Bundesnetzwerk
Bürgerschaftliches
Engagement

DIGITALISIERUNG UND ENGAGEMENT: DATENSCHUTZ UND DATENSICHERHEIT ALS GRUNDRECHTSSCHUTZ

FORUM Nr. 3

FORUM NR. 3

DIGITALISIERUNG UND ENGAGEMENT: DATENSCHUTZ UND DATENSICHERHEIT ALS GRUNDRECHTSSCHUTZ

Die vorliegende Publikation ist die dritte Dokumentation des Projekts »Forum Digitalisierung und Engagement« des Bundesnetzwerks Bürgerschaftliches Engagement (BBE). Sie dreht sich thematisch um den Schwerpunkt „Datenschutz und Datensicherheit“, also im Kern um die Frage, wie Datenschutz und Datensicherheit nicht nur mit besseren Rahmenbedingungen für die Zivilgesellschaft versehen werden können, sondern vor allem, wie sie als Kernthemen für Freiheit und informationelle Selbstbestimmung künftig eine stärkere Rolle spielen können. Datenschutz und Datensicherheit müssen raus aus der Ecke der „lästigen Pflicht“ und zu einem der wichtigen Themen für die produktive Ausgestaltung von Engagementstrukturen werden.

ISBN 978-3-948153-16-8

INHALTSVERZEICHNIS

IMPRESSUM

HERAUSGEBER

Bundesnetzwerk Bürgerschaftliches Engagement (BBE)
Michaelkirchstr. 17/18
10179 Berlin-Mitte

☎ +49 30 62980 100
✉ info@b-b-e.de
🌐 https://www.b-b-e.de

REDAKTION DER PUBLIKATION
Dr. Serge Embacher, Anne-Kathrin Gräfe, Paula Jörres, Dana Milovanovic, Johanna Neuling, Teresa Staiger

REDAKTION DER REIHE
PD Dr. Ansgar Klein, Dr. Lilian Schwalb, Dr. Rainer Sprengel

V.I.S.D.P.
PD Dr. Ansgar Klein

LAYOUT/SATZ
Regina Vierkant (sevenminds)

ERSCHEINUNGSDATUM
Oktober 2021

ISBN 978-3-948153-16-8

Die Erarbeitung der vorliegenden Publikation erfolgte im Rahmen der Tätigkeit des Projekts »Forum Digitalisierung und Engagement« des Bundesnetzwerks Bürgerschaftliches Engagement (BBE). Die Arbeit des Projekts wird durch das Bundesministerium des Innern, für Bau und Heimat und die Robert Bosch Stiftung gefördert.

Bundesministerium des Innern, für Bau und Heimat

Robert Bosch Stiftung

ENTWICKELN. VERNETZEN. STÄRKEN.

Das Bundesnetzwerk Bürgerschaftliches Engagement (BBE) ist das Netzwerk für Zivilgesellschaft, Staat und Wirtschaft zur nachhaltigen Förderung des bürgerschaftlichen Engagements und der Bürgergesellschaft in allen Gesellschafts- und Politikbereichen.

VORBEMERKUNG

Das »Forum Digitalisierung und Engagement« ist ein Projekt des Bundesnetzwerks Bürgerschaftliches Engagement (BBE), bei dem es um grundlegende Verständigung über die Bedeutung des Digitalen Wandels für die organisierte Bürgergesellschaft in Deutschland geht. Über einen Zeitraum von zwei Jahren diskutieren wir mit den Mitgliedern des BBE – aber auch mit weiteren Interessierten aus den Sektoren Staat/Verwaltung, Wirtschaft/Unternehmen und Bürgergesellschaft/Non-Profits – über Perspektiven im Umgang mit Digitalisierung und „künstlicher Intelligenz".

Dass „Corona" auch im Feld der gemeinnützigen Organisationen einen Einstellungs- und Praxiswandel bewirkt hat, ist dabei nur ein Aspekt unter vielen. In erster Linie geht es um eine informierte und selbstbewusste Aneignung in actu – also mitten in einem unabgeschlossenen Prozess Digitaler Transformation, von dem wir sicher bislang nur wissen, dass er unumkehrbar ist. Dass es dazu gegenwärtig keine fertigen Positionen geben kann, sollte uns nicht vom Versuch einer selbstbewussten Mitgestaltung des Digitalen Wandels abhalten. Die geballte Expertise in Praxisfragen, die in den vergangenen Jahren in vielen Vereinen, Verbänden und Initiativen entstanden ist, wird dabei helfen, das eigene Handeln besser zu reflektieren und daraus Schlussfolgerungen für den Ausbau Digitaler Kompetenz zu ziehen.

Im April 2021 stand beim dritten (Online-) Dialogforum im Rahmen des Projekts das Thema „Datenschutz und Datensicherheit als Grundrechtsschutz" im Mittelpunkt der Diskussionen. Wie schon bei den ersten beiden Dialogforen (zu den Themen „Digitale Kompetenz" und „Organisationsentwicklung") standen die Teilnehmenden erneut vor der Aufgabe, ein vom Projektteam verfasstes Policy Paper zu diskutieren. Beim Thema Datenschutz wurde vor allem deutlich, dass die Schaffung besserer Rahmenbedingungen schon allein aufgrund der Komplexität des Themas ein schwieriges Unterfangen darstellt. In vielen gemeinnützigen Organisationen werden Datenschutz und Datensicherheit nach wie vor „mit spitzen Fingern" angefasst: teils, weil man sich hier nicht so gut auskennt, teils aber auch, weil die essenzielle Bedeutung des Umgangs mit Daten im elektronischen Zeitalter als Kern des Erhalts von Freiheit und Selbstbestimmtheit nicht hinreichend präsent ist.

Unser Forum und seine Diskussionen sollen dazu beitragen, hier weiterzukommen und die Zivilgesellschaft stärker für das Thema Datenschutz als Freiheitsthema zu sensibilisieren. Das Projekt und seine Dialogforen, die sich auch auf der Online-Plattform[1] wiederfinden, sollen hier als Katalysatoren dienen.

1 https://www.forum-digitalisierung.de/

VORBEMERKUNG

Im Folgenden dokumentieren wir:

- das Policy Paper „Datenschutz und Datensicherheit als Grundrechtsschutz“ in der abschließenden Fassung, das heißt nach Abschluss aller Kommentierungs- und Beteiligungsrunden,
- einen Kommentar von Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, in Zusammenarbeit mit Nils Leopold, LL. M.,
- einen weiteren Kommentar von Jochim Selzer, Chaos Computer Club,
- schließlich die Expertise „Datenschutz und Datensicherheit im bürgerschaftlichen Engagement“ von Daniel Burchardt, die eigens für das Dialogforum erstellt und dort präsentiert und diskutiert wurde.

Das Team des »Forums Digitalisierung und Engagement« bedankt sich bei allen Teilnehmenden der Veranstaltung für ihren Einsatz und die Bereitschaft, sich auf die intensive Diskussion im weiten Feld Datenschutz und Datensicherheit eingelassen zu haben. Unser Dank gilt außerdem den Autoren Ulrich Kelber, Nils Leopold, Jochim Selzer und Daniel Burchardt.

Serge Embacher
Leiter »Forum Digitalisierung und Engagement«

DR. SERGE EMBACHER, DANA MILOVANOVIC, TERESA STAIGER

POLICY PAPER „DATENSCHUTZ UND DATENSICHERHEIT ALS GRUNDRECHTSSCHUTZ“[1]

Dialogforum: Datenschutz und Datensicherheit als Grundrechtsschutz

Das Forum »Digitalisierung und Engagement« soll im zivilgesellschaftlichen Feld ein gemeinsames Verständnis des Digitalen Wandels erarbeiten. Das Projekt behandelt in einer Reihe von zweitägigen Dialogforen zentrale Aspekte des gegenwärtigen Digitalisierungsprozesses, der auch für das bürgerschaftliche Engagement und die organisierte Bürgergesellschaft mehr und mehr an Bedeutung gewinnt. Dabei verfolgt das Bundesnetzwerk Bürgerschaftliches Engagement (BBE) einen trisektoralen Ansatz, das heißt: Die organisierte Bürgergesellschaft sucht hier den kritisch-konstruktiven Austausch mit Staat und Wirtschaft. Die Dialogforen werden eingerahmt von einer Auftakt- und einer Abschlusskonferenz. Am Ende steht eine Dokumentation des Prozesses mit Handlungsempfehlungen für Politik, Wirtschaft und Bürgergesellschaft.

Das Dialogforum „Datenschutz und Datensicherheit als Grundrechtsschutz“ ist das dritte der Fachforen. Es wird online begleitet durch die seitens des BBE aufgesetzte Partizipationsplattform www.forum-digitalisierung.de.

1 Einige Passagen des Policy Papers entstammen der durch das Forum beauftragten Expertise zum Thema „Datenschutz und Datensicherheit im bürgerschaftlichen Engagement“ von Daniel Burchardt.

1 Bestandsaufnahme – Datenschutz und Datensicherheit als Grundrechtsschutz

Datenschutz und Datensicherheit sind zentrale Begriffe der Digitalisierung und haben ganz praktische Auswirkungen auf die Arbeit der bürgerschaftlich Engagierten. Sie sind für zivilgesellschaftliche Organisationen besonders im Hinblick auf die vielen personenbezogenen und teilweise sensiblen Daten, die bei der täglichen Arbeit entstehen, essenziell. Die Datenskandale der letzten Jahre, die Einführung der europäischen Datenschutz-Grundverordnung (DSGVO) und auch die Diskussionen um Datenschutz in der Corona-Pandemie haben wiederholt vor Augen geführt, welchen Einfluss Datenschutz und eine sichere Dateninfrastruktur auf unser gesellschaftliches Leben haben – und welch hohes Gut vor allem der Datenschutz darstellt. Datenschutz und Datensicherheit sind nichts weniger als Schutzmechanismen für Grundrechte.

Dies wird an zwei „Baustellen“ besonders deutlich:

- Personenbezogene Daten von Mitgliedern sowie von Haupt- und Ehrenamtlichen zu schützen, ist im Digitalen Wandel eine zentrale Aufgabe für jede gemeinnützige Organisation, weil es hier um die Sicherung demokratischer Grundbedingungen, die Abwehr wirtschaftlichen Schadens und die Bewahrung der Reputation von Vereinen, Verbänden und Initiativen geht.

- Die datengetriebenen Geschäftsmodelle (Online-Plattformen und -Anwendungen, -Bezahldienste etc.), auf die mittlerweile auch die meisten gemeinnützigen Organisationen zurückgreifen, produzieren und erheben in erheblichem Maße personenbezogene Daten und damit auch massenhaft Datenschutz- und Datensicherheitsprobleme.

Die beiden Begriffe – Datenschutz und Datensicherheit – werden oftmals vermischt oder fälschlicherweise synonym verwendet. Sie decken jedoch unterschiedliche Aspekte des übergeordneten Themas „Umgang mit Daten" ab. Daten*schutz* beschäftigt sich dabei mit dem rechtlichen Schutz personenbezogener Daten (zum Beispiel: Darf ich die Daten verarbeiten?), während Daten*sicherheit* die technischen Aspekte behandelt (zum Beispiel: Wie schütze ich diese Daten vor unbefugtem Zugriff, Verschlüsselung etc.?). Da die beiden Themenschwerpunkte im Umgang mit Daten eng miteinander verschränkt sind und auch ähnliche Ziele verfolgen, ist es dennoch sinnvoll, sie zusammen zu betrachten.

Datenverarbeitungsvorgänge in gemeinnützigen Organisationen sind sehr vielfältig. Sie umfassen unter anderem:

- die Verarbeitung personenbezogener Daten bei Veranstaltungen,
- die Mitgliederverwaltung,
- Spendenakquise und -verwaltung,
- die Internetpräsenz (Website),
- Mitarbeitenden- und Beitragsverwaltung,
- gegebenenfalls die Lohnabrechnung (inklusive sozialversicherungsrechtlicher Daten).

Während größere Organisationen dabei schon lange eine Vielzahl automatisierter Datenanwendungen nutzen, sind in Zeiten kostengünstiger IT-Angebote auch kleinere Organisationen zunehmend digital organisiert. Auch soziale Medien spielen eine zunehmende Rolle. Denn heute kommen auch kleinere Organisationen kaum ohne den Einsatz von privatwirtschaftlich betriebenen Plattformen aus (zum Beispiel Facebook, Amazon, Google).

Der Diskurs, vor allem um Datenschutz, war und ist nach wie vor von Unverständnis und teilweise einer gewissen Sorglosigkeit geprägt. Die Einführung der DSGVO im Mai 2018 sorgte auch in der organisierten Zivilgesellschaft für große Aufregung. Vereine, Organisationen und Initiativen schienen auf einmal zu bemerken, dass ihr Umgang mit Daten bisher unzureichend war. Viele Aktive sahen sich erstmals mit zunächst unverständlichen und sperrig erscheinenden Aspekten des Datenschutzes – wie etwa dem einer wirksamen Einwilligungserklärung, Datenschutzerklärungen für Websites oder gar Dokumentationspflichten – konfrontiert. Sanktionen und erwartete Abmahnwellen machten Angst und riefen Unverständnis hervor. Der Eindruck war, Datenschutz bedrohe das bürgerschaftliche Engagement und sei sowohl ein Hindernis als auch eine Gängelung für zivilgesellschaftliche Organisationen oder am Ende gar unnütz.

Dieser Eindruck ist – angesichts der Komplexität des Themas – verständlich. Dennoch sollte die Zivilgesellschaft den Datenschutz stärker als Chance begreifen und das auch gegenüber staatlichen Akteuren vertreten und einfordern: In einer Welt, die zunehmend von Daten dominiert wird, kann durch den Fokus auf Datenschutz Vertrauen in Staat und Wirtschaft, aber auch in zivilgesellschaftliche Organisationen gestärkt werden. Datenschutz und die DSGVO müssen als eine bürgerrechtliche Errungenschaft, die die Grundrechte (zum Beispiel das auf informationelle Selbstbestimmung)

schützt, und nicht als lästiger Auswuchs von Bürokratie verstanden werden.

Eine weitere Dimension des datenschutzfreundlichen und sicheren Umgangs mit Daten ist der Stellenwert der digitalen Souveränität – die einer Organisation, eines Unternehmens, eines Wirtschaftssystems oder eines Staates. Man denke nur an die Snowden-Enthüllungen, die gezeigt haben, dass die US-amerikanischen Techkonzerne, die eine marktbeherrschende Macht haben, mit Geheimdiensten zusammenarbeiten (müssen). Dieses und zahlreiche weitere Beispiele belegen, dass es notwendig ist, Datenschutz und Datensicherheit als Grundrechtsschutz aufzufassen und auch so zu behandeln (vgl. Schaar 2020, S. 7–15).

2 Analyse – Datenschutz und Datensicherheit als Grundvoraussetzung von Souveränität im Digitalen Wandel

2.1 Engagementdimension

Ein Umstand lässt sich nicht leugnen: Der kompetente und sichere Umgang mit Daten bringt für gemeinnützige Organisationen definitiv mehr Arbeit mit sich. Es sind neue Verpflichtungen geschaffen worden – etwa umfangreiche Informationspflichten sowie Dokumentationspflichten für sämtliche Unterlagen, Datenschutzerklärungen für die Webseiten, Einverständniserklärungen für die Erstellung und Veröffentlichung von Fotos etc. Vor diesem Hintergrund mag es verständlich sein, dass Datenschutz oft als eine lästige und dem Engagement hinderliche Pflicht dargestellt wird. Dennoch sind Datenschutz und Datensicherheit wichtige Grundrechte, welche es zu schützen und gemeinschaftlich auszugestalten gilt.

Digitales Sicherheitsbewusstsein und daraus resultierendes Sicherheitsverhalten sind bislang in Vereinen, Verbänden und Initiativen zu wenig ausgeprägt (vgl. entsprechende Untersuchungen von DsiN 2019). Bezüglich des Datenschutzes und der Datensicherheit fehlt eine fundierte Risikoeinschätzung, teilweise durch fehlendes Wissen, teilweise aber auch durch Achtlosigkeit und Fahrlässigkeit. Aufgrund von immer wieder öffentlich bekannt gewordenen Datenskandalen, der Komplexität und der technischen Aspekte des Themas herrscht allgemein große Verunsicherung.

Online-Tools werden oft pragmatisch eingeführt oder ad hoc in einer Krisensituation wie der Corona-Pandemie implementiert, wobei in der Eile oder aus Unwissenheit der Datenschutz oft missachtet wird. Dass Datenschutz aber integraler Bestandteil bei jeder Entscheidung für oder gegen ein (neues) Tool sein muss, wird oft vernachlässigt. Es ist ein stetiger Sensibilisierungsprozess, dieses Bewusstsein zu schaffen. Datenschutz darf nicht am Ende einer Entscheidung als lästiges Hindernis wahrgenommen werden, sondern muss am Anfang einer jeden Entscheidung stehen.

2.2 Fehlendes technisches Know-how

Da aber oftmals das individuelle Wissen über die verwendete Technik fehlt, lassen sich die Funktionsweisen und mögliche Datenschutzprobleme des jeweiligen Tools häufig nicht einschätzen. Problematisch ist aber auch, dass häufig einfach nicht klar zu sein scheint, was man darf und welche Tools man nicht benutzen sollte. Viele Tools werden von Datenschutzexpert*innen und Landesdatenschutzbeauftragten sehr unterschiedlich bewertet – aktuelles und bekanntes Beispiel stellt die Videokonferenzlösung Zoom dar. Hier bedarf es einer größeren Einheitlichkeit und somit bindender Standards.

