Datenschutz und Datensicherheit im bürgerschaftlichen Engagement

Dieses Papier ist im Frühjahr 2021 im Auftrag des BBE e.V. entstanden. Es dient als Beitrag zum Dialogforum Datenschutz und Datensicherheit des Projekts „Forum Digitalisierung und 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]

Inhalt

[1] So das 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.

Autor: Dr. Daniel Burchardt, Berlin – Stand: März 2021

1. Zusammenfassung

Die Bedeutung des Datenschutzes gewinnt in einer zunehmend datengesteuerten Welt immer mehr Bedeutung. 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 Bewahrung 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 Akteure des bürgerschaftlichen Engagements strategisch im Rahmen ihrer Kommunikation und Organisationsentwicklung nutzen sollten. Insoweit wird 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 erfolgversprechend 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 und 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 Anbieterin 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 nutzen, um an Daten zu kommen und diese Aufkäufern auf verschiedenen Wegen zur Verfügung zu stellen. An den

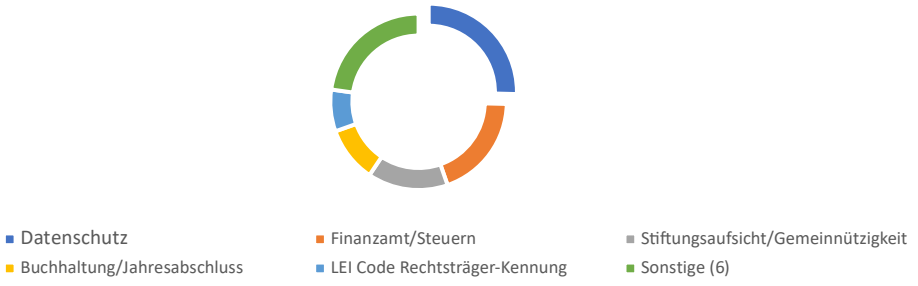
[2] Der Begriff des bürgerschaftlichen Engagements geht über das Ehrenamt hinaus. Er wird hier daher in einem weiteren, dem Begriff der Zivilgesellschaft vergleichbaren Sinne benutzt, der hoheitliches Handeln kontrastiert und das freiwillige, nicht allein auf finanzielle Vorteile gerichtete und das Gemeinwohl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

aufbereiteten Datensätzen sind nicht nur die Schwarzen oder Grauen Schafe interessiert. Auch seriöse Anbieterinnen, die Werbung gezielter anbringen wollen, oder, wie etwa Versicherungen und Banken, die durch eine gezieltere Auswahl ihrer Kund*innen und entsprechende Tarif- bzw. Preisgestaltung wirtschaftliche Risiken minimieren wollen, und auch potenzielle Arbeitgeberinnen, die ihre Personalentscheidungen optimieren wollen, haben vielfach den Nutzen solcher Datensätze erkannt und setzen sie unmittelbar selbst oder mittelbar über spezielle Dienstleisterinnen ein.[3] Natürlich ist die Gesetzgebung gefragt, 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 34% 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:[6]



Bürokratie-Hauptlast nach einer Umfrage unter Verantwortlichen im bürgerschaftlichen Bereich 2019. Quelle: Stiftung Aktive Bürgerschaft

[3] Eingehend zu den Bedrohungen der Grundfreiheiten, die mit der sogenannten *Data Mining Industry* und dem *Surveillance Capitalism* verbunden sind, siehe die EDRI-Publikation Targeted Online (https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf - zuletzt abgerufen am 12. März 2021).

[4] https://de.statista.com/themen/4757/datenschutz-im-internet/ (zuletzt abgerufen am 28. Februar 2021).

