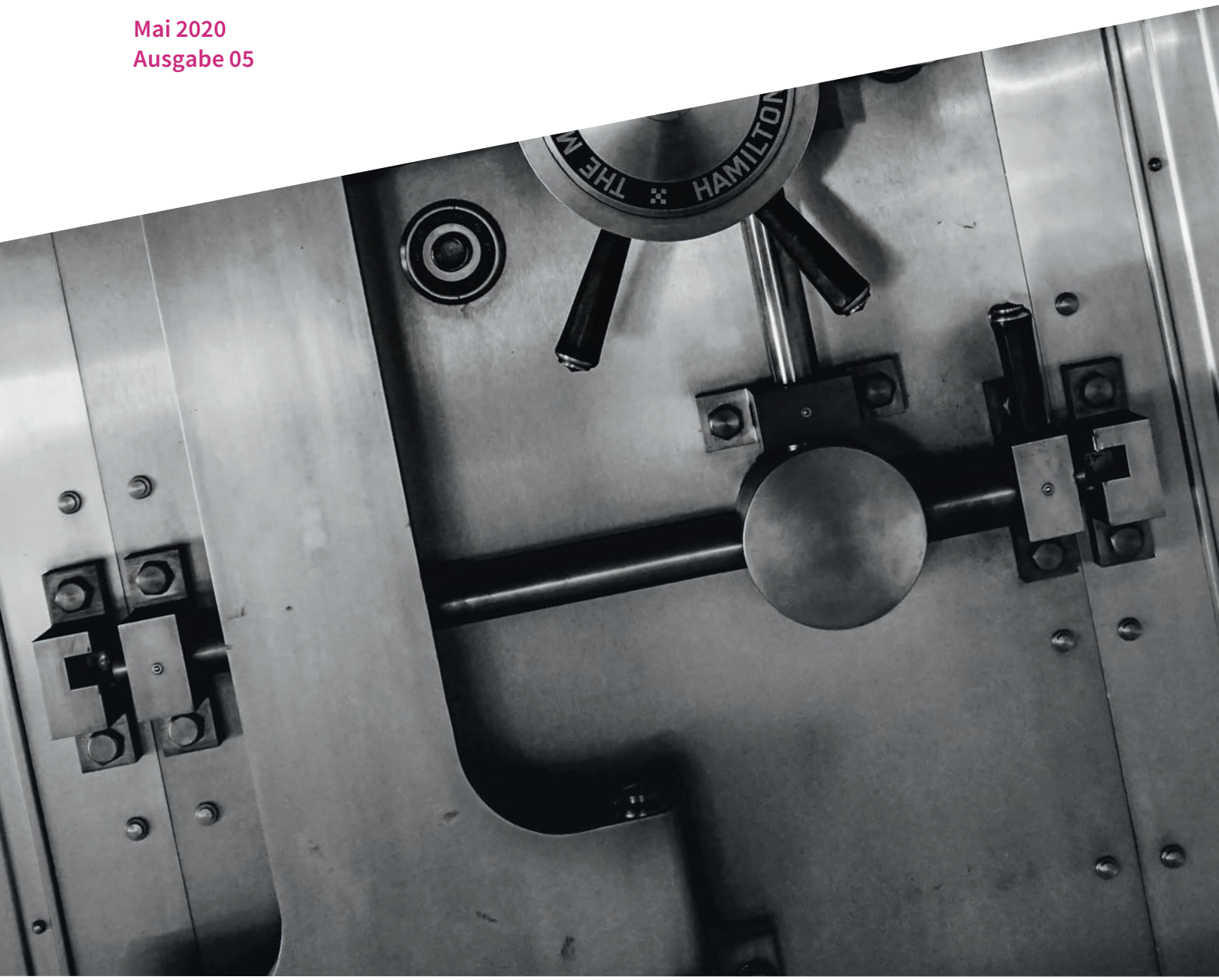
iRights.Lab
Think Tank für die digitale Welt

Data-Governance-Report

mFUND-Begleitforschung vom Think Tank iRights.Lab

Mai 2020
Ausgabe 05



Bundesministerium für Verkehr und digitale Infrastruktur

mFUND
Das Startkapital für die Mobilität 4.0

Data-Governance-Report

Die Verarbeitung von Daten stellt in vielen Bereichen die Grundlage für Innovationen dar. Sei es bei der automatisierten Erkennung von Bauwerkschäden, einer optimierten Verkehrsplanung oder einer anwenderorientierten Bereitstellung von Geo- und Wetterdaten – technologiegestützte Verfahren verarbeiten große Datenmengen und können so Erkenntnisse generieren, Prozesse vereinfachen und die Digitalisierung gemeinwohlorientiert nutzbar machen. Personenbezogene Daten gelten jedoch generell als schützenswert. Die Einführung der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 hat den Datenschutz novelliert und soll ihn europaweit vereinheitlichen. Viele Organisationen hatten sich vorher nur am Rande mit der Thematik befasst. Durch die Novellierung hat sie in der öffentlichen Wahrnehmung an erheblicher Bedeutung gewonnen: Datenschutz ist heute omnipräsent. Es ist unumgänglich, sich mit dem Thema Datenschutz (immer wieder) zu beschäftigen. Das gilt nicht nur für die Organisationsleitung, die rechtlich die Verantwortung trägt, sondern für alle Mitarbeiter*innen, die Daten verarbeiten. Zu Recht stellt Datenschutz daher einen zentralen Baustein eines jeden Data-Governance-Konzeptes dar.

Der vorliegende Report ist der fünfte Data-Governance-Report, der im Rahmen der mFUND-Begleitforschung vom iRights.Lab erarbeitet wurde. Er beleuchtet und erläutert das komplexe Thema Datenschutz. Datenschutz – wozu beschäftige ich mich damit eigentlich? Was weiß ich inzwischen wirklich über die DSGVO? Und wie setze ich Datenschutz in meiner Organisation um? Diesen Fragen widmen wir uns auf den nächsten Seiten.

Viele Organisationen haben sich in den letzten zwei Jahren bereits intensiv mit der DSGVO beschäftigt. Daher ist jetzt eine gute Zeit zur Evaluation. Wir wünschen dabei viel Spaß mit unserem „DSGVO – Refresh Quiz“. Für die weitere Arbeit zu dem Thema Datenschutz präsentieren wir darüber hinaus unsere „Checkliste Datenschutz“, die als Begleiterin durch den Prozess Datenschutz überaus hilfreich ist.

Die DSGVO regelt die Verarbeitung personenbezogener Daten.

Der Ausdruck personenbezogene Daten bezeichnet „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen.“, vgl. Art. 4 Nr. 1 DSGVO.