Vermehrtes individuelles Wissen über den Umgang mit Daten würde staatliche

Empfehlungen unnötig machen bzw. würde für Individuen eine bessere Einordnung ermöglichen. Menschen müssen handlungsfähig gemacht werden, ihr Urteilsvermögen muss gestärkt und ihre bisherige Sorglosigkeit im Umgang mit Daten durch eine kompetente und souveräne Umgangsweise ersetzt werden. In einer zunehmend durch Daten geprägten Welt müssen wir alle tagtäglich bei der Arbeit und im Engagement Entscheidungen im Umgang mit Daten treffen. Wie bereits im Policy Paper zu „Digitale Kompetenz" beschrieben, bedarf es eines Konzeptes der „data literacy", die für Haupt- und Ehrenamtliche gleichermaßen wichtig ist. „Data literacy" bedeutet demnach „die Fähigkeit, planvoll mit Daten umzugehen und sie im jeweiligen Kontext bewusst einsetzen und hinterfragen zu können" (Schüller et al. 2021). Bisher wird dieser Ansatz nur im Hochschulkontext angewendet. Diese Schlüsselkompetenz des 21. Jahrhunderts sollte aber auch im allgemeinen Bildungskontext und in der engagierten Zivilgesellschaft Einzug halten.

Darüber hinaus ist es sinnvoll, in den Organisationen eine Person zu benennen, die etwa als „Datenschatzmeister*in" fungiert. Diese Person, gestützt durch den Vorstand und durch die Mitglieder, sollte das notwendige technische Know-how durch Fortbildungen erlangen können, um dann ein Datenschutzkonzept zugeschnitten auf die Bedarfe der jeweiligen Organisation zu erarbeiten. Die Benennung einer*s Datenschutzbeauftragten muss nicht in jedem Fall erfolgen, da diesem Amt laut DSGVO besondere Pflichten zugeschrieben werden, die für viele Vereine und Initiativen nicht realisierbar sind.

2.3 Informationsbedarf

Neben dem technischen Know-how braucht es mehr Informationsangebote und Kompetenzaufbau. Häufig gab es zum Inkrafttreten der DSGVO innerhalb von Verbandsstrukturen Angebote zur Information und zur Weiterbildung. Diese sollten nicht abgebaut, sondern vielmehr nachhaltig ausgebaut werden. Für Vereine, Organisationen und Initiativen, die außerhalb von Verbandsstrukturen arbeiten, gibt es einen noch größeren Informationsbedarf. Es braucht mehr leicht verständliche und schnell verfügbare Informationen (zum Beispiel in leichter Sprache) sowie eine Art Datenschutzhotline für verschiedene Zielgruppen. Auch kommt kompetenten und vertrauenswürdigen Mentor*innen eine immer wichtigere Rolle zu, um individuelles Wissen zu vermehren und Menschen handlungsfähig zu machen, damit sie sich auf ihr eigenes Urteilsvermögen verlassen können. Denn das ist besonders wichtig im souveränen Umgang mit Daten. Ohne ein gewisses Detailverständnis ist es schwierig, die Entscheidungen, die im Bereich Datenschutz und -sicherheit getroffen werden müssen, kompetent und informiert zu treffen.

2.4 Kommunikation

Man muss jedoch nicht nur die Kompetenz im Umgang mit Daten erhöhen, sondern auch die Kommunikation darüber ändern, um den Engagierten den Mehrwert, die Sicherheit und den Grundrechtsschutz zu demonstrieren, die ihnen ein angemessener und sinnvoller Datenschutz bietet – als Engagierte und als Bürger*innen. Wenn man nun noch den Aspekt der Datensicherheit dazu nimmt, ist ein ausgeprägtes Technologieverständnis oder zumindest ein Bewusstsein für diese Technologien und ihre Sicherheit entscheidend für den Organisationsalltag und für die Gestaltung des Digitalen Wandels im Sinne des Gemeinwohls. Fehlendes Wissen über Daten, Datenschutz und Datensicherheit sowie über die Konsequenzen des daraus resul-

tierenden Fehlverhaltens verhindert einen souveränen Umgang mit den Risiken, aber auch mit den Chancen der Digitalisierung.

Neben Kompetenzaufbau und Informationsangeboten ist weiterhin ein Dialog auf Augenhöhe über das Thema nötig, um sich auszutauschen, um Unsicherheiten zu reduzieren und um fortlaufend für die Wichtigkeit von Datenschutz und Datensicherheit zu sensibilisieren. Digitalisierungsprozesse sind in vielerlei Hinsicht – ob gesellschaftlich, wirtschaftlich oder sozial – so einschneidend, dass sie besonders den Diskurs mit der Zivilgesellschaft benötigen. Eine positive Kommunikation im öffentlichen Diskurs ist unumgänglich. Das Ziel sollte sein: eine sichere und selbstbestimmte Nutzung von digitalen Diensten und Technologien im Engagement und in der Gesellschaft. Das ließe sich durch Veranschaulichung der Risiken und Folgen unsicherer IT-Strukturen erreichen. Lücken im Datenschutz müssen anhand plakativer Beispiele anschaulicher gemacht werden – gepaart mit dem Aufbau Digitaler Kompetenzen in der Schulbildung, im lebenslangen Lernen und im Engagement als Lernort.

2.5 Politische Dimension

Eine Möglichkeit, sich dem teilweise berechtigten Unmut der Organisationen und der überwiegend ehrenamtlich Tätigen über den Umgang mit Daten anzunehmen, wäre es, die Anforderungen der DSGVO für Gemeinnützige anzupassen und leichter handhabbar zu machen. Derzeit gelten für Engagementorganisationen dieselben Vorschriften wie auch für Unternehmen, öffentliche Stellen und internationale Konzerne. Die Kirche ist von dieser Regelung ausgenommen und befugt, eigene Vorschriften zu machen (die sich in der Praxis aber alle im Kern an der DSGVO orientieren). Der Bericht der EU-Kommission zu „Zwei Jahre DSGVO“ im Sommer 2020[2] geht leider nicht auf den Handlungsbedarf in diesem Bereich ein. Hier gilt es nachzusteuern.

In diesem Spannungsfeld zwischen berechtigten Datenschutzanliegen auf der einen und den Bedenken und Sorgen aufgrund fehlender Kompetenzen und Ressourcenmangel der ehrenamtlichen Akteure auf der anderen Seite liegt eine Aufgabe für Politik, etwa durch finanzielle und/oder personelle Unterstützung und Ausnahmeregelungen. In jedem Fall muss der Staat Vereine und Organisationen in die Lage versetzen, die Datenschutzrichtlinien umzusetzen (finanziell und personell, zum Beispiel durch Weiterbildungsangebote).

Des Weiteren bedarf es strengerer rechtlicher Vorgaben nach dem Motto „data protection by design & by default“, das heißt: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, um Software- und Hardwarehersteller*innen stärker in die Pflicht zu nehmen, da die DSGVO diese bisher zu sehr außer Acht lässt (vgl. Wilhelm und Vogt 2020, S. 41–51). Auch muss die Politik strenger in der Durchsetzung gegen digitale Plattformen werden. Hier sind der Digital Services Act[3] und der Digital Markets Act[4] der EU-Kommission Schritte in die richtige Richtung.

Darüber hinaus muss die Politik im Diskurs über digitale Souveränität eine prägende-

2 COM(2020) 264 final vom 24.6.2020. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0264&from=EN (eingesehen am 15.4.2021).

3 COM/2020/825 final vom 15.12.2020. Online: https://eur-lex.europa.eu/legal-content/de/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN (eingesehen am 15.4.2021).

4 COM(2020) 842 final vom 15.12.2020. Online: https://eur-lex.europa.eu/legal-content/de/ALL/?uri=COM:2020:842:FIN (eingesehen am 15.4.2021).

re Rolle übernehmen. Denn eng verwoben mit dem Thema „Umgang mit der Datenverwendung“ ist die Problematik proprietärer Software, die oft Datenschutz im Sinne der DSGVO gar nicht erst ermöglicht. Besonders für kleinere Vereine und Initiativen ist hier aber die Kostenfrage oftmals entscheidend: Denn häufig erwecken die bekannten Tools multinationaler Konzerne den Anschein, es handle sich um kostenfreie oder zumindest vergünstigte Lösungen für gemeinnützige Organisationen, die dann aber wiederum nicht unbedingt datenschutzkonform sind. Es wird also auf die meist proprietären Tools zurückgegriffen. Die Monopolstellung einzelner multinationaler Konzerne hat demnach in letzter Konsequenz auch Folgen für die (engagierte) Zivilgesellschaft.

2.6 Offene Software

Hier ist das Stichwort „Open Source“ relevant, besonders aus der Perspektive der öffentlichen Hand. Um in der Zukunft weniger abhängig von den großen Anbieter*innen zu sein, müssen vermehrt Open-Source-Lösungen erarbeitet und entsprechend Mittel bereitgestellt werden. Es ist wichtig für die digitale Souveränität Deutschlands und der EU, dass die öffentliche Hand die digitale Infrastruktur nicht einfach der Privatwirtschaft überlässt.

Politik und Verwaltung sind derzeit selbst noch zu sehr in der proprietären Nutzung verhaftet, sollten aber vermehrt den Fokus und die Förderung auf offene Software legen – nach der Losung „Öffentliches Geld? Öffentlicher Code!“ mit einer eigenen Sicherheitsstruktur und DSGVO-konformen Datenschutzanforderungen. Offene Software ist dezentral, es wird Wert auf Datensicherheit und Privatsphäre gelegt, die Unabhängigkeit von großen Akteuren bleibt gewahrt und sorgt dadurch für die oft geforderte digitale Souveränität. Dafür muss es natürlich Standards geben und die Pflege und Kontrolle der Software muss durch eine Community gewährleistet werden. Hier kommt das bürgerschaftliche Engagement ins Spiel. Die digitale Community aus Entwickler*innen ist die beste Instanz zur Weiterentwicklung offener Software. Dieses digitale Engagement muss aber mit ausreichend Ressourcen ausgestattet werden. Oft fehlt es den Organisationen an finanziellen und personellen Ressourcen, um einen eigenen Server für Jitsi oder Big Blue Button zu finanzieren, geschweige denn diese Infrastruktur über eine lange Zeit sicher zu betreiben.

3 Konsequenzen – Bewusstsein stärken, Know-how ausbauen, Infrastruktur einfordern

Aus der Analyse des Status quo lassen sich eine Reihe von Handlungsempfehlungen für die Bürgergesellschaft, aber auch gegenüber Politik und Wirtschaft ableiten. Es geht darum, Strukturen und das Bewusstsein zu schaffen, um es gemeinnützigen Organisationen und Initiativen zu ermöglichen, im Umgang mit Daten kompetent, souverän und sicher zu agieren und den Digitalen Wandel mitzugestalten. Es bedarf einer aktiven, digital souveränen Zivilgesellschaft im Digitalisierungsdiskurs, um eine gemeinwohlorientierte Software- und Datennutzung zu realisieren. Nur so kann der Aufbau eines digitalen und der Allgemeinheit dienenden Ökosystems gelingen.

Forderungen an die Zivilgesellschaft:

- Sensibilisierung der Leitungs- oder Vorstandsebene für ihre juristische und moralische Verantwortung im Zusammenhang mit Datenschutz und Datensicherheit („Datenschutz ist Chef*innensache!“),

- Appell, bereits bei Vereinsgründung Datenschutz als zentrales Thema zu berücksichtigen, gegebenenfalls durch Benennung einer Datenschatzmeisterin bzw. eines Datenschatzmeisters,
- Etablierung dauerhafter Informations- und Unterstützungsangebote innerhalb und außerhalb von Verbandsstrukturen auch über zivilgesellschaftliche Strukturen hinaus (zum Beispiel Aufsichtsbehörden),
- zielgruppenorientierte Unterstützungsangebote durch Portale, die sichere, einheitlich zugeschnittene Lösungen bereitstellen, als eine Art Bausteinsystem, welches eine bestimmte Datenschutzqualität bietet (bundesweit, etwa nach dem Vorbild von https://www.digital-vereint.berlin),
- Gründung eines paritätisch besetzten Runden Tisches auf Bundesebene mit gemeinnützigen Organisationen, um Bedarfe zu identifizieren und Lösungen gemeinsam zu evaluieren oder um Systeme gemeinsam zu betreiben sowie um Peer-Learning-Möglichkeiten auszuschöpfen,
- Anregung zur Gründung mehrerer kommunaler Runder Tische zur Entwicklung lokaler Datenschutzkompetenz,
- kontinuierliche Ausbildung und Förderung von Mentor*innen und Einbindung dieser in die bestehende Engagementinfrastruktur (lokale Kompetenzzentren),
- niedrigschwellige, verständliche Angebote: Webinare, Selbstlernkurse, aber auch analoge Seminare vor Ort.

Forderungen an Staat und Wirtschaft:

- positiver, öffentlicher Diskurs über Datenschutz als Grundrechtsschutz (zum Beispiel durch Partnerschaft mit den Verbraucherzentralen),
- Informationsangebote und Aufklärungsarbeit durch eindrückliche Veranschaulichung der Gefahren durch Missachtung des Datenschutzes und der Datensicherheit (zum Beispiel analog zu den Kampagnen der Deutschen Verkehrswacht e. V. oder der Deutschen Lebens-Rettungs-Gesellschaft e. V.),
- digitale Infrastruktur in öffentlicher Hand und Förderung von offener Software unter Berücksichtigung datenschutzrechtlicher Bestimmungen,
- DSGVO-konformes Cloud-System für das Engagement,
- Schaffung kommerzfreier Räume für gemeinnützige Organisationen, zum Beispiel Entwicklung einer Shared-Service-Plattform, die der Zivilgesellschaft zur Verfügung gestellt wird und auch Kompetenzen im Umgang mit freier Software vermittelt (in Anlehnung an www.digital.vereint.berlin),
- Datenskandale in Politik und Verwaltung aufarbeiten und in Zukunft durch eine qualifizierte und sichere IT-Struktur vermeiden,
- Förderung des Technologieverständnisses anhand plakativer Beispiele, Abbau von Ängsten durch Vereinfachung und Veranschaulichung von Daten und ihrer Nutzung,
- Recht auf „Vergessenwerden“ durch Einführung eines obligatorischen Ablauf-/Verfallsdatums für Daten und gespeicherte Informationen,
- rechtliche Vorgaben nach dem Motto „data protection by design & by default“, um Software- und Hardwarehersteller*innen stärker in die Pflicht zu nehmen,
- strengere Durchsetzung des Datenschutzes bei digitalen Plattformen (zum Beispiel durch den Digital Services Act und Digital Markets Act auf EU-Ebene),
- Unternehmen in die Pflicht nehmen, ihre Produkte nachvollziehbar zu ma-

chen, zum Beispiel durch regulatorische Anforderungen, durch Neufassung von Vergabestandards sowie durch ein Zertifizierungsmodell für gemeinwohlorientierte Systeme (vgl. Beining 2019),
- Haftungsreduktionen bzw. -ausnahmen für ehrenamtliche Vorstände,
- Beratungspflicht von Aufsichtsbehörden wieder einführen,
- Förderung von Fort- und Weiterbildungsmaßnahmen,
- Engagementverträglichkeitsprüfung analog zur bereits bestehenden Kulturverträglichkeitsprüfung),
- Etablierung lokaler Kompetenzzentren unter Einbeziehung bestehender Engagementlandesnetzwerke (zum Beispiel angedockt an Bibliotheken, Stadtteilzentren, Volkshochschulen etc.),
- Übernahme von Beratungskosten (zum Beispiel angegliedert bei Verbraucherzentralen),
- verständliche Textfassungen von Datenschutzbestimmungen und Ansprechpartner*innen bei Hersteller*innen/ Anbieter*innen von Software als Ergänzung zu den rechtlich bindenden Textfassungen,
- Etablierung und Förderung eines gemeinwohlorientierten digitalen „Ökosystems“ durch Einbeziehung zivilgesellschaftlicher Akteure (zum Beispiel vermehrt freie Software in Vorhaben der öffentlichen Hand, Vermeidung von Monopolstellungen einzelner Anbieter*innen),
- Etablierung von Datenschutzpartnerschaften zwischen Unternehmen und zivilgesellschaftlichen Organisationen,
- „data literacy“-Programm in Bildungsprogramme integrieren,
- Aufforderung an die Aufsichtsbehörden, den Datenschutz einheitlich zu interpretieren,
- mehr Transparenzpflichten für Anbieter*innen von Software und anderen Internetlösungen (Welche Daten werden erhoben und was wird mit ihnen gemacht? etc.),
- Berücksichtigung personeller Mehrbedarfe für Datenschutz und Datensicherheit bei der Förderung von Organisationen und Projekten.

QUELLEN

- Beining, Leonie 2019: Wie Algorithmen verständlich werden. Ideen für Nachvollziehbarkeit von algorithmischen Entscheidungsprozessen für Betroffene, hg. v. Stiftung Neue Verantwortung/Bertelsmann Stiftung. Berlin/Gütersloh.
- DsiN (Deutschland sicher im Netz) 2019: SicherheitsIndex. Digitale Sicherheitslage der Verbraucher in Deutschland, 2. Auflage.
- Schaar, Peter 2020: Datenschutz-Grundverordnung: der neue Goldstandard. In: vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik, Nr. 231/232 [59(3-4)].
- Schüller, Katharina/Koch, Henning/ Rampelt, Florian 2021: Data-Literacy-Charta, Version 1.2, hg. v. Stifterverband. Berlin.
- Wilhelm, Maria/Vogt, Kira 2020: Goldstandard DSGVO: Zu hohe Datenschutzanforderungen für Vereine und kleine Unternehmen? In: vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik, Nr. 231/232 [59(3-4)].