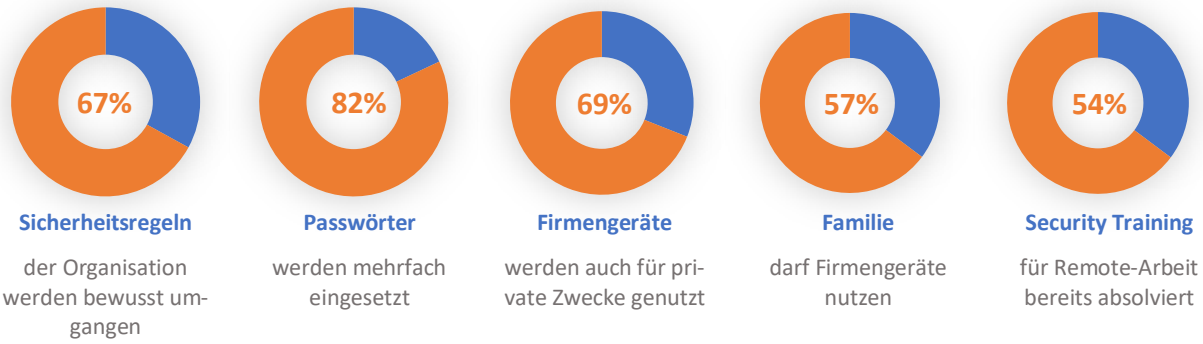
[5] Siehe dazu die Stellungnahmen der Sachverständigen, die in der 71. Sitzung des BT-Ausschusses für Familie, Senioren, Frauen und Jugend am 23. November 2020 gehört wurden (https://www.bundestag.de/ausschuesse/a13/Anhoerungen#url=L2F1c3NjaHVlc3NlL2ExMy9BbmhvZXJ1bmdlbi84MDYzOTAtODA2Mzkw&mod=mod683976 – zuletzt abgerufen am 12. März 2021).

[6] Nach einer Umfrage der Stiftung Aktive Bürgerschaft im Bereich Ehrenamt und Stiftungen in 2019 (https://www.bundestag.de/resource/blob/807244/9c40c6bf38bda815c22bf6501a874eca/19-13-103f-data.pdf – zuletzt abgerufen am 12. März 2021).

Zwar ist der Datenschutz kein von Grund auf neues Phänomen. Im Gegenteil: Bereits vor der Einführung der europäischen Datenschutzgrundverordnung (DS-GVO) 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 DS-GVO 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 DS-GVO ist der Datenschutz aber verstärkt ins öffentliche Bewusstsein vorgedrungen. Viele Ehrenamtliche sahen sich erstmals mit ihnen nicht selten unverständlich und sperrig erscheinenden Aspekten des Datenschutzes, wie etwa dem einer wirksamen Einwilligungserklärung, Datenschutzerklärungen für Websites oder gar Dokumentationspflichten konfrontiert.

Im Jahre 2020 waren laut einer Studie des Meinungsforschungsinstituts Allensbach rd. 17 Mio Menschen in Deutschland ehrenamtlich, dh. freiwillig und unentgeltlich für eine Initiative, einen Verein oder eine andere Organisationsform tätig.[7] Das entspricht rd. einem Fünftel der Bevölkerung. In den letzten Jahren hat es dabei einen recht signifikanten Anstieg gegeben.[8] 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 DS-GVO 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; so etwa im Zusammenhang zum Arbeiten im HomeOffice, das dem Setting nach bürgerschaftlichen Tätigkeiten mitunter nahekommt. Dort ist laut einer im Auftrag von Cyber Ark durchgeführten aktuellen Umfrage[9] das Datenschutzverständnis nur schwach ausgeprägt:



Datenschutz im HomeOffice. Quelle: Cyber Ark

Auffällig an den Ergebnissen der Studie ist, dass 54% der Befragten ein Security-Training bereits absolviert hatten.[10] 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.[11] Dies wiederum untergräbt a priori das Aufkommen einer Kultur des

[7] https://de.statista.com/statistik/daten/studie/173632/umfrage/verbreitung-ehrenamtlicher-arbeit/ (zuletzt abgerufen am 15. Februar 2020).