Woran arbeitet das iRights.Lab im Projekt „Data-Governance“ der mFUND-Begleitforschung?

Im Projekt „Data-Governance im Innovationsprozess“ entwickeln wir ein Self-Governance-Konzept im Bereich datenbasierter Innovationen. Auf dem Weg dahin berücksichtigen wir rechtliche, ethische, technologische, gesellschaftliche und politische Parameter, sodass passende Lösungen für verschiedene Organisationstypen entworfen werden. Wir wollen Behörden und Unternehmen dazu befähigen, eigene Regeln und Strukturen für einen verantwortungsbewussten Umgang mit den von ihnen verwalteten und verwendeten Daten aufzusetzen.

Neuigkeiten aus der mFUND-Begleitforschung des iRights.Lab

Ideensprint Data Governance

Daten sind der zentrale Treiber für digitale Innovationen. Doch wie müssen wir Daten erfassen, speichern und verarbeiten, um ihre Potentiale zu nutzen? Entlang welcher Prinzipien sollte sich das Datenmanagement orientieren? Und wie können Unternehmen, die öffentliche Hand und zivilgesellschaftliche Organisationen ihren Umgang mit Daten gemeinsam verbessern? Diese Fragen bildeten die Grundlage für den Ideensprint „Data Governance“ am 26.02.2020 im Palazzo des iRights.Lab.

In einem Multistakeholderprozess mit gut 30 Akteur*innen aus den vier Sektoren Zivilgesellschaft, Unternehmen/Wirtschaft, öffentlicher Sektor/Behörde und Wissenschaft wurden gemeinsam Herausforderungen in Bezug auf die (eigene) Arbeit mit Daten definiert, geclustert und mit konkreten Maßnahmen adressiert.

Bemerkenswert ist, dass das Thema Datenschutz sowohl im Ideensprint, als auch bei den Interviews mit durch den mFUND geförderten Projekten als sehr relevant im Rahmen einer Self-Data-Governance beurteilt wurde. Trotzdem bestand während des Ideensprints kein besonderes Interesse diese Herausforderung vertiefend zu bearbeiten. Unsere vorhergegangene Befragung der mFUND-Projekte stütz diese Beobachtung: Die Themen Datenschutz und Datensicherheit wurden als nicht-innovationsfördernd eingeschätzt.[1]

„Data Governance bietet die Möglichkeit, einen Schritt zurückzugehen und sich zu fragen: Was ist das eigentliche Ziel der Digitalisierung, was ist die eigentliche Vision und wie sollte diese aussehen?“

Florian Schulze war Impulsgeber bei dem Ideensprint Data Governance des iRights.Labs. Er arbeitet in interdisziplinären Teams an Smart City und Data Governance.

Eindrücke vom Ideensprint am 26.02.2020, Foto: iRights.Lab

1 Data-Governance-Report, Ausgabe 01, S. 4.

Datenschutz ist also eine wichtige Herausforderung im Rahmen einer Self-Data-Governance-Struktur, jedoch ist die Beschäftigung damit scheinbar wenig attraktiv. Daraus ließe sich vorsichtig ableiten, dass Datenschutz im Zusammenhang mit Innovationen tendenziell eher als Pflicht denn als Potential eingeschätzt wird.

Zudem ist erwähnenswert, dass während des Ideensprints ein großes Interesse an der Erörterung „des Faktors Mensch“, wie dem Aufbau von Kompetenzen und der gesellschaftlichen Sensibilisierung zu Data Governance, bestand. Auch ordnungspolitische Themen wurden angeregt diskutiert. Data Governance kann nicht nur mit Softwarelösungen und technischen Erneuerungen begegnet werden. Der Austausch, insbesondere mit den Akteur*innen aus der Zivilgesellschaft, hat die Einbeziehung aller Stakeholder bei dem Aufbau einer Self-Data-Governance Struktur als zu bewältigende Herausforderung in den Mittelpunkt gerückt.

Neben der Diskussion um die Herausforderungen von Data Governance stand die Entwicklung eigener Projektideen im Zentrum des Ideensprints. Außerdem wurden die Teilnehmenden dazu angeregt, weiter im Austausch zu bleiben und gemeinsam an Projektideen zu schleifen. Wir sind gespannt, wie es mit den spannenden Konzepten und Ideen des Tages weitergeht.

Eindrücke vom Ideensprint am 26.02.2020,
Foto: iRights.Lab

Datenschutz – wofür eigentlich?

Haben Sie sich auch schon mal gefragt, wozu es eigentlich Datenschutz braucht? Es gibt viele gute Gründe dafür. Hier präsentieren wir eine Auswahl:

Pragmatische Perspektive

Die pragmatischen Argumente für die Beschäftigung mit der Thematik liegen auf der Hand. Die Einhaltung des Datenschutzes ist gesetzlich vorgeschrieben. Der Verstoß gegen die DSGVO ist im nichtöffentlichen Bereich bußgeldbewehrt. Um sich vor Sanktionen zu schützen, ist die Auseinandersetzung mit dem Datenschutzrecht unumgänglich.

Doch auch unabhängig von offiziellen Regulierungen schützt die Einhaltung der Datenschutzvorgaben und -empfehlungen die eigene Organisation. Gerade die Beachtung der Datensicherheit als ein Teilaspekt des Datenschutzes kann vor überraschenden Manipulationsversuchen und Datenlecks bewahren – diese können zu großen wirtschaftlichen Verlusten und Reputationsschäden führen. Daher sollten im eigenen Interesse die verarbeitenden Daten vor unberechtigten Zugriffen durch Dritte geschützt werden.

Gesellschaftliche Perspektive

Datenschutz nimmt eine wichtige politisch-gesellschaftliche Funktion ein. Das Persönlichkeitsrecht ist eine fundamentale Säule der freiheitlich-demokratischen Grundordnung. Für unser heutiges Verständnis von Datenschutz ist ein Urteil des Bundesverfassungsgerichtes aus dem Jahr 1983 wegweisend gewesen. Darin wurde eine geplante Volkszählung auf Bundesebene als rechtswidrig angesehen, weil sie das „Grundrecht auf informationelle Selbstbestimmung“ verletze. Es wurde argumentiert, dass die Verwendung moderner Datenverarbeitungstechnologien ein Gefühl der Überwachung und der Kontrolle hervorrufen könne. Unsicherheiten über die gespeicherten und vorrätig gehaltenen Informationen würden ein übermäßig konformes Verhalten begünstigen. Daher soll durch den Schutz von personenbezogenen Daten durch den Staat das Entstehen eines Panoptikums[2] – bzw. das Gefühl sich in einem zu befinden – verhindert werden. Datenschutz leistet einen Beitrag zur Wahrung der allgemeinen Handlungsfreiheit und der Menschenwürde. Die freiheitlich-demokratische Grundordnung zu schützen ist sicher eine gute Begründung für die Beschäftigung mit dem mitunter herausfordernden Thema.