PROF. ULRICH KELBER, NILS LEOPOLD

STELLUNGNAHME ZUM POLICY PAPER „DATENSCHUTZ UND DATENSICHERHEIT ALS GRUNDRECHTSSCHUTZ“

Ich bedanke mich für die Gelegenheit zum Austausch. Sowohl in der Analyse als auch in der Bewertung möchte ich Ihrem Positionspapier weitgehend zustimmen. Ich freue mich über die datenschutzfreundliche inhaltliche Positionierung des Bundesnetzwerks Bürgerschaftliches Engagement (BBE), die Betonung der Bedeutung des Datenschutzes für das Vertrauen in bürgerschaftliches Engagement und die durchgehend grundrechtsfreundliche Haltung. Damit beschreitet das Projekt »Forum Digitalisierung und Engagement« einen lobenswerten eigenen Weg im Verhältnis zu denen, die im Datenschutz nur zu oft allein ein bürokratisches Hindernis ihrer Tätigkeit sehen.

Ich bin mir bewusst, dass die Umsetzung der Datenschutz-Grundverordnung (DS-GVO) auch Ihnen sowie den beteiligten Netzwerkorganisationen einiges abverlangt haben dürfte. Umso mehr begrüße ich, dass Sie in Ihrer Positionierung gleichwohl so vehement für das Grundrecht auf Datenschutz und die informationelle Selbstbestimmung eintreten. Das zivilgesellschaftliche Engagement auch Ihrer Mitglieder trägt unsere Demokratie und verdient insgesamt entsprechende Förderung und auch Berücksichtigung bei Compliance-Anforderungen. Ich denke, dass insoweit auch politisch Spielräume für weitere Verbesserungen bestehen.

Dabei teile ich Ihre Analyse, dass gerade bürgerschaftliche Organisationen im Umgang mit den ihnen anvertrauten Informationen und Daten besondere Sorgfalt walten lassen sollten. Denn der Anspruch des Gemeinwohlbezuges geht allgemein mit hohen Integritätserwartungen durch die Öffentlichkeit einher. Bei politisch arbeitenden Organisationen kommt hinzu, dass Informationen und Daten mit Aussagekraft zu politischen Einstellungen und Engagement etwa der Mitgliedschaft besonderen rechtlichen Schutz beanspruchen. Besondere Risiken bzw. Schutzbedarfe für die verarbeiteten Daten von Personen können bei zahlreichen Organisationen des bürgerschaftlichen Engagements eine Rolle spielen. Und schließlich gilt allgemein: Auch kleine Einrichtungen können Verarbeitungen vornehmen, die tiefgreifende Auswirkungen auf die Rechte von Betroffenen haben.

Zugleich ist bekannt, dass bürgerschaftliches Engagement überwiegend auf ehrenamtlicher Leistung basiert. Und dass die Ressourcen in den allermeisten Fällen zumeist so knapp bemessen sind, dass neben der Verfolgung der eigentlichen Vereinsziele für zusätzliche Aufgaben – wie die Einhaltung rechtlicher Vorschriften/ Compliance – in der Regel nur wenige Mittel zur Verfügung stehen. Diese Situation trägt zu der von Ihnen angesprochenen schwierigen Situation realer oder wahrgenommener Abhängigkeiten ehrenamtlicher Verantwortlicher von den Angeboten der großen Plattformanbieter mit bei, darunter soziale Netzwerke, Messenger,

aber auch Datenhostingdienste etc. Genau deshalb ist es so bedeutsam, dass Möglichkeiten zur Bündelung knapper Ressourcen genutzt werden und Angebote zur gemeinsamen Nutzung bestehen.

Die DSGVO stellt eine übergreifende, unterschiedlichste Lebensbereiche erfassende Grundregelung dar. Das ist durchaus eine Errungenschaft, weil in ganz Europa im Prinzip nun einheitliche Regeln gelten. Richtig ist aber auch, dass die Risiken für die informationelle Selbstbestimmung der Bürgerinnen und Bürger je nach Lebensbereich, datenverarbeitender Organisation und Zwecksetzung ganz unterschiedlich verteilt sind. Die DSGVO lässt – vor allem hinsichtlich der Pflichten der Verantwortlichen aus Kapitel IV der DSGVO – gewisse Spielräume für risikoabhängige Differenzierungen, die auch und gerade Organisationen mit Gemeinwohlbezug zugutekommen können.

Gleichwohl sind weitere sachangemessene Anpassungen der DSGVO durchaus wünschenswert. Der Gesetzgeber selbst hat, wie Sie wissen, die Grenze für die Benennungspflicht von Datenschutzbeauftragten – auch unter Verweis auf die Bedürfnisse von Vereinen – erheblich heraufgesetzt. Doch am Ende braucht es vor Ort kompetente Ansprechpersonen. Ich finde es deshalb lobenswert, dass Sie mit der Idee des Datenschatzmeisters/der Datenschatzmeisterin eine zumindest ähnliche Funktion schaffen wollen.

Die unabhängigen Aufsichtsbehörden haben in ihrem zur ersten Evaluation der DSGVO vorgelegten Erfahrungsbericht weitere Erleichterungen für die Praxis und zur Alltagstauglichkeit vorgelegt, die bislang leider nicht aufgegriffen worden sind (vgl. DSK 2019). Ich gehe davon aus, dass die Aufsichtsbehörden auch zur kommenden zweiten Evaluierung der DSGVO weitere Forderungen mit Blick auf Erleichterungen für weniger risikoreiche Verarbeitungen und für Alltags- und Praxistauglichkeit vorlegen werden.

Die Übergangsphase bis zum Inkrafttreten der DSGVO und auch die Monate danach waren für uns Aufsichtsbehörden durch intensive Beratungstätigkeit aller Verantwortlichen geprägt. Mit unterschiedlichen Materialien und Formaten wie den sogenannten Orientierungshilfen haben wir Tools für die Umsetzung der DSGVO in der Praxis erstellt und veröffentlicht. Diese Arbeit der Datenschutzbehörden als Ansprechpartner sowie als Berater auch Ihrer Mitglieder (de facto Hotlines bieten trotz knapper Ressourcen insoweit alle Landesdatenschutzbehörden) zählt zu unserem gesetzlichen Auftrag und wird fortgesetzt – koordiniert erfolgt sie sowohl national auf der Ebene der Datenschutzkonferenz (DSK) als auch auf europäischer Ebene im Rahmen des Europäischen Datenschutzausschusses (EDSA).

Die nicht nur von Ihnen geäußerte Kritik am teilweise unabgestimmten aufsichtsbehördlichen Vorgehen wurde bereits aufgegriffen und aktuell werden Reformvorschläge diskutiert. Ich selbst setze mich für die Schaffung eines ständigen Sekretariats der Datenschutzkonferenz ein, um dem jährlich wechselnden Vorsitz Entlastung zu verschaffen und die Arbeit im Sinne einer einheitlichen Anwendung der DSGVO hier weiter zu professionalisieren.

Zur rechtsstaatlichen Verantwortung aufsichtsbehördlicher Tätigkeit auch gegenüber Organisationen des bürgerschaftlichen Engagements zählt ein verhältnismäßiges Vorgehen. Ich teile Ihre Bewertung, dass das Prinzip „Beratung vor Sanktion“ auch und gerade im Umgang mit ehrenamtlich tätigen und auf Gemeinwohlzwecke ausgerichteten Verbänden besondere Beachtung verdient.

Das allgemeine Problem breiter Nutzung von populären IT-Angeboten, gegen die zugleich grundlegende datenschutzrechtliche Bedenken bestehen, versuchen wir Aufsichtsbehörden zunächst bei der Wurzel zu packen: Entsprechende Verfahren gegen die Unternehmen und das Einwirken auf zuständige EU-Kollegen stehen im Mittelpunkt. Grundsätzlich unterstützen wir auch die weitergehenden politischen Pläne für mehr digitale Souveränität in Europa und mehr rechtliche Einhegung der Plattformanbieter. Entsprechend bringen wir uns – sowohl national als auch auf europäischer Ebene – zugunsten der Rechte der Bürgerinnen und Bürger in die Gesetzesverhandlungen ein. Die Entschließung der DSK zur digitalen Souveränität geht speziell auf Abhängigkeiten von IT-Produkten ein und stellt wie Sie die Bedeutung von Open Source in den Mittelpunkt (vgl. DSK 2020).

Ausdrücklich unterstützen wir Ihre pragmatischen Bemühungen, weitere Förderung für die Umsetzung von Datenschutz und IT-Sicherheit zu erwirken und durch gezieltes Zusammenlegen/Poolen der jeweils unterschiedlich verteilten Lösungskompetenzen und Ressourcen Verbesserungen zu bewirken.

Ich hatte vor diesem Hintergrund bereits vorgeschlagen, zum Beispiel Ehrenamtsserver mit datenschutzgeprüfter Software zu fördern und zu unterhalten, bei denen die Nutzenden nicht Gefahr laufen, gegen Vorschriften zu verstoßen. Ihre Vorschläge etwa für spezielle Cloud-Angebote scheinen mir in dieselbe Richtung zu gehen.

QUELLEN

- Datenschutzkonferenz (DSK) 2019: Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO. Online: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/98DSK_Erfahrungsbericht-DSGVO-Anwendung.pdf;jsessionid=F8ABA43A66C0797E262B1C992B050655.intranet231?__blob=publicationFile&v=4 (eingesehen am 27.7.2021).
- Datenschutzkonferenz (DSK) 2020: Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020. Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen. Online: https://www.datenschutzkonferenz-online.de/media/en/TOP%208%20Entschlie%C3%9Fung%20digitale%20Souver%C3%A4nit%C3%A4t_final.pdf (eingesehen am 27.7.2021).

JOCHIM SELZER

STELLUNGNAHME ZUM POLICY PAPER „DATENSCHUTZ UND DATENSICHERHEIT ALS GRUNDRECHTSSCHUTZ“

Das Ehrenamt ist der Fußabtreter in der Datenschutzhierarchie. Die Aktiven bekommen ein Blatt Papier in die Hand gedrückt, in dem ihnen ewiges Höllenfeuer angedroht wird, wenn sie auch nur den kleinsten Fehler begehen, und das nebenher ihre Dienststelle von jeglicher Verantwortung freispricht. Ein Beipackzettel verlangt faktisch von ihnen die Kenntnisse einer dreijährigen Fachinformatikausbildung sowie fundierte Jurakenntnisse, um halbwegs unbehelligt durch das Minenfeld des Datenschutzes zu navigieren. Bitte hier unterschreiben, dass Sie alles verstanden haben. Fortbildungen? Ach was. Unterstützung? Jetzt wollen wir mal nicht übermütig werden. Hauptamtliche bekommen oft wenigstens ein Dienstlaptop, das von der IT-Abteilung administriert wird. Ehrenamtliche können sehen, wo sie bleiben. So verbrennt man Engagement.

Darüber hinaus wird Datenschutz oft als ein reines Verwaltungsproblem missverstanden. Es geht, vermuten viele, vor allem darum, stapelweise Papier zu schwärzen, und schon stelle sich Datenschutz auf magische Weise von selbst ein. Sie zäumen dabei das Pferd falsch herum auf. Tatsächlich geht es darum, den Grundgedanken verstanden und verinnerlicht zu haben. Habe ich erst einmal begriffen, dass es ein Ausdruck von Respekt ist, meinem Gegenüber zu überlassen, was es mir von sich erzählen will, verhalte ich mich automatisch datenschutzkonform. Der Papierberg verschwindet dadurch nicht vollständig, aber er fällt quasi automatisch als Ergebnis meiner Arbeit ab und ist nicht deren Ausgangspunkt. Aus mir unbekannten Gründen geht dieser Aspekt in den meisten Datenschutzschulungen unter.

Was nicht untergeht, ist das Geschrei, welch Unbill der Datenschutz über die Menschheit gebracht hätte. Organisierte Kriminalität, Terrorismus, Corona-Pandemie, Klimakatastrophe – all das hätten wir schon längst im Griff, wären da nicht die ständig querschießenden Datenschützer. Eine wohlfeile Ausrede, perfekt geeignet, um vom eigenen Versagen abzulenken. Die Wahrheit ist deutlich komplizierter. Vor dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 hatte das Datenschutzrecht die Wirksamkeit einer Sonntagspredigt. Die Leute nicken, sagen „Amen“ und gehen raus, um sich den Rest der Woche nicht darum zu kümmern. Das hat sich geändert, wenn auch meist nur deswegen, weil die Leute sich vor den Strafen fürchten – Strafen, die so gut wie nie Privatleute, sondern meist millionenschwere Konzerne treffen. Was fehlt, ist die Einsicht, dass jede Spam-, jede Phishingmail, jedes geknackte Online-Konto und jeder unerwünschte Werbeanruf nicht etwa an zu viel, sondern an zu wenig Datenschutz liegt.

Ebenfalls oft missverstanden wird die Rolle der Datenschutzbeauftragten. Sie besteht weder darin, ein Namensschild ins Organigramm zu kleben und ansonsten

ergeben jede Eskapade einer Institution abzunicken, noch soll sie sich einen Berg Formalismen aus den Fingern saugen, um die praktische Arbeit maximal zu behindern. Ihre Aufgabe ist vielmehr die einer konstruktiven Nervensäge, einer Person, die sich Abläufe ansieht, ihren Kern zu verstehen versucht und am Ende sagt: „So funktioniert es leider nicht, aber hier ist ein Vorschlag, wie es funktioniert und gleichzeitig die Betroffenenrechte berücksichtigt werden."

Für die Meisten sind Computer nichts mehr als ein Werkzeug, das ihnen bei der Erledigung ihrer eigentlichen Arbeit helfen soll, ähnlich wie eine Sanitäterin den Rettungswagen für ihre Arbeit braucht und sich im Zweifel nicht darum kümmert, ihn zu warten und zu reparieren. Das allerdings verlangen wir von den Ehrenamtlichen – ohne PC-Führerschein und IT-Sicherheitstraining. Deswegen scheint mir eine „Datenschatzmeisterin" auch keine schlechte Idee zu sein. Sie sollte allerdings als Ergänzung, nicht als Ersatz verstanden werden. Weder enthebt sie die Mitarbeiterinnen ihrer Sorgfaltspflicht, noch kann sie die Fachkunde einer Datenschutzbeauftragten erreichen. Idealerweise ist die Datenschutzbeauftragte die Tippgeberin. Unabhängig und nicht weisungsgebunden schaut sie von außen auf die Abläufe einer Institution und sucht nach Verbesserungsmöglichkeiten. Sie muss dabei nicht einmal sagen, wie die Verbesserung konkret aussehen soll. Das könnte die Aufgabe der Datenschatzmeisterin sein, die allerdings ganz normal in den Betrieb eingebunden ist und sich von dort Anregungen sowie Kritik abholt. Am Ende liegt es an jeder Einzelnen, die von der Datenschatzmeisterin zusammen mit der Datenschutzbeauftragten erarbeiteten technischen und organisatorischen Maßnahmen zu leben. Es ist weder Anlass noch eine juristische Handhabe, zu glauben, zwei Dumme gefunden zu haben, die den Kopf hinhalten, während der Rest einfach weiterwurschtelt wie zuvor. Gleichzeitig muss auch klar sein, dass für eine wirksame Aufsicht mehr nötig ist als Lippenbekenntnisse wie „gestützt von Vorstand und Mitgliedern". Im Alltag bleibt davon wenig übrig. Es wird zu Versuchen kommen, rechtlich bedenkliche Messenger, Videokonferenzsysteme oder Webdienste einzusetzen. Es wird Zwischenfälle geben, bei denen Bewerbungsmappen in falsche Hände geraten. Mitarbeiterinnen werden – in bester Absicht – unzulässige Datensammlungen anlegen oder Mitschnitte vertraulicher Gespräche im Netz veröffentlichen. Für die dann entstehenden Konflikte braucht es eine Person außerhalb des Tagesgeschäfts, die im Zweifelsfall auch damit leben kann, sich im Rahmen ihrer Aufgaben nicht nur Freundschaften einzuhandeln. Eine Datenschatzmeisterin steckt dafür zu tief im Betrieb.

Insbesondere für finanziell eher knapp ausgestattete Vereine kann Freie Software Vorteile bringen. So ist es beispielsweise oft möglich, einen kommerziellen Dienst durch eine selbst gehostete Alternative zu ersetzen. Das ist nicht nur aus Datenschutzsicht attraktiv, sondern bietet für technisch interessierte Mitglieder neue Betätigungsfelder. Über die Schattenseiten sollten sich allerdings alle klar sein: Einen Server aufzusetzen und über die ersten euphorischen Wochen zu bringen, ist keine Kunst. Ihn dauerhaft in Betrieb zu halten, Aktualisierungen einzuspielen, abzusichern, Konfigurationsänderungen vorzunehmen, Support und leider oft genug Feuerwehr zu spielen, wenn wieder einmal etwas nicht funktioniert – das bringt wenig Spaß, bringt keinen Ruhm und wird vor allem dann lästig, wenn nachts um zwei Uhr jemand aufgeregt anruft, weil der Mailserver nicht erreichbar ist. Solche Anforderungen lassen sich nicht mit schönen Versprechen erfüllen, sondern mit Schicht-, Vertretungs- und Urlaubsplänen

– Dinge, die über klassisches Ehrenamt weit hinausgehen. Ob und wie Lösungen hierfür aussehen können, lässt sich eventuell mit dem nächstgelegenen Hackspace herausfinden. Gefragt ist jedoch auch die Politik, die sich häufig von großzügigen Hard- oder Softwarespenden der Quasimonopolisten blenden lässt, damit deren Stellung weiter zementiert und übersieht, dass Lösungen aus einer Hand zwar bequem sind, aber Abhängigkeiten schaffen, Handlungsoptionen einschränken und am Ende teuer werden können.