[8] Im Vorjahr lag die Zahl noch um rund eine Million tiefer (a.a.O.).

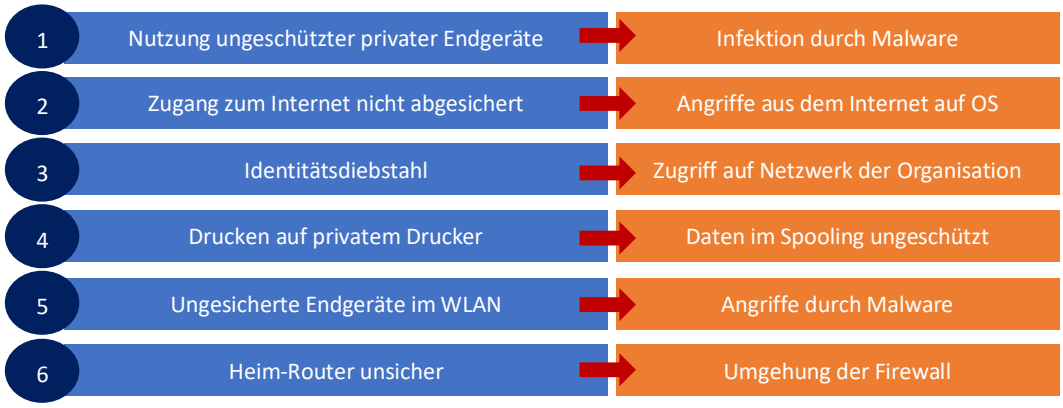
[9] https://www.cyberark.com/press/cyberark-state-of-remote-work-study-poor-security-habits-raise-questions-about-the-future-of-remote-work/ (zuletzt abgerufen am 28. Februar 2021).

[10] Da es eher unwahrscheinlich ist, dass an der Qualität solcher Trainings ganz generell zu zweifeln wäre, ist allem Anschein ein singuläres Training nicht ausreichend. Darauf wird an geeigneter Stelle (sub 7.a.) noch einmal zurückzukommen sein.

[11] 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.

Datenschutzes.[12] Denn das geringere Vorhandensein von Kompetenzen kann leicht in einen Teufelskreis führen. Es gründet nicht selten auf **mangelnden Erfahrungs- und Reflektionsmöglichkeiten** und bewirkt eine **geringere Selbstwirksamkeitserfahrung**, was wiederum in eine geringere Motivation mündet, sich mit dem Thema im Rahmen des persönlichen Engagements auseinanderzusetzen.[13] Mitunter ist beispielsweise sogar die grundlegende Unterscheidung zwischen Datenschutz und Datensicherheit nicht bekannt.[14]

Mangelt es aber am digitalen Sicherheitsbewusstsein, kann Schaden leicht durch Acht- und Sorglosigkeit entstehen. Dazu passt, dass nach aktuellen Erhebungen nur 50% der Personen in Deutschland Sicherheitsvorkehrungen treffen, um ihre Daten im Internet zu schützen.[15] Und laut dem Hasso-Plattner-institut war auch 2020 immer noch „123456" das meistgenutzte Passwort, nach wie vor gefolgt von „123456789".[16] Als die **Top-6-Risikofaktoren** werden im privaten Bereich derzeit expertenseitig die folgenden Punkte gehandelt:



Top-6-Risikofaktoren im Privatbereich. Quelle: Rohde & Schwarz

Zivilgesellschaftsspezifische Datenverarbeitungsvorgänge sind vielfältig, sie umfassen typischer Weise insbesondere die Verarbeitung personenbezogener Daten für Veranstaltungseinladungen, die Mitgliederverwaltung, Spendenwerbung und -Verwaltung, den Öffentlichkeitsauftritt im Internet (Website) und die Mitarbeitenden- und Beitragsverwaltung sowie ggf. die Lohnabrechnung mitsamt der Handhabung sozialversicherungsrechtlicher Daten.[17] 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.