Dieses Konzept hat mit der Zunahme der Verarbeitung von Daten auch durch nicht-staatliche Akteure eine Ausweitung und Wandel

Art. 1 der DSGVO benennt unter anderem die Ziele der DSGVO. Neben der Gewährleistung des freien Verkehrs von Daten schützt sie explizit „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“.

2 Panoptikum (von Panopticon, griechisch: „alles“ und „zum Sehen gehörend“), beschreibt eine Struktur, die eine umfassende und gleichzeitige Überwachung durch eine zentrale Stelle beschreibt. Der Philosoph Michel Foucault bezeichnet dieses Ordnungsprinzip als Modell moderner Überwachungsgesellschaften.

erfahren. Vorläufiger Höhepunkt dürfte sein, dass der Schutz persönlicher Daten ausdrücklich Eingang in die Charta der Grundrechte der Europäischen Union gefunden hat. Das Schutzgut, wie es ursprünglich allein das Grundrecht auf informationelle Selbstbestimmung war, wird dort jedoch nicht näher bestimmt.

Unternehmerische Perspektive

Aus einer ökonomisch-organisatorischen Perspektive bietet ein datenschutzkonformes Verhalten und die Datenschutzsensibilität von wichtigen Stakeholdern ebenfalls Vorteile. Das Vertrauen von Kund*innen und Partner*innen wird durch einen souveränen Umgang mit dem Thema Datenschutz gestärkt. Eine gute Zusammenarbeit wird gefördert, wenn das Gegenüber das Gefühl hat, es wird verantwortungsbewusst mit den eigenen Daten umgegangen. Darüber hinaus können sich Organisationen auch gegenüber Mitarbeiter*innen positionieren. Fachkräfte sind zurzeit begehrt. Bestandteil eines attraktiven Employer Branding kann eine freiwillige Selbstverpflichtung sein, die gesellschaftlichen und wirtschaftlichen Veränderungen der Digitalisierung zu berücksichtigen und in Anbetracht dessen nachhaltig und umsichtig zu wirtschaften. Dieser Unternehmensverantwortung wird „Corporate Social Responsibility“ (CSR) oder „Corporate Digital Responsability“ (CDR) genannt und umfasst auch die Beachtung des Datenschutzes.

Doch nicht nur in der (Außen-)Kommunikation kann die Beschäftigung mit dem Thema Datenschutz für eine Organisation Vorteile mit sich bringen. Die Etablierung von präzisen und vorgegebenen Verfahren der Datenverarbeitung kann zur Optimierung der internen Prozesse beitragen. Compliance und Effizienz hängen oftmals eng zusammen. Datenschutzvorgaben können somit im Rahmen einer Self-Data-Governance die eigenen Betriebsabläufe befördern.

Art. 8 der Grundrechtecharta der EU bestimmt, dass „Daten […] nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden [dürfen]. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.“

DSGVO – Refresh Quiz

Datenschutz-Trägheit war gestern.
Evaluieren Sie sich selber mit einem – durchaus herausfordernden – Datenschutzquiz.
Viel Spaß und gutes Gelingen!

Mehrfachnennungen sind möglich.

1. Für wen und was gilt die DSGVO?

a) Sie gilt für alle Verarbeitungen von personenbezogenen Daten in der EU.
b) Sie gilt für die behördliche und geschäftsmäßige Verarbeitung aller Daten in der EU.
c) Sie gilt für die behördliche und geschäftsmäßige Verarbeitung personenbezogener Daten in der EU.
d) Sie gilt ausschließlich für die behördliche und geschäftsmäßige Verarbeitung personenbezogener Daten in Deutschland.

2. Wie ist der Datenschutz in anderen Mitgliedsstaaten der Europäischen Union geregelt?

a) Alle Mitgliedsstaaten können autonome Datenschutzgesetze erlassen.
b) Die DSGVO ist eine Richtlinie, die Ausgestaltung obliegt den einzelnen Ländern.
c) Die DSGVO ist eine Verordnung, obwohl sie unmittelbar gilt, können die Länder hinsichtlich einzelner Aspekte unterschiedliche Regelungen treffen.
d) Die DSGVO hat den Datenschutz in Europa vollständig vereinheitlicht.

3. Was sind unter Umständen keine personenbezogenen Daten?

a) Meteorologische Daten, die durch einen Satelliten erhoben wurden.
b) Anonyme Daten aus einer Verkehrserhebung.
c) Reine Sachdaten zum Bau einer Immobile.
d) Pseudonymisierte Kontaktinformationen.

4. Was bedeutet „die Verarbeitung“ von personenbezogenen Daten?

a) Die Speicherung von personenbezogenen Daten.
b) Die Verwendung von personenbezogenen Daten.
c) Die Verbreitung von personenbezogenen Daten.
d) Die Löschung von personenbezogenen Daten.

5. Gilt die DSGVO auch für handschriftliche Notizen?

a) Ja, wenn sie geordnet geführt werden.
b) Ja, immer.
c) Nein, außer sie sind elektronisch in einem Akten- und Archivsystem erfasst.
d) Nein.

6. Welche Anforderungen stellt die DSGVO an die Verarbeitung von anonymisierten Daten?

a) Die DSGVO regelt die Verwendung von anonymisierten Daten nicht.

b) Es werden die gleichen Anforderungen wie an pseudonymisierte Daten gestellt.

7. Die Verarbeitung personenbezogener Daten ist in der EU

a) …grundsätzlich verboten, außer sie ist in der DSGVO ausdrücklich erlaubt.

b) …grundsätzlich erlaubt, außer sie ist in der DSGVO ausdrücklich verboten.

8. Unter welchen Voraussetzungen kann die Verarbeitung personenbezogener Daten doch erlaubt sein?

a) Wenn es sich um lediglich historische Daten handelt.

b) Wenn ein berechtigtes Interesse besteht.

c) Wenn es sich um belanglose Daten im Sinne der DSGVO handelt.

d) Wenn sie zur Erfüllung eines Vertrages (mit der betroffenen Person) erforderlich ist.