Handlungsbedarf – wenngleich wenig Aussicht auf Besserung – sehe ich beim Wunsch, die Vorgaben der einzelnen Landesdatenschutzbehörden zu vereinheitlichen. Das beginnt bei deren Aktivität (einige melden sich ständig zu Wort, während sich bei anderen die Frage stellt, ob der Posten überhaupt besetzt ist) und endet bei der schlichten Tatsache, dass neben Theologie wohl Jura das einzige Fach ist, in dem zu einem Sachverhalt mehr divergierende Ansichten möglich sind. Wenn sich 16 Bundesländer nicht einigen können, ob 1,5 oder zwei Meter Abstand in einer Pandemie sinnvoll sind, sollte es nicht wundern, wenn ein Bundesland MS 365 für Teufelszeug hält, während andere es ohne Widerworte durchwinken.

DR. DANIEL BURCHARDT

DATENSCHUTZ UND DATENSICHERHEIT IM BÜRGERSCHAFTLICHEN ENGAGEMENT

„Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. […]. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[1]

1 Zusammenfassung

Die Bedeutung des Datenschutzes nimmt in einer zunehmend datengesteuerten Welt immer mehr zu. Auch der Bereich des bürgerschaftlichen Engagements[2] kann sich dem schon allein aufgrund seiner Größe und gesellschaftlichen Bedeutung nicht entziehen; zumal in seinen vielfältigen Verarbeitungsprozessen nicht selten auch sensible Daten Gegenstand sind. Gleichwohl mangelt es häufig an der Bereitschaft und Kenntnis, um mit Daten verantwortungsvoll umzugehen. Dieser Beitrag umreißt zunächst die wesentlichen datenschutzrechtlichen Anforderungen, die jedes personenbezogene Daten verarbeitende bürgerschaftliche Engagement zu beachten hat, anhand der wesentlichen Grundbegriffe und Prinzipien des einschlägigen Rechts und schlägt zwölf Kernschritte zur Herstellung grundlegender Compliance vor.

In der Folge wird gezeigt, welchen Nutzen die Einhaltung der datenschutzrechtlichen Vorgaben mit sich bringt und warum sich daraus auch und gerade für die Zivilgesellschaft die notwendige Motivation zu ihrer Einhaltung gewinnen lässt. Neben der Be-

1 So das Bundesverfassungsgericht (BVerfG) in seinem für das gesamte Datenschutzrecht grundlegenden „Volkszählungsurteil“ vom 15. Dezember 1983, in dem es das *Recht auf informationelle Selbstbestimmung* prägte. Es erklärte Datenschutz damit zum *Grundrechtsschutz*. Gestützt wird das maßgebende Recht auf Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) in einer Kombination mit nicht weniger als der durch Art. 1 Abs. 1 GG geschützten Menschenwürde: Der Mensch darf nicht zum bloßen Objekt werden.

2 Der Begriff des bürgerschaftlichen Engagements geht über das Ehrenamt hinaus. Er wird hier daher in einem weiteren, dem Begriff der Zivilgesellschaft vergleichbaren Sinne benutzt, der hoheitliches Handeln kontrastiert und das freiwillige, nicht allein auf finanzielle Vorteile gerichtete und das Gemeinwohl fördernde Engagement von Bürger*innen zur Erreichung gemeinsamer Ziele bezeichnet.

wahrung positiver Reputation und der Abwehr wirtschaftlichen Schadens ist es die Sicherung der demokratischen Grundbedingungen jedes bürgerschaftlichen Engagements, das als besonderes Eigeninteresse motivationsbegründend wirken kann. Hiermit können konkrete Ansätze gewonnen werden, die die Akteure des bürgerschaftlichen Engagements strategisch im Rahmen ihrer Kommunikation und Organisationsentwicklung nutzen sollten. Insoweit werden eine Veränderung der Organisationskultur und die aktive Priorisierung des Themas Datenschutz und IT-Sicherheit empfohlen. In einem weiteren Schritt werden konkrete Handlungsempfehlungen für Politik, Aufsichtsbehörden und Verbände formuliert. Dabei wird klar, dass die Forderung von gesetzlichen Änderungen nur wenig Erfolg versprechend ist, dagegen aber der Ausbau gezielter Förderung ebenso im Vordergrund stehen sollte wie Kooperation und Arbeitsteilung sowie Beratung und Austausch.

2 Einleitung und Hintergrund

Persönliche Daten werden immer wertvoller. Ihre wirtschaftliche Verwertbarkeit steigt mit den immerfort wachsenden Möglichkeiten der Auswertung von Daten, namentlich von großen Datenmengen, stetig. Dieser Umstand bringt es aber auch mit sich, dass Daten immer mehr auch in einem zweifelhaften Sinne genutzt werden können. Dadurch droht zunehmend die merkliche Einschränkung von Freiheitsrechten der Bürger*innen. Ein anschauliches Problem besteht beispielsweise darin, dass spezialisierte Datenagenturen alle ihnen verfügbaren Daten über Bürger*innen sammeln und diese zur Erstellung einer „verdeckten Identität“ der erfassten Personen nutzen. Dies wird getan, um die persönlichen Eigenschaften und Eigenheiten von Bürger*innen feststellen und auswerten zu können, etwa ihre Interessen, ihre Ängste und Ziele. Im Erfolgsfall kann dadurch ihr Verhalten vorhergesagt werden, was wirtschaftlich, aber auch staatlicherseits von hohem Interesse sein kann.

Vielfach stammen die dafür genutzten Daten aus legalen Quellen. Viele Nutzer*innen von digitalen Anwendungen sind sich beispielsweise nicht darüber bewusst, dass die von ihnen auf Smartphone und Computer genutzten Anwendungen eine Vielzahl von Daten über sie sammeln und an die Anbieter*innen der Anwendung weiterleiten. Eine solche Weiterleitung ist insbesondere bei kostenlosen Anwendungen der Fall – hier zahlen die Nutzer*innen mit ihren persönlichen Daten, häufig ohne das zu wissen. Es ist allerdings auch anzunehmen, dass zum einen immer noch viele Datensätze missbräuchlich einfach weitergegeben werden, und zwar für Zwecke, für die sie ursprünglich nicht zur Verfügung gestellt wurden. Zum anderen dürften in die Datensätze der Datenverwertungsunternehmen auch solche Daten einfließen, die durch Datenlecks und auch Datenhacks illegal verfügbar gemacht worden sind. Dies freilich, ohne dass die aus- und verwertenden Unternehmen für das Leck oder den Hack im engeren Sinne verantwortlich sein müssen. In diesem Bereich ist in den letzten Jahren eine ganze Industrie neu entstanden, die aufgrund der lockenden hohen Erträge alle Mittel nutzt, um an Daten zu kommen und diese Aufkäufer*innen auf verschiedenen Wegen zur Verfügung zu stellen.

An den aufbereiteten Datensätzen sind nicht nur die schwarzen oder grauen Schafe interessiert. Auch seriöse Anbieter*innen, die Werbung gezielter anbringen wollen – wie etwa Versicherungen und Banken, die durch eine gezieltere Auswahl ihrer Kund*innen und entsprechende Tarif- bzw. Preisgestaltung wirtschaftli-

che Risiken minimieren wollen – und auch potenzielle Arbeitgeber*innen, die ihre Personalentscheidungen optimieren wollen, haben vielfach den Nutzen solcher Datensätze erkannt und setzen sie unmittelbar selbst oder mittelbar über spezielle Dienstleister*innen ein.[3] Natürlich ist die Gesetzgebung gefragt, bei unverhältnismäßigen Auswüchsen bestmöglich Abhilfe zu schaffen. Unter den Bedingungen globalisierter Vernetzung und Nutzung ist dies aber ein schweres Unterfangen. Und selbst ein denkbar restriktives gesetzgeberisches Handeln würde auf absehbare Zeit nicht alle Schwachstellen in der zivilen Nutzung von Daten beseitigen können. Datenschutz spiegelt vor diesem Hintergrund bereits heute ein wesentliches Freiheitsrecht der Bürger*innen, dessen Relevanz in Zukunft noch massiv zunehmen wird. Und schon heute sind 34 Prozent der Bundesbürger*innen Opfer von Datenmissbrauch im Internet.[4]

Daher hat das alles auch mit der Datenverarbeitung im Rahmen des bürgerschaftlichen Engagements zu tun. Denn auch dort werden personenbezogene Daten verarbeitet, die bei nicht ausreichendem Schutz dem Missbrauch dienen können. Und je intimer die Informationen sind, die im Rahmen des bürgerschaftlichen Engagements verarbeitet werden, desto höher fällt der potenzielle Schaden für die Beteiligten aus. Denn häufig sind Menschen gerade gegenüber bürgerschaftlich Tätigen besonders vertrauensvoll und bereit, sich mehr als sonst zu öffnen und Persönliches über sich preiszugeben. Aber egal, wie wichtig die Daten sind – das notwendige Sicherheitsniveau ist immer einzuhalten. Das Bundesverfassungsgericht hat mit seiner eingangs zitierten Entscheidung verdeutlicht, dass die Angabe personenbezogener Daten *nie belanglos*, der notwendige Schutz der Daten also immer zu respektieren ist. Denn die Daten gehören nicht den Verarbeitenden, sondern den Menschen, auf die sie sich beziehen.

3 Bestandsaufnahme

Allerdings fehlt es hierfür im Rahmen bürgerschaftlichen Engagements nicht selten an der notwendigen Bereitschaft. Der Datenschutz wird als Last,[5] mitunter sogar als *unnütze* Last angesehen. Er gilt jedenfalls häufig als die bürokratische Hauptlast schlechthin (vgl. Stiftung Aktive Bürgerschaft 2020). Siehe Abb. 1.

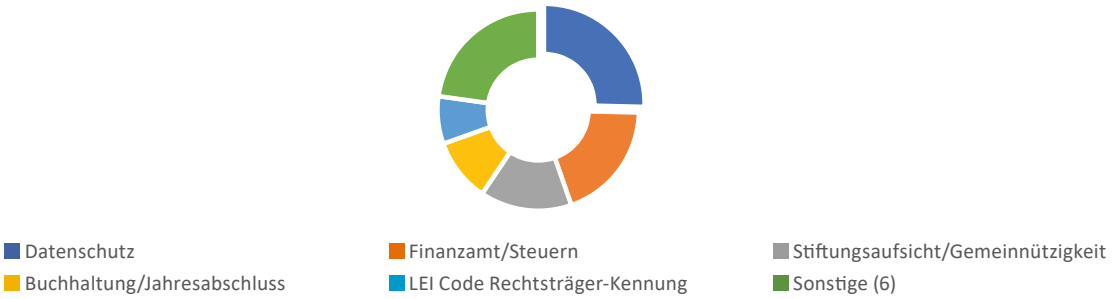
Zwar ist der Datenschutz kein von Grund auf neues Phänomen. Im Gegenteil: Bereits vor der Einführung der europäischen Datenschutz-Grundverordnung (DSGVO) im Mai 2018 bestanden im Bereich des zivilgesellschaftlichen Engagements erhebliche Probleme mit dem Datenschutz. Denn die Anforderungen haben sich in vielerlei Hinsicht nicht wesentlich verändert. Auch vor Inkrafttreten der DSGVO hatte Deutschland in relativer Hinsicht zu anderen europäischen Ländern eine recht anspruchsvolle Datenschutzgesetzgebung. Vieles daraus findet sich nun im europäischen Recht wieder. Mit Inkrafttreten der DSGVO ist der Datenschutz aber verstärkt ins öffentliche Bewusstsein vorgedrungen. Viele Ehrenamtliche sahen sich erstmals mit ihnen nicht selten unverständlich und sperrig erscheinenden Aspekten des

3 Eingehend zu den Bedrohungen der Grundfreiheiten, die mit der sogenannten *Data Mining Industry* und dem *Surveillance Capitalism* verbunden sind, siehe die EDRi-Publikation (o. J.).

4 https://de.statista.com/themen/4757/datenschutz-im-internet/ (eingesehen am 28.2.2021).

5 Siehe dazu die Stellungnahmen der Sachverständigen, die in der 71. Sitzung des Bundestagsausschusses für Familie, Senioren, Frauen und Jugend am 23. November 2020 gehört wurden. Online: https://www.bundestag.de/ausschuesse/a13/Anhoerungen#url=L2F1c3NjaHVlc3NlL2ExMy9BbmhvZXJ1bmdlbi84MDYzOTAtODA2Mzkw&mod=mod683976 (eingesehen am 12.3.2021).

ABB. 1: BÜROKRATIEHAUPTLAST NACH EINER UMFRAGE UNTER VERANTWORTLICHEN IM BÜRGERSCHAFTLICHEN BEREICH 2019
Quelle: Stiftung Aktive Bürgerschaft 2020, S. 2 f.



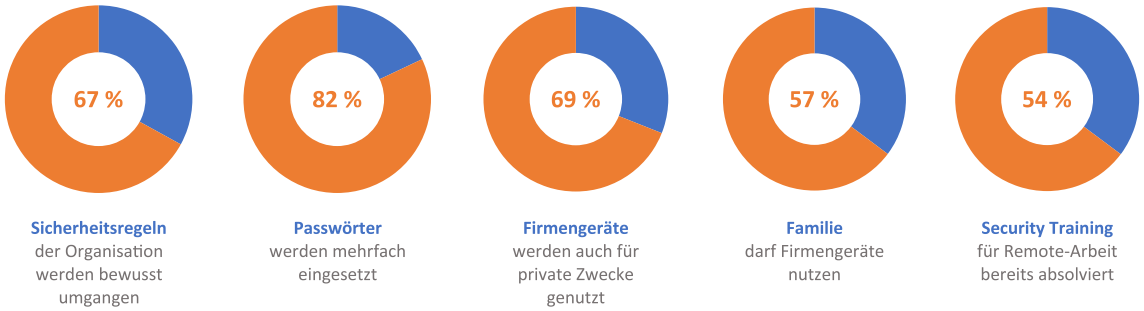
Datenschutzes – wie etwa eine wirksame Einwilligungserklärung, Datenschutzerklärungen für Websites oder gar Dokumentationspflichten – konfrontiert.

Im Jahre 2020 waren laut einer Studie des Meinungsforschungsinstituts Allensbach rund 17 Millionen Menschen in Deutschland ehrenamtlich, das heißt freiwillig und unentgeltlich, für eine Initiative, einen Verein oder eine andere Organisationsform tätig.[6] Das entspricht rund einem Fünftel der Bevölkerung. In den letzten Jahren hat es dabei einen recht signifikanten Anstieg gegeben.[7] Der Zulauf könnte sich verringern, sofern die Bestimmungen des Datenschutzes dauerhaft als übermäßig angesehen würden. Bei dauerhaft fehlender Akzeptanz der Regeln könnten sich womöglich viele Ehrenamtliche abgeschreckt fühlen.

Aber auch viele größere Unternehmen haben rund drei Jahre nach Inkrafttreten der DSGVO noch erhebliche Schwierigkeiten mit der Umsetzung der gesetzlichen Anforderungen. Dies zeigt schon die erhebliche Anzahl von mitunter signifikanten Bußgeldern, die von den Aufsichtsbehörden verhängt werden. Auch Erhebungen bestätigen den Eindruck, etwa im Zusammenhang zum Arbeiten im Homeoffice, das dem Setting nach bürgerschaftlichen Tätigkeiten mitunter nahekommt. Dort ist laut einer im Auftrag von Cyber Ark (2020) durchgeführten aktuellen Umfrage das Datenschutzverständnis nur schwach ausgeprägt. Siehe Abb. 2.

6 https://de.statista.com/statistik/daten/studie/173632/umfrage/verbreitung-ehrenamtlicher-arbeit/ (eingesehen am 15.2.2020).
7 Im Vorjahr lag die Zahl noch um rund eine Million tiefer (ebd.).

ABB. 2: DATENSCHUTZ IM HOMEOFFICE
Quelle: Cyber Ark 2020



Auffällig an den Ergebnissen der Studie ist, dass 54 Prozent der Befragten ein Security-Training bereits absolviert hatten.[8] Es ist daher davon auszugehen, dass die Verhältnisse im Bereich des bürgerschaftlichen Engagements nicht unbedingt besser ausfallen. Es fehlt oft schlicht die Manpower dafür bzw. die fachliche Kompetenz.[9] Dies wiederum untergräbt a priori das Aufkommen einer Kultur des Datenschutzes.[10] Denn das geringere Vorhandensein von Kompetenzen kann leicht in einen Teufelskreis führen. Es gründet nicht selten auf *mangelnden Erfahrungs- und Reflexionsmöglichkeiten* und bewirkt eine *geringere Selbstwirksamkeitserfahrung*, was wiederum in eine geringere Motivation mündet, sich mit dem Thema im Rahmen des persönlichen Engagements auseinanderzusetzen (vgl. Croll 2021, S. 4). Mitunter ist beispielsweise sogar die grundlegende Unterscheidung zwischen Datenschutz und Datensicherheit nicht bekannt.[11]

Mangelt es aber am digitalen Sicherheitsbewusstsein, kann Schaden leicht durch Acht- und Sorglosigkeit entstehen. Dazu passt, dass nach aktuellen Erhebungen nur 50 Prozent der Personen in Deutschland Sicherheitsvorkehrungen treffen, um ihre Daten im Internet zu schützen.[12] Und laut dem Hasso-Plattner-Institut (HPI 2020) war auch 2020 immer noch „123456" das meistgenutzte Passwort, nach wie vor gefolgt von „123456789". Als die *Top-6-Risikofaktoren* werden im privaten Bereich derzeit von Expert*innen die folgenden Punkte gehandelt: Siehe Abb. 3.