---

[12] So lassen sich etwa die Ergebnisse einer Umfrage bei der AWO verstehen, https://www.b-b-e.de/fileadmin/Redaktion/05_Newsletter/01_BBE_Newsletter/2021/02/Newsletter_4-Gruenecker.pdf (zuletzt abegrufen am 07. März 2021), S. 4f.

[13] Vgl. Coll, a.a.O., S. 4.

[14] 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 (zB. 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.

[15] https://de.statista.com/themen/4757/datenschutz-im-internet/ (zuletzt abgerufen am 28. Februar 2020). Immerhin halten nur 7% das Internet für sicher, wenn es um ihre persönlichen Daten geht, a.a.O. Das sind aber immer noch 7% zu viel.

[16] https://hpi.de/news/jahrgaenge/2020/die-beliebtesten-deutschen-passwoerter-2020-platz-6-diesmal-ichliebedich.html (zuletzt abgerufen am 28. Februar 2021).

[17] „Verarbeitung" meint alle mit Daten denkbaren Vorgänge, wie das Speichern (z.B. im Posteingangsordner), das Löschen, Verändern, Übertragen etc. Alle üblichen Datenverarbeitungen im Bereich des bürgerschaftlichen Engagements fallen darunter.

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.

4. Die wesentlichen datenschutzrechtlichen Anforderungen[18]

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 Datenschutzgrundverordnung [DS-GVO] und das Bundesdatenschutzgesetz [BDSG] ergänzt durch Landesdatenschutzgesetze und ggf. bereichsspezifische Regelungen) zu folgen.[19] 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.[20] Entgegen einem weit verbreiteten Irrglauben sind die Regeln auch dann einzuhalten, wenn keine Datenschutzbeauftragte bestellt werden muss.[21]

Die Vorschriften zum Datenschutz legen fest, dass **jede Verarbeitung personenbezogener Daten**[22] **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**, d.h. allgemein vorgesehene Verarbeitung personenbezogener Daten das Kriterium der relevanten Speicherung erfüllen wird.

Ausnahmen von dem **Verarbeitungsverbot** bestehen nur insoweit, als

---

[18] 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.

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

[20] 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 20 Personen, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

[21] Die Pflicht, eine Datenschutzbeauftragte zu bestellen, dürfte – zumal nach der Anhebung der Schwellenanzahl in § 38 Abs. 1 S. 1 BDSG auf 20 Personen – nur in selteneren Fällen greifen.

[22] 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 hervorgehen, 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 DS-GVO). 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 DS-GVO bzw. § 22 Abs. 1 BDSG (sowie in besonderen Ausnahmefällen ggf. 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.

- die berechtigte Person, auf die sich die personenbezogenen Daten bezieht, ihre **Einwilligung**[23] **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 worden sein und darf nicht unlauter beeinflusst worden sein (z.B. durch Täuschung oder bei Ausnutzung eines Machtgefälles). Die Einwilligung sollte **dokumentiert** werden.

Wichtig für bürgerschaftlich Engagierte ist zudem häufig, dass sie **dem Datengeheimnis, 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 der Verschwiegenheitspflicht sogar strafrechtlich relevant sein.[24] 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** (z.B. bei Beantragung einer Mitgliedschaft) oder die **Vertragserfüllung** (z.B. 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 (z.B. zur Einwerbung von Folgespenden). Dann ist vor der Verarbeitung eine **Interessenabwägung**[25] 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 iVm. Art. 35 Abs. 3 lit. B DS-GVO eine **Datenschutzfolgenabschätzung** notwendig wird, die dabei obligatorisch zur Bestellung einer 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;

---

[23] 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.

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

[25] zB. in Anlehnung an den *Legitimate Interest Assessment Test* der ICO.