9. Welche Anforderungen bestehen hinsichtlich der Wirksamkeit einer Einwilligung?

a) Freiwilligkeit

b) Informiertheit

c) Ausdrücklichkeit

d) Widerrufbarkeit

10. Was wird nicht in der DSGVO geregelt?

a) Die Zulässigkeit von automatisierten Einzelfallentscheidungen.

b) Besondere gesetzliche Zulässigkeitsvoraussetzungen für Scoring-Verfahren.

c) Schadensersatzansprüche aufgrund von benachteiligenden Entscheidungen die durch Softwareanwendungen getroffen wurden.

d) Die rechtliche Handhabung von „Daten als Entgelt“.

Auswertung: DSGVO – Refresh Quiz

Jeweils einen Punkt gibt es sowohl für **jede korrekt angekreuzte**, als auch für **jede richtigerweise nicht-angekreuzte Antwort.**
Maximale Punkteanzahl: 36 (Summe alle Antwortmöglichkeiten)

1. Für wen und was gilt die DSGVO?

c) Die DSGVO **gilt für die behördliche und geschäftsmäßige Verarbeitung personenbezogener Daten in der EU**. Sie gilt gleichermaßen für den öffentlich-rechtliche und den privatwirtschaftlichen Sektor. „Geschäftsmäßig" bedeutet nicht nur mit Gewinnerzielungsabsicht, sondern umfasst auch Vereine, Kirchen und anderen gemeinnützige und nicht-profitorientierte Einrichtungen. Die DSGVO gilt nicht für die rein persönliche oder familiäre Datenverarbeitung. Sie regelt nur die Verarbeitung von personenbezogenen Daten. Das sind gem. Art. 4 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person') beziehen". Die DSGVO gilt in der gesamten EU.

2. Wie ist der Datenschutz in anderen Mitgliedsstaaten der Europäischen Union geregelt?

c) **Die DSGVO ist eine Verordnung, obwohl sie unmittelbar gilt, können die Länder hinsichtlich einzelner Aspekte unterschiedliche Regelungen treffen.** Verordnungen gelten grundsätzlich unmittelbar und vereinheitlichen das Recht. Hinsichtlich einzelner Aspekte hat die DSGVO den Mitgliedstaaten jedoch explizit einen Gestaltungsfreiraum überlassen, die sogenannten Öffnungsklauseln. In diesen Bereichen können die einzelnen Länder voneinander abweichende Bestimmungen erlassen. So normiert der Art. 37 IV DSGVO, dass auch aus anderen als den dort genannten Gründen eine Verpflichtung zur Benennung eines oder einer Datenschutzbeauftragen bestehen kann. Deutschland hat sich dafür entschieden: So müssen Organisationen, die in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, eine Person als Datenschutzbeauftragte*n benennen.

3. Was sind unter Umständen keine personenbezogenen Daten?

a)b)c) **Meteorologische Daten, die durch einen Satelliten erhoben wurden**, **anonyme Daten aus einer Verkehrserhebung** und **reine Sachdaten zum Bau einer Immobile** sind wohl in den meisten Fällen keine personenbezogenen Daten. Das ist jedoch kein Automatismus, denn der Personenbezug ist weit gefasst und umfasst auch gemischte Daten. Die Daten des Wettersatelliten beispielsweise würden personenbezogen, wenn sich die Programmierer*innen in den Datensätzen sozusagen verewigt hätten. Daten, von denen man glaubte, die seien anonym, lassen sich oftmals doch auf eine einzelne Person beziehen. Und sachliche Daten zu einem Grundstück lassen Rückschlüsse zur Person des*der Eigentümer*in zu. Es wird daher – besonders von Aufsichtsbehörden – eine Meinung vertreten, nach der letztendlich alle Daten personenbezogene Daten seien. Das stimmt so nicht. Es sind durchaus Daten denkbar, die keinen Personenbezug aufweisen. Um die bestehende Unsicherheit der Abgrenzung zu mildern, hat die EU eine Verordnung über die nicht-personenbezogenen Daten erlassen, die mehr Klarheit bringen soll: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN*. Nichtsdestotrotz ist es aufgrund der Weite des Personenbezuges, wie er von den Aufsichtsbehörden vertreten wird, im Alltag ratsam den Personenbezug im Zweifel anzunehmen.

4. Was bedeutet „die Verarbeitung“ von personenbezogenen Daten?

a)b)c)d) Die Verarbeitung von personenbezogenen Daten umfasst sowohl **die Speicherung**, **die Verwendung**, **die Verbreitung** und **die Löschung**. Der Begriff der Verarbeitung bezeichnet gem. Art. 4 Nr. 2 DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“. Alle genannten Beispiele sind – neben diversen anderen Vorgängen – explizit aufgezählt. Der Begriff der Verarbeitung umfasst tatsächlich in der Praxis jegliche Handhabung von Daten.

5. Gilt die DSGVO auch für handschriftliche Notizen?

a) Die DSGVO gilt für handschriftliche Notizen, **wenn sie geordnet geführt werden.** Handschriftliche Notizen – obwohl nicht digitalisiert – unterfallen der DSGVO schon, wenn sie in einem Dateisystem erfasst sind, da sie dann als Datei gelten. Ein Dateisystem wird in Art. 4 Nr. 6 definiert. Der Begriff bezeichnet „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird“. Ein bestimmtes Ordnungssystem, wie ein Verzeichnis, ist nicht erforderlich. So sind zum Beispiel auch handschriftliche Gesprächsnotizen in einem chronologisch geführten Notizbuch von dem Anwendungsbereich der DSGVO erfasst.

6. Welche Anforderungen stellt die DSGVO an die Verarbeitung von anonymisierten Daten?

a) **Die DSGVO regelt die Verwendung von anonymisierten Daten nicht.** Anonymisierte Daten sind grundsätzlich nicht von der DSGVO erfasst. Das kann die Arbeit mit ihnen erleichtern. Jedoch ist eine vollständige Anonymisierung mitunter schwer (oder gar nicht) zu erreichen und unter Umständen gehen damit zentrale Informationswerte der Daten verloren. Zudem wird unter Aufsichtsbehörden die Ansicht vertreten, dass der Prozess der Anonymisierung selbst unter die DSGVO fällt, was z. B. die Pflicht zu einer umfassenden Datenschutzfolgenabschätzung auslösen kann.

7. Die Verarbeitung personenbezogener Daten ist in der EU …

a) **… grundsätzlich verboten, außer sie ist in der DSGVO ausdrücklich erlaubt.** Die DSGVO verbietet ganz generell die Verarbeitung von personenbezogenen Daten (sog. Verbotsprinzip). Gleichzeitig stellt sie Ausnahmen von diesem grundsätzlichen Verbot auf. In der rechtlichen Praxis ist diese Unterscheidung von großer Bedeutung, wenn es um die Beweislast geht. Damit keine Bußgelder fällig werden, muss die verantwortliche Person beweisen, dass die Verarbeitung personenbezogener Daten zulässig war. Im Zweifel wird sonst gegen sie entschieden.