8 Da es eher unwahrscheinlich ist, dass an der Qualität solcher Trainings ganz generell zu zweifeln wäre, ist allem Anschein nach ein singuläres Training nicht ausreichend. Darauf wird an geeigneter Stelle (Kapitel 7.1.) noch einmal zurückzukommen sein.

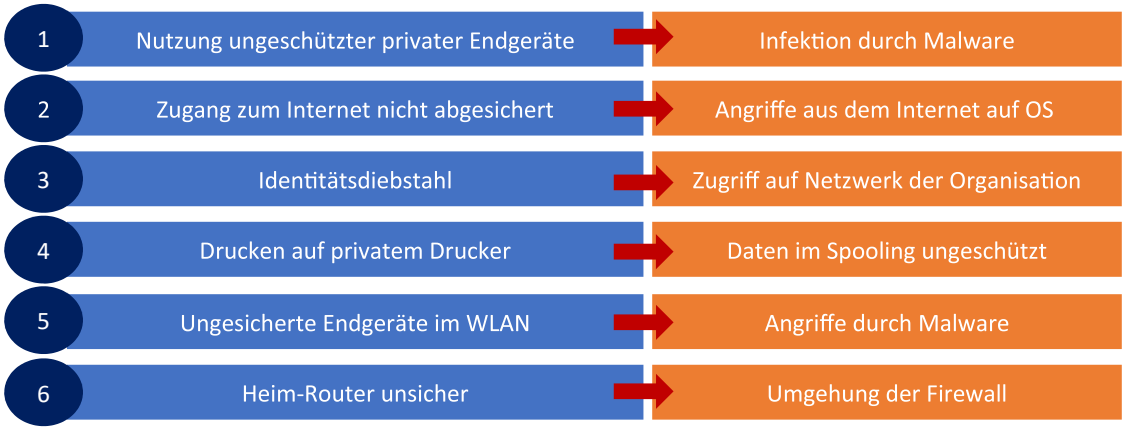
9 Das zeigt sich besonders beim Thema Verschlüsselung. Zwar ist diese nicht immer unbedingt nötig. Daten werden aber häufig auch dann unverschlüsselt gespeichert, wenn ihre Sicherung durch Verschlüsselung – wie etwa bei Gesundheitsdaten oder Minderjährige betreffende Daten – eindeutig angezeigt ist und im Extremfall schwerwiegende Folgen haben könnte.

10 So lassen sich etwa die Ergebnisse einer Umfrage bei der AWO verstehen (Grünecker 2021, S. 4 f.).

11 Der Datenschutz beschreibt den Schutz des Einzelnen vor der Beeinträchtigung seines Persönlichkeitsrechts durch den Umgang mit seinen Daten (*Schutz der Person*). Die Datensicherheit will den Schutz vor ungewolltem Datenverlust (zum Beispiel durch Defekt einer Festplatte, Verlust eines Speichersticks oder Brand) sicherstellen (*Schutz der Daten*). Die Datensicherheit ist regelmäßiger Teil des Datenschutzes, geht aber auch darüber hinaus.

12 https://de.statista.com/themen/4757/datenschutz-im-internet/ (eingesehen am 28.2.2020). Immerhin halten nur 7 % das Internet für sicher, wenn es um ihre persönlichen Daten geht (ebd.). Das sind aber immer noch 7 % zu viel.

ABB. 3: TOP-6-RISIKOFAKTOREN IM PRIVATBEREICH
Quelle: Rohde & Schwarz 2021



Zivilgesellschaftsspezifische Datenverarbeitungsvorgänge sind vielfältig. Sie umfassen typischerweise insbesondere die Verarbeitung personenbezogener Daten für Veranstaltungseinladungen, die Mitgliederverwaltung, Spendenwerbung und -verwaltung, den Öffentlichkeitsauftritt im Internet (Website) und die Mitarbeitenden- und Beitragsverwaltung sowie gegebenenfalls die Lohnabrechnung mitsamt der Handhabung sozialversicherungsrechtlicher Daten.[13] Während größere Organisationen dabei schon lange eine Vielzahl automatisierter Datenanwendungen nutzen, sind in Zeiten kostengünstiger IT-Angebote auch kleinere Organisationen zunehmend digital organisiert. Auch die sozialen Medien tragen gewissermaßen hierzu bei. Denn heute kommen auch kleinere Organisationen kaum ohne den Einsatz von Plattformen wie Facebook und Messengern wie Whatsapp aus. Im Newsletter-Bereich wird zunehmend auf Adressdaten verarbeitende Dienstleister wie Mailchimp gesetzt und auch Petitionslisten finden sich heute häufig nur noch digital.

Wird dem Datenschutz im zivilgesellschaftlichen Bereich nicht die verdiente Bedeutung zugemessen, ist dies daher schon vor dem Hintergrund der schlichten Masse an verarbeiteten Daten ein Problem. Datenschutz ist eine gesamtgesellschaftliche Aufgabe. Und die *Gemeinwohlorientierung* des bürgerschaftlichen Engagements prädestiniert diesen Bereich dazu, sich entsprechend seiner Bedeutung auch zu beteiligen. Dadurch wird sichergestellt, dass personenbezogene Daten in allen Lebensbereichen gleichermaßen geschützt sind.

13 „Verarbeitung" meint alle mit Daten denkbaren Vorgänge, wie das Speichern (zum Beispiel im Posteingangsordner), das Löschen, Verändern, Übertragen etc. Alle üblichen Datenverarbeitungen im Bereich des bürgerschaftlichen Engagements fallen darunter.

4 Die wesentlichen datenschutzrechtlichen Anforderungen[14]

Auch bürgerschaftlich Engagierte und die sie beschäftigenden Organisationen sind zur Abwehr der besonderen Schadensgeneigtheit der ungeschützten Verarbeitung personenbezogener Daten verpflichtet, den datenschutzrechtlichen Vorschriften (im Allgemeinen sind das die europäische Datenschutz-Grundverordnung [DSGVO] und das Bundesdatenschutzgesetz [BDSG], ergänzt durch Landesdatenschutzgesetze und gegebenenfalls bereichsspezifische Regelungen) zu folgen.[15] Dabei spielt auch keine Rolle, ob eine Organisation als gemeinnützig anerkannt ist, ob sie deutschlandweit oder nur lokal handelt, ob sie nur ehrenamtliche oder auch hauptberufliche Kräfte hat: Werden personenbezogene Daten verarbeitet, greifen die datenschutzrechtlichen Vorschriften. In der Praxis sind damit *nahezu alle Organisationen* betroffen, denn bereits die Verwaltung von Mitglieder- oder Interessentendaten löst datenschutzrechtliche Verpflichtungen aus – wobei auch die Größe der Organisation keine grundsätzliche Rolle spielt.[16] Entgegen einem weit verbreiteten Irrglauben sind die Regeln auch dann einzuhalten, wenn kein*e Datenschutzbeauftragte*r bestellt werden muss.[17]

14 Natürlich können hier nur erste allgemeine Hinweise geliefert werden. Eine abschließende Darstellung der Anforderungen kann dabei nicht erfolgen. Jede einzelne Konstellation ist in der Praxis für sich zu bewerten.

15 Ausnahmen bestehen im Ergebnis auch nicht für kirchliche Einrichtungen. Diese können zwar im Rahmen der ihnen nach Art. 91 DSGVO eingeräumten Möglichkeit der Eigengesetzgebung Regelungen in eigener Regie erlassen. Diese dürfen aber dabei das Datenschutzniveau der DSGVO nicht substanziell unterschreiten.

16 Unterschiede können sich aber beispielsweise im Hinblick auf die Pflicht zur Bestellung einer Datenschutzbeauftragten ergeben. Die Grenze liegt nach § 38 Abs. 1 S. 1 BDSG bei zwanzig Personen, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

17 Die Pflicht, eine Datenschutzbeauftragte zu bestellen, dürfte – zumal nach der Anhebung der Schwellenanzahl in § 38 Abs. 1 S. 1 BDSG auf zwanzig Personen – nur in selteneren Fällen greifen.

Die Vorschriften zum Datenschutz legen fest, dass *jede Verarbeitung personenbezogener Daten*[18] *grundsätzlich verboten* ist. Zumindest betrifft dies automatisierte und teilautomatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind bzw. gespeichert werden sollen. Schon diese Definition kann auf viele undurchsichtig wirken. Im Grunde lässt sich aber sagen, dass in der Praxis *nahezu jede organisierte*, das heißt allgemein vorgesehene Verarbeitung personenbezogener Daten das Kriterium der relevanten Speicherung erfüllen wird.

Ausnahmen von dem *Verarbeitungsverbot* bestehen nur insoweit, als

- die berechtigte Person, auf die sich die personenbezogenen Daten beziehen, ihre *Einwilligung*[19] *in die Verarbeitung erteilt* hat, *oder*
- eine *Rechtsvorschrift die Verarbeitung erlaubt*.

Die Einwilligungserklärung hat eine grundlegende Bedeutung im bürgerschaftlichen Engagement. Um wirksam zu sein, muss sie *„informiert"* und *freiwillig* erfolgen. Die einwilligende Person muss über Zweck und Umfang der Einwilligung vollständig in Kenntnis gesetzt und darf nicht unlauter beeinflusst worden sein (zum Beispiel durch Täuschung oder bei Ausnutzung eines Machtgefälles). Die Einwilligung sollte *dokumentiert* werden.

Wichtig für bürgerschaftlich Engagierte ist zudem häufig, dass sie *dem Datengeheimnis* unterliegen, also *zur Verschwiegenheit verpflichtet* sind. Oft wird dazu eine *Verschwiegenheitsverpflichtungserklärung* abzugeben sein. Insbesondere dürfen Kenntnisse über personenbezogene Daten, die Engagierte im Rahmen ihrer Tätigkeiten, etwa

- im persönlichen Gespräch oder durch
- Einsicht in Akten, Dateien, Listen und sonstige Dokumente und Datenträger oder
- durch Beobachtung

gewonnen haben, *nicht weitergegeben* werden. Mitunter kann eine Verletzung

18 Personenbezogene (oder besser: auf Personen beziehbare) Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu gehören unter anderem: Namen, Geburtsdatum, Adresse, Beruf, Einkommen etc. Es gibt darüber hinaus *besondere Kategorien* von Daten. Dazu gehören Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (vgl. § 9 Abs. 1 DSGVO). Besondere Kategorien personenbezogener Daten sind *besonders schützenswert*. Deren Verwendung unterliegt daher *höheren Anforderungen*. Der Unterschied der beiden Kategorien von Daten kann in der Praxis wesentlich sein. Zum einen kommt es durch die Kataloge des § 9 Abs. 2 DSGVO bzw. § 22 Abs. 1 BDSG (sowie in besonderen Ausnahmefällen gegebenenfalls spezialgesetzliche Regelungen) zu einer *erheblichen Eingrenzung der möglichen Gründe der Verarbeitung*. Zum anderen muss sich das einzuhaltende *Schutzniveau* der Bedeutung der Daten und der daher möglichen Schadenstiefe anpassen. In bürgerschaftlichem Zusammenhang sind solche Daten insbesondere im Zusammenhang mit der Mitgliedschaft in oder Spende für eine Organisation mit entsprechender Ausrichtung (politisch, religiös, weltanschaulich, im Zusammenhang zur sexuellen Orientierung, dem Vorliegen einer Behinderung etc.) denkbar. Bereits die Tatsache der Mitgliedschaft bzw. der Spende stellt dann ein sensibles Datum dar.

19 Um wirksam zu sein und jedes Missverständnis über ihren Umfang zu vermeiden, muss die Einwilligungserklärung immer so *konkret* wie möglich formuliert sein. Die Einwilligung kann nämlich immer nur zu einem bestimmten Zweck erteilt werden, der in Inhalt und Umfang klar erkennbar sein muss. Wichtig ist, dass Zweifel an der Freiwilligkeit einer Einwilligungserklärung leicht deren Unwirksamkeit begründen können. Die Einwilligungserklärung sollte schon aus Transparenz- und Dokumentationsgründen immer schriftlich bzw. in Textform abgegeben werden. Sie kann jederzeit widerrufen werden.

der Verschwiegenheitspflicht sogar strafrechtlich relevant sein.[20] Hierüber sind Engagierte besonders gut durch die Leitung der Organisation, für die sie tätig sind, aufzuklären und entsprechend anzuleiten. Engagierte haben zu beachten, dass das Datengeheimnis auch nach der Beendigung der bürgerschaftlichen Tätigkeit fortbesteht.

Neben der Einwilligung ist im bürgerschaftlichen Bereich oft auch als Rechtsgrund zur Datenverarbeitung die *Anbahnung eines Vertrages* (zum Beispiel bei Beantragung einer Mitgliedschaft) oder die *Vertragserfüllung* (zum Beispiel Durchführung der Mitgliedschaft oder Weiterreichung der Daten im Rahmen einer Petition, Bearbeitung von Daten bei Spende) wichtig. Die Initiative muss dabei grundsätzlich von der betroffenen Person ausgehen. In einigen Fällen kommt als Rechtsgrund allerdings auch das *berechtigte Interesse* in Betracht. Hier kann die Initiative auch von der Organisation ausgehen (zum Beispiel zur Einwerbung von Folgespenden). Dann ist vor der Verarbeitung eine *Interessenabwägung*[21] vorzunehmen, die die vernünftigen Erwartungen der betroffenen Person berücksichtigt. Die Abwägung ist zu dokumentieren. Es ist nicht möglich, den Rechtsgrund im Nachhinein auszutauschen (Verstoß gegen Transparenz und Fairness [Treu und Glauben]).

Werden Daten besonderer Kategorien verarbeitet, kann es sein, dass gemäß § 38 Abs. 1 S. 2 BDSG i. V. m. Art. 35 Abs. 3 lit. B DSGVO eine *Datenschutzfolgenabschätzung* notwendig wird, die dabei obligatorisch zur Bestellung einer*eines Datenschutzbeauftragten führt. Hierin findet auch bereits ein wesentlicher Grundsatz des Datenschutzrechts Ausdruck: der *risikobasierte Ansatz*. Je größer das Risiko, das für die Betroffenen durch die Verarbeitung eintreten kann, desto höher muss das Schutzniveau ausfallen.

Wie groß das Risiko aber auch immer ist. Die folgenden *wesentlichen Prinzipien* haben für alle Datenverarbeitungen Geltungsanspruch:

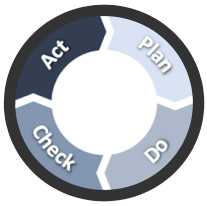
- *Fairness*: Alle Verarbeitung hat sich an Treu und Glauben zu orientieren;
- *Rechtmäßigkeit*: Jede Verarbeitungstätigkeit muss über ihren Zweck auf eine Rechtsgrundlage zurückzuführen sein;
- *Zweckbindung*: Daten können nur für den angegebenen Zweck verarbeitet werden;
- *Transparenz*: Die betroffene Person muss wissen, was mit ihren Daten passiert;
- *Datenminimierung*: Die Verarbeitung muss sich auf die zur Zweckerreichung unbedingt notwendigen Daten beschränken;
- *Richtigkeit*: Die Daten müssen richtig sein und sind nötigenfalls zu korrigieren;
- *Speicherbegrenzung*: Die Daten werden nur bis zum Entfallen des Rechtsgrundes der Verarbeitung bzw. bis zur Zweckerreichung gespeichert;
- *Integrität und Vertraulichkeit*: Die Daten sind angemessen zu schützen;
- *Rechenschaftspflicht*: Die Einhaltung der datenschutzrechtlichen Vorschriften ist nachzuweisen.

Am effektivsten können diese Prinzipien eingehalten werden, wenn dazu systematisch vorgegangen wird, das heißt ein *Datenschutz-Management-System* eingerichtet wird. Das heißt: Die Organisation der Abläufe dergestalt, dass die Einhaltung des Datenschutzes sichergestellt und do-

20 Insbesondere kommen Strafbarkeiten nach §§ 201, 201a, 202 sowie mitunter auch nach § 203 StGB in Betracht.

21 Zum Beispiel in Anlehnung an den *Legitimate Interest Assessment Test* der ICO.

kumentiert ist. Der wichtigste Punkt ist dabei, dass die Aufgabe Datenschutz eine *kontinuierliche* ist, die nie beendet werden kann, solange personenbezogene Daten verarbeitet werden. Daher ist immer wieder in einen *Überprüfungszyklus*[22] einzusteigen: Ist der Schutz der Daten einmal geplant worden, dann wird er nach einiger Zeit seiner Praxis einer Prüfung unterzogen. Notwendige Änderungen fließen dann in die erneute Planung ein etc.: Planen/Ausführen/Überprüfen/Ändern.[23]



Verantwortlich für Berücksichtigung und Nachhalten der oben genannten Prinzipien und der aus ihnen folgenden datenschutzrechtlichen Verpflichtungen ist bei juristischen Personen im Ergebnis[24] das Organ, das die betreffende Organisation rechtsgeschäftlich im Außenverhältnis vertritt – beispielsweise ist dies auf Vereinsebene der Vorstand. Bei Personenmehrheiten, die keine juristische Person bilden, sind diese grundsätzlich gemeinsam verantwortlich.