- **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, d.h. ein **Datenschutz-Management-System** eingerichtet wird. Das heißt die Organisation der Abläufe dergestalt, dass die Einhaltung des Datenschutzes sichergestellt und dokumentiert 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**[26] 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 usw.: Planen/Ausführen/Überprüfen/Ändern.[27]

Verantwortlich für Berücksichtigung und Nachhalten der oben genannten Prinzipien und der aus ihnen folgenden datenschutzrechtlichen Verpflichtungen ist bei juristischen Personen im Ergebnis[28] 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[29] und beschreiben jeden Verarbeitungsvorgang in einem **Verarbeitungsverzeichnis**.

Schritt 3: Es ist zu prüfen, ob eine **Datenschutzbeauftragte** 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 Datenschutzfolgen-Abschätzung dokumentiert sein.[30]

[26] Auch „PDCA-Zyklus" (nach Plan/Do/Check/Act) oder „Demingkreis" genannt.

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

[28] Genaugenommen ist verantwortlich nach Art. 4 Ziff. 7 DS-GVO 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*.

[29] Da datenschutzrechtliche Vorschriften nur greifen, wenn personenbezogene Daten verarbeitet werden, bedeutet dies im Umkehrschluss auch, 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 personenenbezogene Daten beinhalten und solchen, die dies nicht tun, durchaus zu Vereinfachungen kommen.

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

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.

Schritt 7: Es sind proaktiv **Informationsmöglichkeiten** für die Betroffenen, die über Verarbeitungen und ihre **Rechte**[31] informiert werden müssen, ebenso zu schaffen wie die Möglichkeit der Geltendmachung von Betroffenenrechten (hierzu ist ein Prozess aufzusetzen).[32]

Schritt 8: Ggf. 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.[33]

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

- **Schulung**[34] aller personenbezogene Daten verarbeitenden Engagierten und Mitarbeitenden
- Einführung einer planhaften **Datenschutz-Richtlinie**,[35] 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[36] eingesetzten Gerät (Ausschluss anderer Mitnutzer), Firewall und aktuellem Virenschutz (hierbei geht es im Wesentlichen um das Niveau, das informierte Laien ohnehin schon zum Standard machen), Abschließen des Aktenschranks. Empfehlenswert *kann*[37] die geschützte Dokumentenverwaltung in der Cloud sein (bei DS-GVO-konformer Anbieterin)
- Einholen von **Verschwiegenheitsverpflichtungserklärungen/Verpflichtung auf das Datengeheimnis**

Schritt 10: Ein **Prozess für den Fall einer Datenschutzverletzung** (Meldepflicht ggü. 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.

Schritt 11: Die Website der Organisation ist mit einer **Datenschutzerklärung** auszustatten. Die Nutzung von **Fotos** ist zu überprüfen.[38] Sofern Einbindungen in Social Media erfolgen, ist besonders mit besonderer

---

[31] 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.

[32] 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.

[33] Das Europäische Datenschutzniveau darf nicht unterschritten werden. Dies ist vertraglich sicherzustellen, sofern kein Angemessenheitsbeschluss vorliegt.

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

[35] 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.

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

[37] 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.

[38] Ein Foto kann unter die Kategorie biometrischer Daten fallen, so dass 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, so dass 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.

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 ggf. 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, 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 Sicherheits-Anspruch, 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.[39] Bei Fragen kann die zuständige Aufsichtsbehörde kontaktiert werden, die meist helfend zur Seite steht.[40]

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, wie gleich noch näher dargestellt wird, sowohl finanzieller als auch personaler Natur drohen kann. 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.[41] Denn die teilweise bereits vorhandene Wertschätzung des Themas Datenschutz,[42] die im Hinblick auf die Datengetriebenheit entscheidender Wirtschaftszweige sowie die noch zu erwartenden Datenskandale in ansehbarer Zeit noch

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

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

[41] Dies wäre in grundsätzlicher Hinsicht nur auf europäischer Ebene durch Anpassung der DS-GVO möglich.