8. Unter welchen Voraussetzungen kann die Verarbeitung personenbezogener Daten doch erlaubt sein?

b)d) Die Verarbeitung personenbezogener Daten kann erlaubt sein, wenn **ein berechtigtes Interesse besteht** oder **wenn sie zur Erfüllung eines Vertrages (mit der betroffenen Person) erforderlich ist.** Daneben gibt es weitere Erlaubnistatbestände. Bekannt ist vor allem die Zulässigkeit der Verarbeitung personenbezogener Daten aufgrund des Vorliegens einer Einwilligung. Art. 6 normiert jedoch weitere Erlaubnistatbestände. „Belanglose“ oder

„lediglich historische“ Daten kennt die DSGVO nicht. Sobald ein Personenbezug gegeben ist, unterfallen Daten – unabhängig von ihrer Wertigkeit oder Sensibilität – dem Regelungsregime der DSGVO.

9. Welche Anforderungen bestehen hinsichtlich der Wirksamkeit einer Einwilligung?

a)b)c)d) Alle Antworten **(Freiwilligkeit**, **Informiertheit**, **Ausdrücklichkeit**, **Widerrufbarkeit)** sind richtig. Die Wirksamkeit einer Einwilligung ist an hohe Anforderungen geknüpft. Neben den vier genannten Voraussetzungen muss zudem die Einwilligungsfähigkeit vorliegen. An eine besondere Form ist die Einwilligung hingegen nicht geknüpft. Aus Nachweisgründen sollte sie jedoch dokumentiert werden. Das kann schriftlich, elektronisch oder durch die Aktennotiz eines*r Zeug*in erfolgen. Weil die Einwilligung grundsätzlich jederzeit widerruflich ist, stellt sie eine Herausforderung und gewissermaßen eine Rechtsunsicherheit für die Verantwortlichen des Datenverarbeitungsprozesses dar. Zudem kann das Einholen einer Einwilligung rechtswidrig sein, wenn sie für den konkreten Verarbeitungsvorgang nicht erforderlich ist. In diesem Fall bestünde bereits eine andere Rechtsgrundlage und es läge keine Freiwilligkeit vor. Daher sollte bei der Verarbeitung personenbezogener Daten zuerst geprüft werden, ob ein anderer Rechtsgrund – wie ein vertraglicher oder gesetzlicher Anspruch oder ein berechtigtes Interesse – vorliegt. Nicht jede Verarbeitung personenbezogener Daten braucht eine Einwilligung. Ihre Abfrage ist meist nur sinnvoll, wo wirklich kein anderer Rechtsgrund zu finden ist.

10. Was wird nicht in der DSGVO geregelt?

b)c)d) In der DSGVO werden weder **besondere gesetzliche Zulässigkeitsvoraussetzungen für Scoring-Verfahren**, noch **Schadensersatzansprüche aufgrund von benachteiligenden Entscheidungen die durch Softwareanwendungen getroffen wurden**, noch **die rechtliche Handhabung von „Daten als Entgelt“** geregelt. Die DSGVO reiht sich neben anderen Gesetzestexten ein. So wird z. B. das Scoring in § 31 BDSG definiert. Es gelten zwar die allgemeinen Regelungen der DSGVO, aber in Deutschland bestehen für den Spezialfall weiterhin die besonderen Voraussetzungen des Bundesdatenschutzgesetzes (BDSG). Auf Grundlage der DSGVO können keine Schadensersatzansprüche wegen eines diskriminierenden Ergebnisses eines Verarbeitungsprozesses von Daten geltend gemacht werden. Es gilt diesbezüglich in Deutschland das Allgemeine Gleichbehandlungsgesetz (AGG). Ob Daten rechtlich als Gegenleistung gelten können war umstritten. Klarheit hat die Verabschiedung der Digitale-Inhalte-Richtlinie 2019 gebracht, die noch in deutsches Recht umgesetzt werden muss. Die Zulässigkeit von automatisierten Einzelfallentscheidungen ist in Art. 22 der DSGVO geregelt. Ab wann eine Entscheidung als ausschließlich automatisiert gilt, ist jedoch in den Details noch unklar.

33 Punkte oder mehr:
Datenschutzcrack

Wow, Sie kennen sich sehr gut aus. Nicht mal die mitunter trickreichen Fragen konnten Sie irritieren. Toll, dass Menschen wie Sie sich so für das wichtige Thema Datenschutz interessieren.

28-32 Punkte:
Datenschutzbeauftragte

Sie kennen Sich gut aus. Sind sie vielleicht in Ihrer Organisation die mit der Einhaltung des Datenschutzes beauftragte Person? Sie hätten auf jeden Fall gute Voraussetzungen dafür.

27-16 Punkte:
Datenschutzinteressiert

Sie haben schon mal von der DSGVO gehört und konnten auch einige Fragen richtig beantworten. Ein paar Fragen haben Sie aber doch verunsichert. Ein Glück finden Sie auf den nächsten Seiten eine hilfreiche Checkliste zum Thema Datenschutz.

15 Punkten oder weniger:
Datenschutznewbie

Cool, dass Sie gerade das Quizz gemacht haben. Jetzt sollten Sie Sich das Thema genauer anschauen, es gibt noch viel zu lernen.

Datenschutz-Checkliste

Datenschutz ist unter der DSGVO als ein Prozess gemeint. Anders als der Begriff der **Check**liste suggeriert, ist Datenschutz kein Thema, das in kürzester Zeit abgehakt werden kann. Vielmehr ist eine kontinuierliche Beschäftigung mit den damit verbundenen Fragen und Herausforderungen gefordert. Die von uns entwickelte Liste versteht sich daher als stetige Begleiterin für ein datenschutzkonformes Verhalten. Sie ist eine strukturierte Erinnerung an die wesentlichen Voraussetzungen und ermöglicht eine regelmäßige Evaluation der eigenen Self-Data-Governance in Bezug auf Datenschutz. Sie ist so aufgebaut, dass sie sowohl von Organisationen genutzt werden kann, die sich bereits intensiv mit Datenschutz beschäftigt haben, als auch von Organisationen, die gerade erst ihr Datenschutzkonzept aufsetzten. Die Liste bietet eine umfassende Orientierung. Sollten Bereiche vollständig unbekannt und neu sein, ist eine tiefergehende Auseinandersetzung empfehlenswert.