Die folgenden *zwölf Punkte* stellen die *wichtigsten Schritte* dar, die Verantwortliche im Rahmen des bürgerschaftlichen Engagements jedenfalls gehen sollten:

Schritt 1: Zur Erfüllung der Nachweispflicht sollte ein *Datenschutzordner* angelegt werden, in dem die gesamte Datenschutzdokumentation abgelegt wird. Auch sollten darin alle nennenswerten Datenschutzzwischenfälle aufgelistet werden.

Schritt 2: Die Verantwortlichen verschaffen sich einen *Überblick* über alle verarbeiteten personenbezogenen Daten[25] und beschreiben jeden Verarbeitungsvorgang in einem *Verarbeitungsverzeichnis*.

Schritt 3: Es ist zu prüfen, ob eine*ein *Datenschutzbeauftragte*r* zu bestellen ist.

Schritt 4: Es ist zu prüfen, ob eine *Datenschutzfolgenabschätzung* vorzunehmen ist. Diese ist in der Regel nicht erforderlich. Sofern durch die Datenverarbeitung aber ein höheres Risiko begründet ist, sollte die Durchführung einer *Datenschutzfolgenabschätzung* dokumentiert sein.[26]

Schritt 5: Es ist zu prüfen, ob für alle Verarbeitungsvorgänge ein *Rechtsgrund* gegeben ist. Dieser ist im Verarbeitungsverzeichnis jeweils zu hinterlegen.

Schritt 6: Es sollte die Möglichkeit der *Eingrenzung* der Verarbeitung unter Beachtung der Zweckbindung, Datenminimierung (-sparsamkeit) und Speicherbegrenzung geprüft werden.

22 Auch „PDCA-Zyklus“ (nach Plan/Do/Check/Act) oder „Demingkreis“ genannt.

23 Diese Herangehensweise entspricht den regulären Compliance-Grundsätzen. Datenschutzmanagement ist damit prädestiniert, nicht etwas Besonderes, sondern Teil einer effektiven und umfassenden Compliance-Struktur zu sein.

24 Genau genommen ist verantwortlich nach Art. 4 Ziff. 7 DSGVO die (natürliche oder) juristische Person (Behörde, Einrichtung oder andere Stelle), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, *selbst*.

25 Da datenschutzrechtliche Vorschriften nur greifen, wenn personenbezogene Daten verarbeitet werden, bedeutet dies im Umkehrschluss, dass für Verarbeitungsvorgänge, bei denen keine personenbezogenen Daten verarbeitet werden, die Vorschriften der DSGVO bzw. des BDSG auch keine Anwendung finden. Zwar ist in praktischer Hinsicht kaum denkbar, dass bei einer bürgerschaftlich tätigen Organisation überhaupt keine personenbezogenen Daten verarbeitet werden. Allerdings kann es schon durch die Möglichkeit der Unterscheidung zwischen solchen Datenverarbeitungsprozessen, die personenbezogene Daten beinhalten, und solchen, die dies nicht tun, durchaus zu Vereinfachungen kommen.

26 Insbesondere bei einer Verarbeitung besonderer Kategorien von Daten kann es durchaus ratsam sein, professionelle individuelle Beratung in Anspruch zu nehmen.

Schritt 7: Es sind proaktiv *Informationsmöglichkeiten* für die Betroffenen, die über Verarbeitungen und ihre *Rechte*[27] informiert werden müssen, ebenso zu schaffen wie die Möglichkeit der Geltendmachung von Betroffenenrechten (hierzu ist ein Prozess aufzusetzen).[28]

Schritt 8: Gegebenenfalls notwendige datenschutzkonforme *Auftragsverarbeitungsverträge* sind abzuschließen, sofern Dritte einbezogen werden, die nicht selbst verantwortlich sind, wie etwa die Steuerberatung. Bei Übermittlung in ein außereuropäisches Drittland ist besondere Vorsicht geboten.[29]

Schritt 9: Dem individuellen Risiko angemessene *Sicherheitsmaßnahmen* technischer und organisatorischer Natur sind zu implementieren. Dazu gehören insbesondere:

- *Schulung*[30] aller personenbezogene Daten verarbeitenden Engagierten und Mitarbeitenden;
- Einführung einer planhaften *Datenschutzrichtlinie*,[31] die mindestens all die in dieser Liste genannten Punkte abdeckt; jährlich sollte dabei die Erkennung und Behebung von Schwachstellen vorgesehen werden (*PDCA-Zyklus*);
- *Zugriffs- und Zutrittsbeschränkungen*; inklusive eines Passwortschutzes für einen abgetrennten Bereich auf einem privat[32] eingesetzten Gerät (Ausschluss anderer Mitnutzer*innen), Firewall und aktuellem Virenschutz (hierbei geht es im Wesentlichen um das Niveau, das informierte Lai*innen ohnehin schon zum Standard machen), Abschließen des Aktenschranks. Empfehlenswert kann[33] die geschützte Dokumentenverwaltung in der Cloud sein (bei DS-GVO-konformen Anbieter*innen);
- Einholen von *Verschwiegenheitsverpflichtungserklärungen/Verpflichtung auf das Datengeheimnis*.

Schritt 10: Ein *Prozess für den Fall einer Datenschutzverletzung* (Meldepflicht gegenüber der Aufsichtsbehörde) ist zu etablieren: Ist man in der Lage, den Eintritt einer Datenschutzverletzung zu erkennen und sich darum zu kümmern (persönliche Verantwortung)? Es muss (nachweislich) sichergestellt sein, dass die Aufsichtsbehörde grundsätzlich binnen 72 Stunden informiert wird, wenn es zu einer Datenschutzverletzung gekommen ist. Die davon betroffenen Personen müssen ebenfalls über die Verletzung informiert werden, sofern ein „hohes Risiko" für deren Rechte und Freiheiten besteht.

27 Betroffene haben das Recht auf Auskunft, Berichtigung, Löschung („Vergessenwerden"), Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch gegen die Verarbeitung (aus berechtigtem Interesse), Widerruf der Einwilligung und darauf, nicht einer automatisierten Entscheidungsfindung unterworfen zu sein.

28 Eine Vereinfachung kann es im Zusammenhang mit dem Recht auf Information beispielsweise sein, wenn Mitglieder auf eine abgesicherte Weise Einblick in die über sie gespeicherten Stammdaten über die Vereinswebsite erhalten und sie dort verwalten können.

29 Das europäische Datenschutzniveau darf nicht unterschritten werden. Dies ist vertraglich sicherzustellen, sofern kein Angemessenheitsbeschluss vorliegt.

30 Wie oben unter 3. bereits angesprochen, ist ein singuläres Training nicht ausreichend. Es sollte regelmäßig aufgefrischt werden.

31 Wenn die Aufsicht kommt, ist es auf jeden Fall gut, überhaupt etwas vorweisen zu können, selbst wenn noch nicht alles zu 100 % passt. Wenn aber die Aufsicht ein vollständiges Ignorieren der bestehenden Pflichten erkennt, kann schwerer Schaden für Organisation und Verantwortliche eintreten.

32 Wichtig ist zu verstehen, dass der Verantwortliche auch dann verantwortlich im Sinne des Datenschutzes bleibt, wenn Verarbeitungsprozesse auf den Geräten von Privaten durchgeführt werden.

33 Das ist nicht voraussetzungslos. Insbesondere ist der Anbieter angemessen mit einem Auftragsverarbeitungsvertrag zu verpflichten. Die Anbieterin ist sehr sorgfältig auszuwählen. Das Produkt muss zur Anwendung passen.

Schritt 11: Die Website der Organisation ist mit einer *Datenschutzerklärung* auszustatten. Die Nutzung von *Fotos* ist zu überprüfen.[34] Sofern Einbindungen in Social Media erfolgen, ist mit besonderer Vorsicht vorzugehen. Hier kann es im Hinblick auf die Verarbeitungen des *Social-Media*-Anbieters leicht zu einer gemeinsamen Verantwortlichkeit kommen, also dazu, dass auch die ehrenamtliche Organisation für diese Datenverarbeitung als verantwortlich angesehen werden kann. Das erhöht den Haftungsumfang so erheblich, dass im Regelfall ohne genaue Prüfung davon abzusehen sein wird.

Schritt 12: Insbesondere für Vereine empfiehlt sich zudem:

- Die Regelungen zum Datenschutz in der *Vereinssatzung* sollten gegebenenfalls angepasst werden.
- In den *Aufnahmeanträgen* neuer Mitglieder sollten einschlägige Regelungen zum Datenschutz enthalten sein; zusätzlich kann sich ein gesondertes Informationsblatt zur Information der Mitglieder über Nutzung und Verarbeitung personenbezogener Daten empfehlen.

Natürlich kann nicht jeder von einem Tag auf den anderen für verschlüsselte Festplatten, integeres, also unmanipulierbares Booten, für die Verschlüsselung der Informationsströme auf dem Transportweg, die starke Authentisierung aller beteiligten Kommunikationsendpunkte sowie die Einbindung in ein anspruchsvolles IT-Sicherheits-Management sorgen. Andererseits macht es aber auch keinen Sinn, den Kopf dauerhaft in den Sand zu stecken. Es muss eine *sinnvolle Balance* gefunden werden. Konkret sollte dabei der Vorteil des *risikobasierten Ansatzes* gesehen und genutzt werden. Sofern die Risiken gering sind, weil die Datenverarbeitung der Organisation nur mit einer sehr geringen Schadenswahrscheinlichkeit und geringer Schadenstiefe einhergeht, können schon wenige Maßnahmen zu einer angemessenen Absicherung führen, was auch ein wenig Entspannung bedeuten kann. Sofern aber ein größeres Risiko entweder aufgrund einer höheren Eintrittswahrscheinlichkeit oder aufgrund der Ausmaße des drohenden Schadens gegeben ist, sollte keine notwendige Mühe gescheut werden. Als *Merksatz* kann gelten: Je größer der mögliche Schaden für die Betroffenen, desto höher sind die Anforderungen an den Schutz der Daten. Dabei ist auch klar: Je stärker der Sicherheitsanspruch, desto geringer die Verfügbarkeit. Es muss also eine Lösung gefunden werden, die *betreibbar, beherrschbar und wirtschaftlich wie vom Aufwand her vertretbar* ein angemessenes Sicherheitsniveau bietet.[35] Bei Fragen kann die zuständige Aufsichtsbehörde kontaktiert werden, die meist helfend zur Seite steht.[36]

34 Ein Foto kann unter die Kategorie biometrischer Daten fallen, sodass die Verarbeitung von vornherein eines speziellen rechtlichen Grundes bedarf und besondere Vorsicht bei der Verarbeitung zu walten hat. Zudem grenzt das Kunsturhebergesetz die Veröffentlichung von Fotos stark ein, sodass diese in der Regel eine spezifische Einwilligung der abgebildeten Person erforderte. Denn da bei der Veröffentlichung eine Vielzahl von Personen auf das Foto zugreifen und es nachbearbeiten und verändern kann, ist das Interesse der berechtigten Person besonders zu berücksichtigen. Im Zweifel ist die Person also immer um ihre Einwilligung zu bitten, deren Widerruf jederzeit für die Zukunft möglich ist.

35 Wichtig ist auch, dass man bei aller besonderen Beachtung der technischen Einrichtungen und Abläufe den *analogen Bereich* nicht vergisst. Daten sollten zu Hause nicht ungeschützt Dritten zugänglich sein, auch unterwegs sollten Dritte keinen Einblick bekommen können (zum Beispiel bei unbedarftem Lesen in der Bahn).

36 Ein echter *Anspruch auf Beratung* steht aber nur einer Datenschutzbeauftragten zu, § 40 Abs. 6 S. 1 BDSG.

5 Nutzen des Datenschutzes für die Zivilgesellschaft sowie Darstellung möglicher Motivationen zur Anpassung einschlägigen Verhaltens

Datenschutz ist für bürgerschaftliche Organisationen schon im Hinblick auf die nicht selten sensiblen Daten, die im Rahmen des Engagements benötigt und erhoben werden, von entscheidender Bedeutung. Nicht nur, dass der Organisation durch die Nichtbeachtung des Datenschutzes schwerer Schaden unmittelbar sowohl finanzieller als auch personaler Natur drohen kann, wie gleich noch näher dargestellt wird. Auch der *Verlust der Reputation* ist mitunter von entscheidender Bedeutung. Sollte sich bei zu vielen Akteuren im Bereich des bürgerschaftlichen Engagements dauerhaft ein zu lockeres oder gar distanziertes Verhältnis zum Datenschutz durchsetzen und zum Standard werden, könnte der Reputationsverlust sogar auf jedes bürgerschaftliche Engagement zurückfallen. Die Zivilgesellschaft hat schon daher ein erhebliches *Eigeninteresse* an der Einhaltung des Datenschutzes. Und der Verlust des guten Rufes wäre selbst dann zu befürchten, wenn der Bereich des bürgerschaftlichen Engagements vom Datenschutz ausgenommen werden würde.[37] Denn die teilweise bereits vorhandene Wertschätzung des Themas Datenschutz,[38] die im Hinblick auf die Datengetriebenheit entscheidender Wirtschaftszweige sowie die noch zu erwartenden Datenskandale in ansehbarer Zeit noch erheblich ansteigen dürfte, würde jedes bürgerschaftliche Engagement von vornherein als problematisch erscheinen lassen.

Wie bereits angesprochen, wird Datenschutz zwar nach wie vor oft als lästige Angelegenheit behandelt, die nur zusätzlicher Auswuchs überbordender Bürokratie ohne eigenen Mehrwert ist. Allerdings schützt diese Kritik ebenso wenig vor Strafe wie Unwissenheit. Der Verlust des guten Rufes ist das eine. Sich aus Nachlässigkeit gegebenenfalls ergebende Haftungsfragen das andere. Verstöße gegen datenschutzrechtliche Bestimmungen können mit erheblichen Bußen geahndet werden. Ein Verstoß kann so im schlimmsten Fall eine kritische finanzielle Belastung der Organisation bedeuten. Eine persönliche und schlimmstenfalls sogar strafrechtliche Haftung der verantwortlichen Personen, beispielsweise des Vorstands, tritt dann womöglich noch hinzu.[39] Sicher ist es schwer zu erklären, dass jemand für sein ehrenamtliches Engagement auch noch in Haftung genommen wird. Dennoch ist das nicht ausgeschlossen.[40] Zwar ist die Wahrscheinlichkeit gering, dass die Aufsicht in kleinen Organisationen routinemäßig vorbeischaut, um sie zu kontrollieren. Allerdings kann es auch einfach sein, dass sich jemand beschwert. Das kann die Person sein, um deren Daten es geht. Es kann aber auch einfach jede dritte Person sein, die sich entweder aus guten Gründen um den Datenschutz in der Organisation sorgt oder ihr schlicht Böses will. Solchen Hinweisen/Anzeigen gehen die Aufsichtsbehörden grundsätzlich nach. Die Einhaltung eines angemessenen Datenschutzniveaus ist also auch daher notwendig, um Schaden von der eigenen Organisation, der für sie Verantwortlichen und mittelbar auch den Mitarbeitenden und Engagierten abzuhalten. Datenschutz ist so ein Teil des *Selbstschutzes der Zivilgesellschaft*.

37 Dies wäre in grundsätzlicher Hinsicht nur auf europäischer Ebene durch Anpassung der DSGVO möglich.

38 Bereits vor Inkrafttreten der DSGVO war nach einer YouGov-Umfrage die Mehrheit der Deutschen davon überzeugt, dass dem Datenschutz eine hohe Wichtigkeit zukommt. Online: https://www.sinusinstitut.de/fileadmin/user_data/sinus-institut/Bilder/news/Datenschutztag/Pressetext_Datenschutztag_SINUSYouGov.pdf (eingesehen am 5.3.2021).

39 Relevant ist regelmäßig immerhin eine ordnungswidrigkeitsrechtliche Haftung nach § 130 OWiG.

40 Zivilrechtlich ist die Haftung in vielen Fällen allerdings gemäß § 31a BGB beschränkt.

Und noch ein dritter, dreifaltiger Punkt ist wichtig; im Ergebnis sogar der wichtigste. Denn ein weiteres wesentliches Interesse der Zivilgesellschaft am Datenschutz ergibt sich schon aus der ihr von Natur aus *inhärenten Orientierung am Gemeinwohl*. Wer, wenn nicht sie, muss ein besonderes Interesse daran haben, dass den Bürger*innen kein Schaden droht – weder durch eigenes Handeln noch durch das Handeln anderer? Schon aus diesem Grund ist es wichtig, dass der bereits zahlenmäßig äußerst relevante Bereich des bürgerschaftlichen Engagements zur Etablierung eines *datenschutzsensiblen Gemeinsinns* beiträgt.

Die Digitalisierung kann ein sehr mächtiges Werkzeug zur Beteiligung, zur Einbindung, zur Teilhabe sein – entweder der Mitglieder und/oder eines Kreises von externen Interessierten. Sie kann dabei ein Werkzeug sein, die eigene Arbeit zu verbessern, zu erweitern und einem größeren Publikum vorzustellen. Die Digitalisierung und die Nutzung ihrer Vorteile und Chancen kann aber aufgrund der erheblichen Risiken nur gelingen, wenn mit ihr gleichzeitig ein *digitalisierungstypisches Mindset* Einzug hält, das den *Datenschutz als Selbstverständlichkeit* mit umfasst. Bleibt der Datenschutz außen vor, müsste à la longue mit einem verminderten Engagement der Bürger*innen gerechnet werden.