[42] Bereits vor Inkrafttreten der DS-GVO war nach einer YouGov-Umfrage die Mehrheit der Deutschen davon überzeugt, dass dem Datenschutz eine hohe Wichtigkeit zukommt (https://www.sinusinstitut.de/fileadmin/user_data/sinus-institut/Bilder/news/Datenschutztag/Pressetext_Datenschutztag_SINUSYouGov.pdf - zuletzt abgerufen am 05. März 2021).

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 ggf. 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.[43] Sicher ist es schwer zu erklären, dass jemand für sein ehrenamtliches Engagement auch noch in Haftung genommen wird. Dennoch ist das nicht ausgeschlossen.[44] 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**.

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 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**, dessen **Motivation zum Engagement** – zweitens – durch

[43] Relevant ist regelmäßig immerhin eine ordnungswidrigkeitsrechtliche Haftung nach § 130 OWiG.

[44] Zivilrechtlich ist die Haftung in vielen Fällen allerdings gemäß § 31a BGB beschränkt.

effektiven Datenschutz sichergestellt ist. Und – drittens – an dem dem Datenschutz zu verdankenden sicheren Einsatz digitaler **Werkzeuge** und dem aus diesem folgenden **Nutzen**.

Die Zukunft des bürgerschaftlichen Engagements im Hinblick auf die Digitalisierung zeigt sich also verschachtelt. Eine Zukunft des mündigen, engagierten Bürgers, 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 Teilhabe 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 mitgedacht wird.[45]

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 es einen **Mehrwert** für die Organisation bietet – auch im Sinne der Vorbereitung auf das digitale Zeitalter, mit dem die Organisation es dann – gewappnet mit neuen Wegen und Instrumenten zur Kommunikation und Organisation – aufnehmen kann.[46] 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 Repräsentanten 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**;[47] 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.

---

[45] 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.

[46] 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. Coll, Thesenpapier zum Themenfeld Digitale Kompetenz im bürgerschaftlichen Engagement (https://www.b-b-e.de/fileadmin/Redaktion/05_Newsletter/01_BBE_Newsletter/2021/02/Newsletter-4-croll.pdf - zuletzt abgerufen am 07. März 2021), S. 6 f.

[47] 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.

3. Das Themenbewusstsein muss regelmäßig **aufgefrischt** werden. Die Motivation der Anwender*innen muss aufrechterhalten werden, so dass 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 Datenschutz-Grundverordnung (DS-GVO) 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

a. 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. solche Verpflichtungen, die sich in der Praxis als solche erweisen, revidiert werden. Die DS-GVO auf europäischer Ebene und das BDSG auf nationaler Ebene Deutschlands bedürfen einer ständigen Überprüfung[48] und ggf. auch Anpassung; die **Gesetze sind fortdauernd zu perfektionieren**. Fest steht aber auch, dass die DS-GVO (und das BDSG) auch im Rahmen des bürgerschaftlichen Engagements Geltung beansprucht. Eine Freistellung von einzelnen oder allen datenschutzrechtlichen Vorschriften sieht die DS-GVO nicht vor.[49] 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 DS-GVO eingeräumten Öffnungsklauseln bewegen. Ohne eine solche Öffnungsklausel stellte eine Abweichung unter den Standard der DS-GVO grundsätzlich den Verstoß gegen höherrangiges Recht dar. Das von der DS-GVO vorgegebene Datenschutzniveau kann vom deutschen Gesetzgeber nicht unterschritten werden.[50]

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

---

[48] Die erste Überprüfung nach Art 97 DS-GVO 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 - zuletzt abgerufen am 26. März 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/ - zuletzt abgerufen am 26. März 2021]), was aber aufgrund der kurzen bisherigen Umsetzungszeit keine Aussicht auf Erfolg haben dürfte.