Angesprochen werden von der DSGVO vor allem die „Verantwortlichen".

Der Ausdruck Verantwortliche bezeichnet „die natürliche Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet", Art. 1 Nr. 7 DSGVO.

Die Checkliste kann eine Rechtsberatung vorbereiten, ergänzen oder nachbereiten. Sie ersetzt jedoch nicht eine individuelle, juristische Beratung. Das liegt zum einen daran, dass Datenschutz ein komplexes Thema ist, welches oftmals nur in der Betrachtung des jeweiligen Einzelfalls gelöst werden kann. Zum anderen ist die Entwicklung des Rechtsgebietes Datenschutz dynamisch. Es fehlt noch an klärender Rechtsprechung, auch Technologie verändert sich laufend und selbst die Aussagen der verschiedenen zuständigen Datenschutzaufsichtsbehörden sind weder rechtsverbindlich, noch widerspruchsfrei. Daher kann bei komplexeren Fragen unter Umständen eine kontinuierliche Beratung geboten sein.

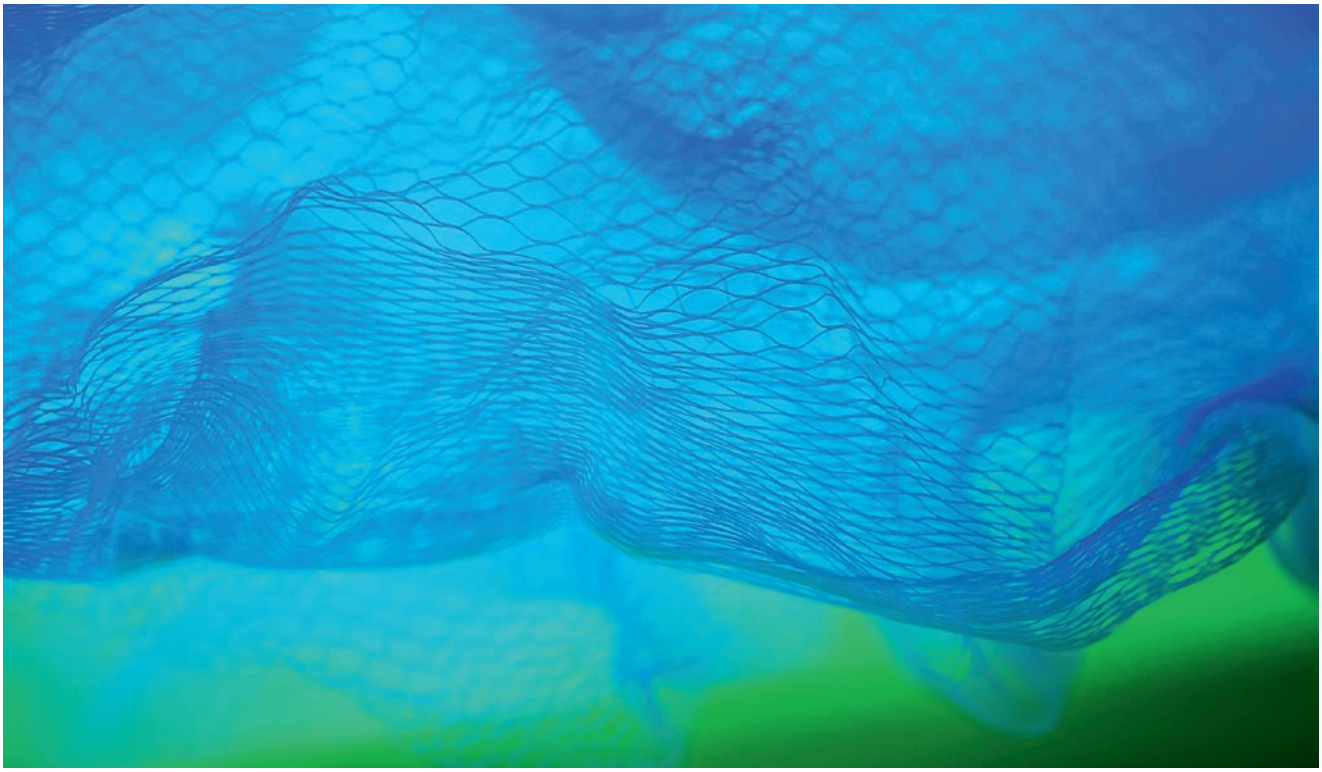


Foto: Pietro Jeng / Unsplash

DATENSCHUTZ-CHECKLISTE

DOKUMENTATION

1 DATENVERARBEITUNGSVERZEICHNIS

Sind alle datenschutzrelevanten Vorgänge identifiziert? Wer verarbeitet welche Daten zu welchem Zweck? Welche Rechtsgrundlage besteht jeweils?

2 DATENSCHUTZMAßNAHMEN

Wurde eine Übersicht aller Datenschutzmaßnahmen erstellt? Wird diese Übersicht oder ein ggf. vorhandenes Datenschutzkonzept regelmäßig aktualisiert?

UMSETZUNG VON PRINZIPIEN

10 GRUNDSÄTZE DER DATENVERARBEITUNG

Werden die Grundsätze der DSGVO bei allen Prozessen im Blick behalten?

11 ALLGEMEINE PFLICHTEN

Wurden datenschutzfreundliche Technikgestaltungen erwogen und ggf. umgesetzt (Privacy by Design)? Wurden alle Prozesse auf datenschutzfreundliche Voreinstellungen hin überprüft (Privacy by Default)?

REAKTIONS-MECHANISMEN

12 BETROFFENENRECHTE

Wer ist für die Erfüllung von Betroffenenrechten zuständig? Sind die Voraussetzungen geschaffen, sodass Ansprüche ggf. erfüllt werden können?

13 DATENSCHUTZVERLETZUNG

Welche Maßnahmen müssen ergriffen werden, wenn es zu einer Datenschutzverletzung kommt?

RAHMEN-BEDINGUNGEN

3 DATENSCHUTZSENSIBILITÄT

Besteht ein allgemeines Bewusstsein für das Thema Datenschutz? Wird Datenschutz regelmäßig in der Organisation thematisiert? Werden die dafür benötigten Ressourcen zur Verfügung gestellt?

4 ZUSTÄNDIGKEITEN

Wer aus der Organisation ist für was zuständig? Sind alle Verantwortlichkeiten geklärt?

5 TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

Ist die Datensicherheit gewährleisten? Ist sichergestellt, dass der Zugang zu Daten nur für berechtigte Personen möglich ist?