Den Grund dafür verdeutlicht das eingangs zitierte Bundesverfassungsgericht, das die potenziellen Gefahren eines zu geringen Schutzes klar vor Augen hatte: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare *Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens* ist.“

Allein schon insoweit hat also die Zivilgesellschaft quasi ein grundlegendes dreifaches Interesse am Datenschutz: Erstens als *Errungenschaft des mündigen Bürgers bzw. der mündigen Bürgerin*, dessen bzw. deren *Motivation zum Engagement* – zweitens – durch effektiven Datenschutz sichergestellt ist. Und – drittens – an einem dem Datenschutz zu verdankenden sicheren Einsatz digitaler *Werkzeuge* und einem aus diesem folgenden *Nutzen*.

Die Zukunft des bürgerschaftlichen Engagements im Hinblick auf die Digitalisierung zeigt sich also verschachtelt. Eine Zukunft des mündigen, engagierten Bürgers bzw. der mündigen, engagierten Bürgerin – die Grundlage jeder Zivilgesellschaft – lässt sich ohne eine eingehegte Digitalisierung nicht denken. Gleichzeitig ist der Digitale Wandel ein wesentlicher Erfolgsfaktor des bürgerschaftlichen Engagements in der Zukunft. Nur wenn die Digitalisierung als Gesamtprozess einerseits und die Teilha-

be der Bürgergesellschaft daran andererseits derart gelingt, dass Datenschutz und Datensicherheit gelingen, wird das bürgerschaftliche Engagement eine vielversprechende Zukunft haben.

6 Folgerungen für bürgerschaftliche Organisationen, insbesondere zu Kommunikation und Organisationsentwicklung

Ist das Eigeninteresse der Zivilgesellschaft am Datenschutz demnach offenkundig, fragt es sich, wie diese Erkenntnis *in der Breite des Engagements verankert* werden kann. Eines vorneweg: Kurzfristige Erfolge sind nicht zu erwarten. Es wird *Zeit und Aufwand* erfordern, in dieser Frage echte Veränderungen zu ermöglichen. Diese werden erst dann erreicht sein, wenn sich eine *Organisationskultur* herausgebildet hat, die Datenschutz als Selbstverständlichkeit ansieht und bei allen Prozessen von Anfang bis Ende automatisch mitdenkt.[41]

Für das Herausbilden einer solchen Kultur muss klar transportiert werden, dass *Datenschutz alle angeht*. Dabei ist darauf hinzuweisen, dass dem Träger des bürgerschaftlichen Engagements bei Nichteinhaltung ein schwerer Schaden drohen kann, ebenso wie auch dem bürgerschaftlichen Engagement insgesamt ein *Reputationsschaden* droht, wenn dem Datenschutz langfristig nicht die Bedeutung beigemessen wird, die ihm zukommt. Es könnte anderenfalls etwa dazu kommen, dass sich *Hemmschwellen* herausbilden, bürgerschaftliche Leistungen anzunehmen, daran mitzuwirken oder sie zu befördern. Zusätzlich ist die Erkenntnis wichtig, dass Datenschutz einen *Mehrwert* für die Organisation auch im Sinne der Vorbereitung auf das digitale Zeitalter bietet, mit dem die Organisation es dann – gewappnet mit neuen Wegen und Instrumenten zur Kommunikation und Organisation – aufnehmen kann.[42] Zudem ist die Einhaltung der Vorschriften ein *echtes Asset*, mit dem für die eigene Organisation *geworben* werden kann.

Erkennbar ist, dass dies alles eine entsprechende *Organisationsentwicklung* voraussetzt. Keine bürgerschaftliche Organisation wird daran langfristig vorbeikommen. Dies umso mehr, da in vielen Organisationen die Repräsentant*innen überkommener Strukturen nicht das notwendige Mindset dafür mitbringen, die Veränderungen zu schaffen. Einer solchen Organisationsentwicklung helfen die folgenden Punkte:

1. Datenschutz muss wichtig genommen werden: Datenschutz ist *Chefsache*;[43] die Wichtigkeit des Datenschutzes ist im Innen- wie Außenverhältnis unmissverständlich zu kommunizieren.

2. Jeder neu beginnenden bürgerschaftlich engagierten Person ist die Wichtigkeit *von vornherein* nahezubringen.

3. Das Themenbewusstsein muss regelmäßig *aufgefrischt* werden. Die Motivati-

41 Dies meinen die Grundsätze Privacy by Design (Datenschutz ist schon in der Gestaltung [eines Prozesses] von vornherein angelegt) und Privacy by Default (die Standards [einer Prozessvorgabe] sind datenschutzsicher). Die Einhaltung bewirkt zum einen, dass die Datenverarbeitung von Anfang an mit einem geringeren Risiko belastet ist. Zum anderen sind dadurch spätere Veränderungen an den Prozessen deutlich leichter datenschutzkonform ausführbar. Bestehende Prozesse sind auf die Einhaltung zu überprüfen.

42 So kann der strategische Einsatz von Social Media nicht nur eine höhere Werbewirksamkeit entfalten, sondern mitunter auch die Plattformen bereitstellen, die den notwendigen Kompetenzerwerb ermöglichen (vgl. Croll 2021, S. 6 f.).

43 Denn die Leitung ist für die Einhaltung der datenschutzrechtlichen Regeln (auch persönlich) verantwortlich. Die oder der Datenschutzbeauftragte – sofern es diese Position in der Organisation gibt – unterstützt die Leitung nur.

on der Anwender*innen muss aufrechterhalten werden, sodass sie sich dauerhaft sicherheitsbewusst verhalten.

4. Jede Organisation sollte gezielt prüfen, ob unter den Mitgliedern oder anderen zur Verfügung stehenden Kräften solche Personen zu finden sind, die mit dem notwendigen Mindset ausgestattet sind und die *Veränderungen antreiben* können.

Wesentlich ist also häufig nicht (allein) die technische Dimension des Themas, sondern die kulturelle, die erst vollendet ist, wenn der Datenschutz, der alle angeht, auch von allen wichtig genommen wird. Auch Datenschutzmuffel im zivilgesellschaftlichen Bereich sollten sich daher sogleich die folgenden Fragen stellen:

- Welche Anforderungen aus der DSGVO wurden bislang nicht umgesetzt? Was wurde vernachlässigt?
- Welche Hinweise hat die Organisation bislang nicht umgesetzt und welche Folgen kann das Ignorieren nach sich ziehen?
- Bei welchen Verarbeitungen besteht ein erhöhtes Risiko für einen Datenschutzverstoß?
- Wo wird sorglos mit personenbezogenen Daten umgegangen?
- Welches Image hat die Organisation in der Öffentlichkeit und was setzt sie mit einem zu gering ausgeprägten Datenschutz aufs Spiel?

7 Handlungsempfehlungen für Staat und Verbände

7.1 Politik

Datenschutz darf nicht als Hemmschuh und Fortschrittsbremse oder als Schikane begriffen werden. Dabei ist auch zu beachten, dass es nicht zu überflüssigen, weil sinnfreien Verpflichtungen kommt bzw. dass solche Verpflichtungen revidiert werden. Die DSGVO auf europäischer Ebene und das BDSG auf nationaler Ebene Deutschlands bedürfen einer ständigen Überprüfung[44] und gegebenenfalls auch Anpassung; die *Gesetze sind fortdauernd zu perfektionieren*. Fest steht aber, dass die DSGVO (und das BDSG) auch im Rahmen des bürgerschaftlichen Engagements Geltung beanspruchen. Eine Freistellung von einzelnen oder allen datenschutzrechtlichen Vorschriften sieht die DSGVO nicht vor.[45] Insoweit besteht für die Politik auf Bundes-, Landes- und kommunaler Ebene also nur ein *begrenzter Spielraum*. Eine Abschwächung der gesetzlichen Vorgaben muss sich im Rahmen der von der DSGVO eingeräumten Öffnungsklauseln bewegen. Ohne eine solche Öffnungsklausel stellte eine Abweichung unter den Standard der DSGVO grundsätzlich den Verstoß gegen höherrangiges Recht dar. Das von der DSGVO vorgegebene Datenschutzniveau kann vom deutschen Gesetzgeber nicht unterschritten werden.[46]

Inhaltlich wird beispielsweise diskutiert, von der Pflicht, *Verarbeitungsverzeichnisse* zu führen, gänzlich abzusehen. Ungeachtet der grundsätzlichen Frage der rechtlichen Möglichkeit hierzu ist aber

44 Die erste Überprüfung nach Art. 97 DSGVO fand turnusgemäß statt (siehe den im Grunde mit den Regelungen recht zufriedenen Bericht der Kommission unter https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf [eingesehen am 26.3.2021]). Teilweise wurden aus dem Parlament bereits Forderungen nach Änderungen laut (so etwa durch den EVP-Abgeordneten Voss [https://www.axel-voss-europa.de/europaeischer-datenschutz/ – eingesehen am 26.3.2021]), was aber aufgrund der kurzen bisherigen Umsetzungszeit keine Aussicht auf Erfolg haben dürfte.

45 Siehe beispielsweise die Antwort auf die entsprechende parlamentarische Anfrage. Online: https://www.europarl.europa.eu/doceo/document/P-8-2018-003121-ASW_DE.html (eingesehen am 1.3.2021).

46 Eine Veränderung des Rechts auf europäischer Ebene ist naturgemäß zumeist mit ungleich größeren Schwierigkeiten verbunden als auf nationaler Ebene.

Folgendes festzuhalten: Sich einen Überblick zu verschaffen, ist zwar eine Mühe. Diese ist aber nicht nur häufig mit recht überschaubarem Aufwand verbunden, sondern meist auch mit lohnenswertem Ertrag. Nicht selten wird erst hierdurch erkannt, welche überflüssigen Daten verarbeitet werden und welche überflüssigen Wege Daten nehmen, sodass Verarbeitungsprozesse durchaus effizienter gestaltet werden können, und zwar auch im Sinne des Engagements selbst. Die Verzeichnisse sind zudem die Grundlage für die entscheidende Sensibilisierung und Anfang aller Auseinandersetzung mit dem Thema Datenschutz. Wollte man diesen Schritt entfallen lassen, wäre nicht nur dem Datenschutz, sondern letztlich auch dem Engagement ein Bärendienst erwiesen, da der fehlende Schutz früher oder später auf das Engagement zurückfiele (vgl. hierzu Kapitel 5).

Auch wird diskutiert, die Pflicht zur Bestellung der*des Datenschutzbeauftragten im zivilgesellschaftlichen Bereich entfallen zu lassen. Dagegen spricht schon, dass der Schutz im Rahmen des zivilgesellschaftlichen Engagements aufgrund der vielen „externen“ Schnittstellen wohl grundsätzlich schwächer ausfällt, die Tätigkeit also gefahrgeneigter ist und ein*e Datenschutzbeauftragte*r bei Überschreiten einer geeigneten Schwellenzahl als Korrektiv sehr hilfreich sein kann. Andererseits könnte zwar überlegt werden, die *Schwellenzahl* für den Bereich des zivilgesellschaftlichen Engagements anzuheben oder ob die Erfüllung gewisser Grundbedingungen – zum Beispiel dem Vorliegen einer ausreichenden Dokumentation und eines etablierten Datenschutzkonzeptes – die Bestellung entfallen lassen kann. Allerdings besteht insoweit im Bereich des bürgerschaftlichen Engagements auch noch eine weitere Möglichkeit der Mitigation: Die Aufsichtsbehörden können bei der Frage, wann eine Person „ständig“ mit der Verarbeitung von Daten beschäftigt ist, durchaus *wohlwollende Maßstäbe* anlegen.

Auch ist theoretisch denkbar, dass der deutsche Gesetzgeber im Bereich der *Informationspflichten* und der *Ausübung der Betroffenenrechte* für den zivilgesellschaftlichen Bereich gewisse Erleichterungen schafft.[47] Eine wesentliche Entleerung des Datenschutzrechts im Bereich der Zivilgesellschaft darf damit aber aus den oben genannten Gründen nicht verbunden werden.

Mitunter wird ein gesetzgeberisches Entgegenkommen dergestalt gefordert, *Haftungsreduktionen bzw. -ausnahmen* für unbeabsichtigte Verstöße gegen Datenschutzbestimmungen speziell für den zivilgesellschaftlichen Bereich festzulegen. Es ist allerdings äußerst zweifelhaft, inwieweit hier überhaupt substanzieller Spielraum des nationalen Gesetzgebers besteht. Dieser ist immerhin durch Art. 83 DSGVO beschränkt. Die Verordnung fordert, dass Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen.

Das alles heißt aber nicht, dass die Politik überhaupt nicht dazu aufgerufen wäre, etwas zu tun. Einen wesentlichen Punkt kann der Gesetzgeber aber unproblematisch und schnell umsetzen: Er kann die alte Rechtslage vor Inkrafttreten des aktuellen BDSG wiederherstellen und die Aufsichtsbehörden zur *Beratung* auch gegenüber Verantwortlichen *verpflichten*, mindestens jedoch gegenüber Verantwortlichen im Bereich des zivilgesellschaftlichen Engagements.

47 Und zwar über die Anwendung der Öffnungsklausel nach Art. 23 Abs. 1 lit. e DSGVO, wenn die Leistungsfähigkeit zivilgesellschaftlicher Akteure als „wichtiges Ziel“ im Sinne dieser Norm verstanden und als gefährdet angesehen würde.

Die Politik hat auch dafür Sorge zu tragen, dass die Vorteile eines effektiven Datenschutzes für die Bevölkerung sichtbar und bekannt werden. Dabei ist zentral, durch grundlegende *Aufklärungsarbeit sozial robuste Orientierungen* für den verantwortungsvollen Umgang mit Daten zu vermitteln, sodass sowohl der Datenschutz als auch der durch ihn entstehende zusätzliche Aufwand allgemein akzeptiert und wertgeschätzt werden.[48]

Da die Politik aufgefordert ist, die Digitalisierung inklusiv und sicher zu gestalten, hat sie auch sicherzustellen, dass der Schritt in die Digitalisierung umfassend gelingt und dass nicht wichtige Teile der Gesellschaft zurückbleiben. Aufgrund der Bedeutung des zivilgesellschaftlichen Engagements kommt der Politik in Bund, Ländern und Kommunen eine Garantenstellung zu, auch diesem bedeutenden Feld gesellschaftlichen Lebens den Sprung ins digitale Zeitalter zu ermöglichen. Insoweit kann die Politik die für die Compliance bürgerschaftlicher Organisationen notwendigen *Fort- und Weiterbildungsmaßnahmen* in den oben identifizierten Bereichen entscheidend fördern. Aufgrund des Umfangs der durch Datenschutz und Datensicherheit begründeten Anforderungen wird die Zivilgesellschaft den Sprung nicht ohne Förderung schaffen können. Es sind Programme aufzusetzen, mit denen die *Readiness der Zivilgesellschaft* gesteigert werden kann. Neben der *Organisationsentwicklung und dem Leadership* ist besonders auch die *Befähigung* der Engagierten zu fördern, mit den neuen Techniken und ihren Bedingungen datenschutzkonform umzugehen. Es muss sichergestellt werden, dass sich die Digitalisierung weiter als Integrationsfaktor beweisen kann (wie sie es beispielsweise in Zeiten von Corona bereits getan hat) und keine Spaltung in den Organisationen in Techies und Abgehängte bewirkt.

Es bedarf insoweit der *finanziellen und sachlichen*[49] *Unterstützung* vonseiten der Kommunen, der Länder und des Bundes.[50] Aufgrund der äußerst hohen Bedeutung des zivilgesellschaftlichen Engagements ist das auch eine durchaus lohnende Investition. Insbesondere die *Kommunen*, die ganz erheblich etwa von Vereinsarbeit und Bürgerengagement profitieren,[51] sind insoweit gefragt. Bürgerschaftliche Initiativen sind für sie eine besonders wichtige Stütze. Und digitales Engagement ist dabei schon heute nicht mehr wegzudenken – von digital organisierter Nachbarschaftshilfe für ältere Menschen über digitale Formen der Bürgerbeteiligung an demokratischen Prozessen bis hin zu digital durchgeführten Vereinsangeboten für Kinder. Die Zukunft des bürgerschaftlichen Engagements lässt sich also ohne Digitalisierung nicht denken. Es gilt, seine Teilhabe *an*, *durch* und *in* digitalen Medien zu sichern und auszubauen. Digitale Technologien können zum einen Formen des freiwilligen Engagements wie die klassische Vereinsarbeit erleichtern. Zum anderen ermöglichen sie, Zeiten und Einsatzorte des Engagements flexibler zu bestimmen sowie neue Formen und Inhalte bürgerschaftlichen Engagements zu schaffen, etwa wenn Digitalisierung selbst zum Gegenstand wird.[52]

48 Dies empfiehlt sich insbesondere auch als Aufgabe für die neue Bundeszentrale für Digitale Aufklärung.

49 Beispielsweise unterstützt die Niedersächsische Landesregierung mit ihrem Förderprogramm „Digitalbonus“ einschlägige Investitionen derzeit mit einem nicht rückzahlbaren Zuschuss. Vergleichbare Programme gibt es auch in anderen Bundesländern.