[49] Siehe beispielsweise die Antwort auf die entsprechende parlamentarische Anfrage https://www.europarl.europa.eu/doceo/document/P-8-2018-003121-ASW_DE.html (zuletzt abgerufen am 01. März 2021).

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

gestaltet werden können, und zwar durchaus 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 (s.o. sub 5.).

Auch wird diskutiert, die Pflicht zur Bestellung der 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 eine Datenschutzbeauftragte 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, z.B. 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.[51] 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 DS-GVO 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.

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, so dass Datenschutz und der durch ihn entstehende zusätzliche Aufwand allgemein akzeptiert und wertschätzt wird.[52]

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 die 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

[51] Und zwar über die Anwendung der Öffnungsklausel nach Art. 23 Abs. 1 lit. e DS-GVO, wenn die Leistungsfähigkeit zivilgesellschaftlicher Akteure als „wichtiges Ziel" im Sinne dieser Norm verstanden und als gefährdet angesehen würde.

[52] Dies empfiehlt sich insbesondere auch als Aufgabe für die neue Bundeszentrale für Digitale Aufklärung.

Organisationsentwicklung und 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**[53] **Unterstützung** von Seiten der Kommunen, der Länder und des Bundes.[54] 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,[55] 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.[56]

Wichtig ist, dass das **Enabling des bürgerschaftlichen Engagements als Dauerprozess** angesehen wird. Zum einen konnte oben (sub 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**.[57] 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 50 und bei Frauen) im Wesentlichen durch **Learning by Doing** statt.[58] 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.

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.

---

[53] Beispielsweise unterstützt die Niedersächsische Landesregierung mit seinem Förderprogramm Digitalbonus einschlägige Investitionen derzeit mit einem nicht rückzahlbaren Zuschuss. Vergleichbare Programme gibt es auch in anderen Bundesländern.

[54] Bei der Einforderung von Unterstützung seitens der Politik ist immer mitzubedenken, auf welcher Ebene (Land, Bund, Europa) die Forderung anzubringen ist.

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

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

[57] 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.

[58] Vgl. Digital-Index 2019/2020, S. 26 f.; Coll, a.a.O., S. 4.

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

b. Aufsichtsbehörden

Auch an die Adresse der Datenschutzbehörden richten sich einige Forderungen. Neben der oben (sub 7.a.) bereits angesprochenen wohlwollenden Bewertung des hinsichtlich der Bestellung einer Datenschutzbeauftragten relevanten Tatbestandsmerkmals „ständig“, ist auch die **Beratung** gegenüber Verantwortlichen im Bereich des zivilgesellschaftlichen Engagements auch ohne ausdrücklichen Auftrag durch das BDSG wieder (wie unter Geltung des BDSG a.F.) 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 DS-GVO) 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 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.

Aus der im Hinblick auf das anspruchsvolle Datenschutzrecht einerseits und im Hinblick auf 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**.

c. 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) 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, so dass notwendige Veränderungs- und Anpassungsprozesse fundiert begründet betrieben und dafür nötige spezifische Unterstützungen ggf. 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 DS-GVO 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.[59] Als besonders praxisrelevant kann sich die

[59] Ein Unterschreiten des Niveaus der DS-GVO 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 die

Konkretisierung der berechtigten Interessen, die Präzisierung einer fairen und transparenten Verarbeitung (z.B. im Hinblick auf die Erfüllung von Informationspflichten) und die Konkretisierung technischer und organisatorischer Maßnahmen durch Verhaltensregeln erweisen.

Darüber hinaus können Verbände **Erfahrungsaustausche organisieren**, ggf. auch die **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 **Datenschutz-Patenschaften** für Organisationen des bürgerschaftlichen Engagements bereitstellen.

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

———

Einhaltung der Regeln bei der Bewertung eines Datenschutzvorfalls besonderes Gewicht verleihen, was sich im Rahmen der Ahndung als günstig herausstellen dürfte.