6 DATENSCHUTZBEAUFTRAGTE*R

Wird ein*e Datenschutzbeauftragte*r benötigt? Falls ja, wurde intern eine Person oder ein*e externe*r Berater*in ernannt? Werden die sonstigen Voraussetzungen dahingehend erfüllt, insbesondere die Aufsichtsbehörde über die Benennung zu informieren?

7 DATENSCHUTZFOLGENABSCHÄTZUNG

Besteht voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung der Daten? Wenn ja, wurde eine Datenschutzfolgenabschätzung (DSFA) durchgeführt?

8 BEACHTUNG BESONDERER ANFORDERUNGEN

Gelten Besonderheiten, z. B. weil besonders geschützte Daten verarbeitet oder personenbezogene Daten in Drittstaaten übertragen werden?

9 DATENSCHUTZHINWEISE

Wird regelmäßig und automatisiert eine Datenschutzaufklärung für alle Betroffenen vorgenommen? Ist diese präzise, transparent, verständlich und leicht zugänglich?

Vertiefende Hinweise zur Verwendung der Checkliste

Der Aspekt der Dokumentation steht bewusst am Anfang der Liste, da sie eine wesentliche Grundlage für die weiteren Schritte bildet. Außerdem normiert die DSGVO eine umfassende Rechenschaftspflicht in Art. 5 II. Das bedeutet im Zweifel muss von den Verantwortlichen belegt werden können, dass eine Verarbeitung rechtmäßig war. Es ist der Aufsichtsbehörde dann Einblick in die Dokumentation zu gewähren. Deswegen wird die Führung eines **Datenverarbeitungsverzeichnis** explizit in Art. 30 DSGVO gefordert. Dieses Verzeichnis stellt sicher, dass der Überblick über alle Prozesse behalten wird. Wichtig ist, dass wirklich alle relevanten Datenverarbeitungen erfasst werden. Das beinhaltet zum Beispiel auch analoge Datenverarbeitungen und solche, die durch einen Dritten in Form einer Auftragsdatenverarbeitung geschehen. Die dafür notwendigen Verträge und Dokumentationen sollten vorhanden sein.

Die kontinuierliche Dokumentation aller **Datenschutzmaßnahmen** wird regelmäßig unterschätzt. Im Falle einer Prüfung ist die Vorlage eines Datenschutzkonzeptes unter Umständen jedoch sehr wichtig. Zudem hilft es, selbst den Überblick zu behalten und den Datenschutz in der eigenen Organisation strukturiert anzugehen – und Erfolge zu identifizieren. Betont werden soll hier erneut der Prozesscharakter von Datenschutz – es reicht nicht aus, dieses Verzeichnis einmal anzulegen, um „den Datenschutz zu erledigen“.

Eine grundsätzliche **Datenschutzsensibilität** ist eine zentrale Rahmenbedingung für ein datenschutzkonformes Verhalten jeder Organisation. Eine regelmäßige Schulung der Mitarbeiter*innen ist sehr empfehlenswert. Darüber hinaus bieten sich z. B. regelmäßige Rundmails, Updates in Teamsitzungen oder etablierte Zeitslots, in denen Verständnis- und Nachfragen gesammelt besprochen werden, an. Die verschiedenen Maßnahmen können unterschiedliche Ressourcen (Zeit, Geld, Materialien, externe Expertise, o.ä.) voraussetzen. Wir empfehlen darüber hinaus, das generelle Framing von Datenschutz zu beachten: Eine rechtliche Verpflichtung klingt weniger attraktiv, als ein Beitrag zum Schutz der Grundrechte und Grundfreiheiten – und beeinflusst damit die Bereitschaft zur Auseinandersetzung mit der Thematik.

Von grundlegender Bedeutung sind klare **Zuständigkeiten** und Verantwortlichkeiten. Teilweise reicht eine einmalige Zuweisung (z. B. die Benennung einer Datenschutzbeauftragten) und teilweise muss kontinuierlich geprüft werden, welche Person jeweils verantwortlich ist (z. B. bei der Löschung von nicht mehr benötigten Daten). Die Etablierung von Prozessen, um etwa strukturiert Auskünfte an Betroffene erteilen zu können oder im Falle von Datenpannen innerhalb der geforderten 72 Stunden korrekt reagieren zu können, ist eine nicht zu unterschätzende Herausforderung in vielen Organisationen.

Um Datenschutzverletzungen vorzubeugen, sind Zugangsbeschränkungen essentiell. **Technisch-organisatorische Maßnahmen (TOM)** gem. Art. 24 DSGVO können auf den unterschiedlichsten Ebenen, sowohl analog als auch digital, etabliert werden. Dazu zählt zum Beispiel das zur Verfügung stellen von abschließbaren Büroräumen, die Verwendung sicherer Passwörter oder das Schreddern von Dokumenten vor der Entsorgung. Der Umfang der Maßnahmen sollte im Verhältnis zu dem Risiko der Datenverarbeitung stehen.

Jede Organisation sollte zu Beginn eine Bestandsaufnahme machen, um festzustellen, welche Voraussetzungen zu erfüllen sind. Die Benennung einer **Datenschutzbeauftragten** regelt Art. 37 DSGVO. In Deutschland wurde die 10-Personen-Regel gelockert: Sind mindestens 20 Personen in einer Organisation mit der automatisierten Datenverarbeitung beschäftig, muss eine Datenschutzbeauftragte schriftlich ernannt werden.

Um festzustellen, ob eine **Datenschutzfolgenabschätzung** gem. Art. 35 DSGVO nötig ist, muss eine Risikoanalyse vorgenommen werden. Das Risiko eines Datenverarbeitungsprozesses ergibt sich aus der Schwere des Schadens (Schutzbedarf) sowie der Eintrittswahrscheinlichkeit dieses Schadens. Alle Einträge des Datenverarbeitungsverzeichnis müssen überprüft werden. Besteht bei einem Prozess ein hohes Risiko, ist eine DSFA nötig. Wo sie tatsächlich notwendig ist, kann das erhebliche Aufwände auslösen.

Über die Verarbeitung von personenbezogenen Daten muss informiert werden. **Datenschutzhinweise** sollten für Kunden*innen, Geschäftspartner*innen und Arbeitnehmer*innen, aber auch die Webseitenbesucher*innen, Bewerber*innen und sonstige Dritte zur Verfügung gestellt werden. Bei der Erstellung der Information ist zu beachten, dass die DSGVO in Art. 12 bestimmte Anforderungen an die Inhalte stellt.