50 Bei der Einforderung von Unterstützung seitens der Politik ist immer mit zu bedenken, auf welcher Ebene (Land, Bund, Europa) die Forderung anzubringen ist.

51 So ist etwa der Mitgliederschwund in lokalen Vereinen ein erhebliches Problem der Kommunen, das mitunter deren Verödung bewirkt.

52 Die Vielfalt des digitalen Engagements *selbst* hat mehr Sichtbarkeit und Anerkennung verdient und sollte politisch gewürdigt sowie ideell, finanziell und strukturell gefördert werden.

Wichtig ist, dass das *Enabling des bürgerschaftlichen Engagements als Dauerprozess* angesehen wird. Zum einen konnte oben (Kapitel 3) gezeigt werden, dass ein einmaliges Training regelmäßig nicht ausreichend ist, die Befähigung der Einzelnen nachhaltig zu steigern. Zum anderen ist Digitalisierung ohnehin nicht als einmaliger Prozess zu einem bestimmten Zeitpunkt abgeschlossen, sondern bedingt eine *Daueraufgabe*.[53] Dies nicht nur im Hinblick auf die Anpassung der technischen Antworten auf die sich fortentwickelnden Probleme, sondern auch im Sinne der persönlichen Bereitschaft, den Datenschutz entsprechend seiner notwendigen Integration in alle Organisationsabläufe als einen routinemäßigen, kontinuierlichen und nachhaltigen individuellen Lernprozess zu begreifen.

Qualifizierungsangebote dürfen sich zudem nicht darauf beschränken, nur abstraktes Wissen zu vermitteln. Es hat sich nämlich gezeigt, dass Qualifizierungsangebote inhaltlich zwar eine hilfreiche, nicht aber unbedingt hinreichende Bedingung für eine gelingende Digitalisierung darstellen: Der Erwerb entsprechender Kompetenzen findet (insbesondere in der Altersgruppe ab fünfzig und bei Frauen) im Wesentlichen durch *Learning by Doing* statt (vgl. Digital-Index 2019/2020, S. 26 f.; Croll 2021, S. 4). Daher sind Qualifizierungsangebote inhaltlich so zu gestalten, dass sie für die Nutzer*innen durch die Anpassung an die tatsächlichen Bedarfe *unmittelbar anwendbare und umsetzbare Ergebnisse* liefern.

53 Von den Engagierten muss dies nicht überwiegend als Belastung angesehen werden. Nach dem D21-Digital-Index 19/20 gaben 68 % der Befragten an, lebenslanges Lernen eher als Privileg denn als Belastung anzusehen. Insoweit lässt sich der digitale Einsatz im Ehrenamt und der damit verbundene Wissenszuwachs bei vielen Ehrenamtlichen sogar noch als Vorteil darstellen.

Die Umsetzung der Fördermaßnahmen kann insbesondere durch geeignete engagementunterstützende Organisationen und Verbände erfolgen. Diese sind als *Wegbereiter* einer digitalisierungsfesten Zivilgesellschaft nachhaltig zu fördern. Dazu müssen sie zu Fördermöglichkeiten (öffentliche wie private) auch *gezielt beraten* können.

Schließlich ist zu fordern, dass der Gesetzgeber bei allen gesetzlichen Veränderungen im Bereich des Datenschutzes eine konsequente *Engagementverträglichkeitsprüfung* vornimmt.

7.2 Aufsichtsbehörden

Auch an die Adresse der Datenschutzbehörden richten sich einige Forderungen. Neben der oben (Kapitel 7.1) bereits angesprochenen wohlwollenden Bewertung des hinsichtlich der Bestellung einer*eines Datenschutzbeauftragten relevanten Tatbestandsmerkmals „ständig“ ist die *Beratung* gegenüber Verantwortlichen im Bereich des zivilgesellschaftlichen Engagements auch ohne ausdrücklichen Auftrag durch das BDSG wieder (wie unter Geltung des BDSG alte Fassung) aufzunehmen. Das sollten die Datenschutzaufsichtsbehörden schon im eigenen Interesse tun. Dadurch steigern sie nicht nur das *Datenschutzniveau* innerhalb ihres Zuständigkeitsbereichs, sondern lösen damit auch einen *Multiplikationseffekt* aus, da Beratungserfolge so auch in die breitere Gesellschaft getragen werden.

Zudem erfahren die Behörden nicht nur Wesentliches über den aktuellen Stand der Umsetzung, sondern verbessern auch ihre *Reputation* in der Öffentlichkeit und insbesondere der Zivilgesellschaft und bei jenen staatlichen Stellen, welche über ihre sachangemessene Ausstattung (vgl. Art. 52 Abs. 4 DSGVO) mitentscheiden. Die

Aufsichtsbehörden sollten sich also die Zivilgesellschaft zum Verbündeten machen und dafür ein *Fortbildungs- und Beratungszentrum* zugunsten zivilgesellschaftlicher Akteure einrichten. So hat etwa das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bereits eine Hotline eingerichtet, die schnelle und unkomplizierte Hilfe verspricht. Es könnte sich allerdings empfehlen, dass sich die Länder auf eine verstärkte Kooperation im Sinne effizienter *Arbeitsteilung* einigen. So könnte ein Bundesland in Absprache mit den anderen Ländern etwa besondere Kapazitäten für den Bereich des bürgerschaftlichen Engagements entwickeln und bereitstellen. Alternativ bzw. zusätzlich könnte eine entsprechende Beratungs- und Programmstelle bei dem Bundesbeauftragten für Datenschutz eingerichtet werden.

Mit Blick auf das anspruchsvolle Datenschutzrecht und die häufig nur schwer einholbare Kompetenz andererseits erwächst zudem für die Aufsichtsbehörden die Pflicht, gerade und insbesondere im Bereich des zivilgesellschaftlichen Engagements den *Grundsatz „Beratung vor Sanktion" anzuwenden*.

7.3 Verbände

Im Bereich des Digitalen kommt den Verbänden eine Vielzahl an Aufgaben zu. Neben ihrer *Vorbildfunktion* nehmen sie die *Rolle des Transformators und Mittlers* ein. Konkret sollten Verbände – wenn möglich – eine *Ansprechperson* (eine Datenschutzreferentin bzw. einen Datenschutzreferenten) benennen, die für ihre Mitglieder *für Auskunft und Coaching* bereitsteht. Bei ihren Mitgliedern sollten sie digitalisierungsspezifische Organisationsentwicklung und Leadership fördern, wofür sie gezielt finanzielle Unterstützung von der Politik einfordern sollten. Der Auf- und Ausbau von *Netzwerken*, um den Bedarfen ihrer Mitglieder auf politischer Ebene *verstärktes Gehör* zu verschaffen, ist hierbei zu forcieren. Auch sollten sie dafür sorgen, dass die Erfahrungen der zivilgesellschaftlichen Akteure *wissenschaftliche Begleitung und Auswertung* finden, sodass notwendige Veränderungs- und Anpassungsprozesse fundiert begründet betrieben und dafür nötige spezifische Unterstützungen gegebenenfalls entsprechend eingefordert werden können.

Verbände, die Kategorien von Verantwortlichen (also eine in gewisser Hinsicht homogene Gruppe wie etwa bürgerschaftlich engagierte Vereine) vertreten, haben zudem gemäß Art. 40 Abs. 2 DSGVO die Möglichkeit, die Anwendung der datenschutzrechtlichen Vorschriften für ihren Bereich zu präzisieren, indem sie *Verhaltensmaßregeln* (*Codes of Conduct*) erarbeiten und diese für die Branche von der zuständigen Aufsichtsbehörde genehmigen lassen.[54] Als besonders praxisrelevant können sich die Konkretisierung der berechtigten Interessen, die Präzisierung einer fairen und transparenten Verarbeitung (zum Beispiel im Hinblick auf die Erfüllung von Informationspflichten) und die Konkretisierung technischer und organisatorischer Maßnahmen durch Verhaltensregeln erweisen.

Darüber hinaus können Verbände *Erfahrungsaustausche organisieren*, gegebe-

54 Ein Unterschreiten des Niveaus der DSGVO bzw. des BDSG ist dadurch nicht möglich. Durch Verhaltensmaßregeln kann indes ein höheres Maß an Rechtssicherheit erreicht werden. Zwar bedeutet die Einhaltung der Regeln nicht automatisch die Einhaltung des Gesetzes. Die Verantwortlichkeit bleibt vielmehr vollen Umfangs bestehen. Aber die Einhaltung der genehmigten Regelungen kann als Indiz für Datenschutzkonformität herangezogen werden, also für die Annahme der Erfüllung der Pflichten der Verantwortlichen. Jedenfalls würde die Aufsichtsbehörde der Einhaltung der Regeln bei der Bewertung eines Datenschutzvorfalls besonderes Gewicht verleihen, was sich im Rahmen der Ahndung als günstig herausstellen dürfte.

nenfalls auch eine *Aufgabenteilung* bei der Erarbeitung von Lösungen. Neben den Verbänden können auch größere Vereine Teilaufgaben übernehmen, indem sie erarbeitete Informationen für andere aufbereiten. Lokale *Kompetenzzentren* für den Wissensverkehr könnten hier hilfreich sein. Die Verbände könnten zudem *Best Practice hervorheben* und fördern sowie in *Transferwerkstätten* die Weitergabe des generierten Wissens sicherstellen.

Auch können die Verbände *Kooperationen in den Bereich der Wirtschaft* herstellen. Unternehmen könnten im Rahmen ihres PR-relevanten Wirkens etwa *Datenschutzpatenschaften* für Organisationen des bürgerschaftlichen Engagements bereitstellen.

Und schließlich könnten Verbände durch das geförderte Aufsetzen, die Verbreitung und Sicherung von gemeinsamen bedarfsgerechten *Kommunikations- und Verwaltungstools* – und sonstiger Datenschutz und Datensicherheit zuträglicher *CivicTech* – die Handlungsfähigkeit ihrer Mitglieder bei Nutzung von Synergien erhöhen und erleichtern.

QUELLEN

- Croll, Jutta 2021: Thesenpapier zum Themenfeld Digitale Kompetenz im bürgerschaftlichen Engagement. In: BBE-Newsletter, 04/2021. Online: https://www.b-b-e.de/fileadmin/Redaktion/05_Newsletter/01_BBE_Newsletter/2021/02/Newsletter-4-croll.pdf (eingesehen am 7.3.2021).
- Cyber Ark 2020: CyberArk State of Remote Work Study: Poor Security Habits Raise Questions About the Future of Remote Work. Online: https://www.cyberark.com/press/cyberark-state-of-remote-work-study-poor-security-habits-raise-questions-about-the-future-of-remote-work/ (eingesehen am 30.7.2021).
- Digital-Index 2019/2020: Wie digital ist Deutschland? Jährliches Lagebild zur Digitalen Gesellschaft, hg. v. Initiative D21. Online: https://initiatived21.de/app/uploads/2020/02/d21_index2019_2020.pdf (eingesehen am 20.7.2021).
- EDRi (European Digital Rights) o. J.: Targeted Online. An industry broken by design and by default. Online: https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf (eingesehen am 12.3.2021).
- Grünecker, Johannes 2021: Digitale Kompetenzen im Engagement der AWO. Ein Erfahrungs- und »Wirkungsbericht« des Dialogforums »Digitale Kompetenz«. In: BBE-Newsletter, 04/2021. Online: https://www.b-b-e.de/fileadmin/Redaktion/05_Newsletter/01_BBE_Newsletter/2021/02/Newsletter_4-Gruenecker.pdf (eingesehen am 7.3.2021).
- HPI (Hasso-Plattner-Institut) 2020: Die beliebtesten deutschen Passwörter 2020 - Platz 6 diesmal: ichliebedich, Pressemitteilung vom 16. Dezember 2020. Online: https://hpi.de/news/jahrgaenge/2020/die-beliebtesten-deutschen-passwoerter-2020-platz-6-diesmal-ichliebedich.html (eingesehen am 28.2.2021).
- Rohde & Schwarz 2021: Mitschrift zu einem Online-Vortrag.
- Stiftung Aktive Bürgerschaft 2020: Stellungnahme der Stiftung Aktive Bürgerschaft. Öffentliche Anhörung zum Thema „Datenschutzgrundverordnung (DSGVO) bzw. Bürokratieabbau im Ehrenamt“ am 23. November 2020 im Ausschuss für Familie, Senioren, Frauen und Jugend des Deutschen Bundestages. Online: https://www.bundestag.de/resource/blob/807244/9c40c6bf38bda815c22bf6501a874eca/19-13-103f-data.pdf (eingesehen am 30.7.2021).

AUTOR*INNEN

Dr. Daniel Burchardt wurde im Verfassungsrecht mit einem Schwerpunkt auf Freiheitsrechten promoviert. Seit einigen Jahren ist er auch im Bereich des Datenschutzes tätig und hat wiederholt bundesweit wie auch international tätige Organisationen zu diesem Thema beraten.
✉ info.burchardt@mailbox.org

Dr. Serge Embacher leitet den Arbeitsbereich Fachprojekte in der Geschäftsstelle des Bundesnetzwerks Bürgerschaftliches Engagement (BBE) und koordiniert in dieser Funktion das »Forum Digitalisierung und Engagement«.
✉ serge.embacher@b-b-e.de

Prof. Ulrich Kelber ist seit Januar 2019 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Er ist Diplom-Informatiker und war von 2000 bis 2018 Mitglied des Deutschen Bundestages. Seit Juli 2019 ist er zudem als Honorarprofessor für Datenethik an der Hochschule Bonn-Rhein-Sieg tätig.
✉ poststelle@bfdi.bund.de

Nils Leopold, LL. M. (Rechtsinformatik), ist seit 2020 beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) beschäftigt. Er ist Volljurist und gelernter Rechtsanwalt. Er war zuvor beim Deutschen Bundestag, bei der Datenschutzaufsicht des Landes Schleswig-Holstein (ULD) sowie als Bundesgeschäftsführer einer bürgerrechtlichen NGO in Berlin tätig.
✉ poststelle@bfdi.bund.de

Dana Milovanovic ist Referentin im Projekt »Forum Digitalisierung und Engagement« in der Geschäftsstelle des Bundesnetzwerks Bürgerschaftliches Engagement (BBE). Sie verfügt über einen Bachelor- und Masterabschluss der Europa-Universität Viadrina in den Fächern Kulturwissenschaften und Soziokulturelle Studien. In der Digitalisierung sieht sie großes Potenzial für das bürgerschaftliche Engagement und dessen nachhaltige Weiterentwicklung. Das Forum stellt für sie ein essenzielles Austauschformat der Zivilgesellschaft zu den drängenden Fragen in Bezug auf den Digitalen Wandel dar.
✉ dana.milovanovic@b-b-e.de

Jochim Selzer ist Diplom-Mathematiker. Seit 2001 arbeitet er als Applikationsadministrator bei der Deutschen Post IT Services, seit 2008 fungiert er als ehrenamtlicher Datenschutzbeauftragter der Evangelischen Kirche im Kirchenkreis Bonn. Im selben Jahr ist er auch Mitglied im Arbeitskreis Vorratsdatenspeicherung geworden. Seit März 201 engagiert sich Selzer als Mitorganisator von bis dato circa dreißig Kryptoparties mit Schwerpunkt im Raum Köln-Bonn, zuletzt auf dem Global Media Forum in Bonn und dem Jahrestreffen des Netzwerks Recherche in Hamburg. Er ist Mitglied im Chaos Computer Club.
✉ js@crypto.koeln

Teresa Staiger ist Referentin im Projekt »Forum Digitalisierung und Engagement« in der Geschäftsstelle des Bundesnetz-

werks Bürgerschaftliches Engagement (BBE). Zuvor war sie am Max-Planck-Institut für Intelligente Systeme tätig. Sie hat ihr Studium an der Johannes-Gutenberg-Universität Mainz und Cardiff University (B. A. Politikwissenschaft und Geschichte) und an der Philipps-Universität Marburg (M. A. Politikwissenschaft) absolviert. Sie interessiert sich besonders für eine gemeinwohlorientierte Digitalisierung, die durch eine digital souveräne und engagierte Zivilgesellschaft begleitet wird.
✉ teresa.staiger@b-b-e.de

BBE-NEWSLETTER ONLINE

BBE-NEWSLETTER

Der BBE-Newsletter informiert 14-täglich über die Engagementpolitik und -debatte in Deutschland, interessante Publikationen und Veranstaltungen sowie Aktuelles aus dem BBE. In monatlichen Themenschwerpunkten vertiefen Autor*innen aus Politik, Zivilgesellschaft, Wirtschaft und Wissenschaft zivilgesellschaftliche Themen.

https://www.b-b-e.de/newsletter

BBE EUROPA-NACHRICHTEN

Die BBE Europa-Nachrichten zu Engagement und Partizipation in Europa bieten monatlich Informationen und Hintergrundberichte zu europäischen Fragen der Engagementpolitik und -förderung, Gastbeiträge namhafter Europa-Expert*innen sowie Hinweise auf internationale Beteiligungsverfahren.

https://www.b-b-e.de/eunewsletter

INFOLETTER

Der Infoletter zur Woche des bürgerschaftlichen Engagements erscheint vierteljährlich, informiert über die Aktivitäten zu Vorbereitung und Durchführung der Aktionswoche, stellt Engagementprojekte vor und hält über die Nachrichten, Aktionen und Materialien rund um das bürgerschaftliche Engagement auf dem Laufenden.

https://www.engagement-macht-stark.de/downloads/infoletter/

NEWSLETTER-ABO

https://www.b-b-e.de/newsletter-abo