Die **Grundsätze der Datenverarbeitung** sind in Art. 5 DSGVO normiert und stellen eine wichtige Orientierung dar. Zum Beispiel sollte im Sinne der Datenminimierung überprüft werden, dass keine für die Erreichung legitimer Zwecke unnötigen Daten verarbeitet und nicht mehr benötigte Daten gelöscht werden. Die einzelnen Grundsätze beinhalten jedoch keine konkreten Handlungsanweisungen, sondern müssen interpretiert und mit Blick auf den spezifischen Kontext ausgelegt werden.

Durchaus bekannt sind die Stichwörter „Privacy by Design“ und „Privacy by Default“, die **allgemeinen Pflichten** von Verantwortlichen beschreiben und in Art. 25 DSGVO geregelt sind. Ersteres begrüßt zum Beispiel eine automatisierte Pseudonymisierung im Datenverarbeitungsprozess (stellt gleichzeitig eine TOM dar). Hingegen verbietet letzteres unter anderem vorangeklickte Kästchen bei Cookie-Einstellungen. So eingängig das Konzept, so sperrig erweist sich hier aber oft die Umsetzung im Detail. Daher ist oftmals schon im Designprozess die Einbeziehung von juristischem Sachverstand sinnvoll.

Eine Organisation muss sich auf mögliche Anfragen und Prozesse vorbereiten, zum Beispiel die Ausübung von **Betroffenenrechten**. Betroffene von Datenverarbeitungsprozessen können unterschiedliche Ansprüche geltend machen: ihr Recht auf Auskunft, auf Berichtigung, auf fristgemäße Löschung der verarbeiteten Daten, auf Einschränkung der Verarbeitung (Sperrung) oder das Recht auf Datenübertragbarkeit.

Für den Fall einer **Datenschutzverletzung** – also Unregelmäßigkeiten in der Verarbeitung der Daten, die zu einem Risiko für Betroffene führen können – sollte eine Art Notfallplan bereitliegen. In ihm sollte zum Beispiel notiert sein, wer in welchem Fall informiert werden muss. So werden Fristen hinsichtlich der Meldepflicht nicht versäumt.

Grundsätzlich gilt, dass Ressourcen sinnvoll eingesetzt werden sollten. Maßnahmen können daher nach Dringlichkeit bzw. Wichtigkeit (wenn z. B. ein Bußgeld oder die zeitnahe Ausübung von Betroffenenrechten wahrscheinlich ist) und der Aufwandseinschätzung für die jeweiligen Maßnahmen klassifiziert werden. Jede Maßnahme zur Sicherstellung des Datenschutzes ist ein Schritt in die richtige Richtung. Daher empfiehlt es sich mit einfachen und schnell umzusetzenden Schritten zu beginnen.

Schritt für Schritt zum Datenschutz

1. Ermittlung des aktuellen Standes der Datenverarbeitung: Welche Daten verarbeite ich?
2. Stand Datenschutz: Welche Datenschutzvorkehrungen habe ich bereits getroffen?
3. Notwendige Maßnahmen: Welche Maßnahmen fehlen noch?
4. Klassifizierung der Maßnahmen: Wie dringend und wie aufwändig ist die jeweilige Umsetzung?
5. Umsetzung der Maßnahmen: Wann setzte ich welche Maßnahmen um?
6. Evaluierungen: Befolge ich alle vorherigen fünf Schritte regelmäßig?

Das iRights.Lab

Das iRights.Lab ist ein unabhängiger Think Tank zur Entwicklung von Strategien und praktischen Lösungen, um die Veränderungen in der digitalen Welt vorteilhaft zu gestalten. Wir unterstützen öffentliche Einrichtungen, Stiftungen, Unternehmen, Wissenschaft und Politik dabei, die Herausforderungen der Digitalisierung zu meistern und die vielschichtigen Potenziale effektiv und positiv zu nutzen. Dazu verknüpfen wir in einem interdisziplinären Team rechtliche, technische, ökonomische, betriebswirtschaftliche und gesellschaftspolitische Expertise. Wir gestalten und begleiten Strategieprozesse, führen interdisziplinäre Analysen durch und entwickeln Handlungsempfehlungen. Wir möchten die inhaltliche Auseinandersetzung zu zentralen Fragestellungen der Digitalisierung fördern.

Die Begleitforschung des iRights.Lab zu Data-Governance bei datengetriebenen Innovationen läuft bis Ende 2020. Neben dem iRights.Lab beschäftigt sich auch die Begleitforschung des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) im Rahmen eines Arbeitsforums mit dem Thema Datenschutz und Compliance. Ziel der gesamten Begleitforschung des mFUND ist es, datenbasierte Innovationsprojekte zu unterstützen.

Siehe auch: www.irights-lab.de

Der mFUND

Im Rahmen der Forschungsinitiative mFUND fördert das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) seit 2016 Forschungs- und Entwicklungsprojekte rund um digitale datenbasierte Anwendungen für die Mobilität 4.0. Neben der finanziellen Förderung unterstützt der mFUND mit verschiedenen Veranstaltungsformaten die Vernetzung zwischen Akteuren aus Politik, Wirtschaft und Forschung sowie den Zugang zum Datenportal mCLOUD.

Siehe auch: www.mfund.de

Aufgrund der Corona-bedingten Sonderregelungen hat das BMVI einen kurzfristigen Förderaufruf speziell für kleine und mittlere Unternehmen (KMU) gestartet. Bewerbungen werden noch bis zum 15.07.2020 entgegengenommen. Näher Informationen finden Sie unter: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/neuer-mfund-aufruf-corona.html

Impressum

iRights.Lab GmbH, Schützenstraße 8, D-10117 Berlin

Telefon: +49 (0)30 40 36 77 230
Fax: +49 (0)30 91 68 18 49

E-Mail: kontakt@irights-lab.de
www.irights-lab.de

facebook: facebook.com/irights.lab
twitter: @irightslab
instagram: @irights.lab

Geschäftsführer: Philipp Otto

Registergericht: Amtsgericht Berlin-Charlottenburg, Registernummer: HRB 185640
Finanzamt Friedrichshain/Prenzlauer Berg | Steuer-Nr. 30/359/50503 | USt-IdNr.: DE311181302

Inhaltlich Verantwortlicher i.S.d. § 55 Abs. 2 RStV: Philipp Otto (Anschrift siehe oben)

Autorin: Levke Burfeind
Redaktion: Annika Albert, Dr. Wiebke Glässer, Philipp Otto, Michael Puntschuh

Gestaltung: tigerworx.de, Titelfoto: Jason Dent / Unsplash

Das Projekt „Data-Governance im Innovationsprozess“ wird gefördert vom Bundesministerium für Verkehr und digitale Infrastruktur im Rahmen des mFUND.
www.mfund.de

iRights.Lab
Think Tank für die digitale Welt