Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

LEITFADEN

vom 1. Dezember 2018

der Datenschutzbehörden von Bund und Kantonen

zur Anwendung des Datenschutzrechts auf die digitale Bearbeitung von Personendaten im Zusammenhang mit Wahlen und Abstimmungen in der Schweiz

Letzte Aktualisierung 1. Juni 2019

Der Leitfaden entstand in Zusammenarbeit mit den Experten
Urs Maurer-Lambrou, Fürsprecher, LL.M., und Prof. Dr. Adrian Vatter, Politologe.

Zur Förderung der allgemeinen Verständlichkeit wird im vorliegenden Dokument auf spezifische Gesetzesverweise verzichtet.

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Inhaltsverzeichnis

1 Zweck und Adressaten des Leitfadens

Die digitale Gesellschaft ist eine globale Realität, in der sich auch Wahlen und Abstimmungen auf allen föderalen Stufen der Eidgenossenschaft abspielen. Es treten laufend neue Datenbearbeitungs-Phänomene in Erscheinung, die sich auf das Wahl- oder Abstimmungsverhalten auswirken können. Online-Kommunikation bietet den Akteuren des politischen Meinungsbildungs-Prozesses die Chance, rasch und kostengünstig bei den Stimmberechtigten Botschaften abzusetzen oder mit ihnen in einen Dialog zu treten, gerade auch, wenn diese traditionellen Medien aus Kosten- oder anderen Gründen meiden und vornehmlich digitale Datenplattformen für ihren Informationsbedarf und den sozialen Austausch nutzen.

Im E-Commerce-Bereich werden automatisiert grosse Mengen von Personendaten beschafft und bearbeitet. Durch Analysen dieser Daten werden bestehenden oder potentiellen Kunden mit personalisierten Werbebotschaften auf ihr Profil passende Waren und Dienstleistungen angeboten. Die automatisierten Bearbeitungsmethoden von «Big Data», «Analytics», Profilbildung und «Microtargeting» werden auch zur gezielten Ansprache von Stimmberechtigten zwecks Vermittlung von Informationen eingesetzt, mit denen Parteien und Interessengruppen die politische Meinungsbildung im Vorfeld von Abstimmungen und Wahlen zu beeinflussen suchen.

Soweit diese Bearbeitungsmethoden Bezüge zu bestimmten oder bestimmbaren Personen herstellen und von Privaten oder Bundesorganen ausgehen, unterliegen sie dem Bundesgesetz über den Datenschutz (DSG) und der Aufsichtstätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Wenn solche Bearbeitungen von Organen des öffentlichen Rechts der Kantone ausgehen, die sich mit der Durchführung von Wahlen und Abstimmungen befassen, sind indessen die kantonalen Datenschutzgesetzgebungen und die lokale Datenschutzaufsicht massgebend, woraus sich denn auch die gemeinsame Autorenschaft dieses Leitfadens durch den EDÖB und die Konferenz der kantonalen Datenschutzbeauftragten (Privatim) ableitet.

Die Garantie der politischen Rechte schützt gemäss Bundesverfassung die freie Willensbildung und die unverfälschte Stimmabgabe. Die Datenschutzbehörden leisten einen Beitrag zum verfassungsmässigen Ablauf des politischen Prozesses, indem sie die Akteure dazu anhalten, die von der Datenschutzgesetzgebung garantierte Wahrung der Privatsphäre und informationellen Selbstbestimmung der Bevölkerung sowie die davon abgeleiteten Grundsätze für die Bearbeitung von Personendaten zu respektieren. Wer Daten im Kontext von Wahlen und Abstimmungen bearbeitet, soll sich bewusst sein, dass das Datenschutzrecht Angaben zu politischen und weltanschaulichen Ansichten einem höheren Schutzniveau unterstellt als vergleichbare Daten im gewerblich-kommerziellen Umfeld.

Die Datenschutzbehörden verfassen diesen Leitfaden in Ausübung ihrer gesetzlichen Aufgabe, Private und öffentliche Organe zu beraten sowie die Öffentlichkeit für systemische Risiken der Personendatenbearbeitung zu sensibilisieren. Er ist als Auslegungshilfe zu verstehen, um das aus dem Jahre 1992 stammende DSG im dynamischen Umfeld der Digitalisierung auf die Datenbearbeitung im Kontext von Wahlen und Abstimmungen anzuwenden. Er richtet sich an alle Akteure der politischen Meinungsbildung und will sie dazu anhalten, die digitalen Bearbeitungsmethoden erkenn- und nachvollziehbar zu machen. Von diesem datenschutzrechtlichen Anspruch auf Transparenz abzugrenzen gilt es die in der öffentlichen Diskussion unter dem Schlagwort der sog. «Fake News» thematisierte Problematik des Wahrheitsgehalts von Sachinhalten, die weder Gegenstand der Datenschutzgesetzgebung ist noch Thema dieses Leitfadens sein kann. Ebenso bleibt die Thematik des E-Votings hier ausgeklammert.

2 Politische Parteien und Interessengruppen

Die Datenbearbeitung im politischen Prozess und die damit verbundene legitime Zielsetzung, auf die politische Meinungsbildung einzuwirken, gehen in erster Linie von politischen Parteien und Interessengruppen aus, die unter privatrechtlichen Rechtsformen wie bspw. des Vereins oder der Stiftung politische, religiöse, soziale, wissenschaftliche und weitere ideelle Zwecke verfolgen.

Obwohl dazu noch keine umfassende Rechtsprechung vorliegt, ist davon auszugehen, dass digitale Datenbearbeitungen im Zusammenhang mit dem politischen Prozess allein schon aufgrund ihrer Zweckausrichtung, weltanschauliche Ansichten von vielen Menschen zu beeinflussen, in der Regel dem für besonders schützenswerte Personendaten geltenden Schutzniveau unterliegen. Dies insbesondere dann, wenn automatisierte Analysemethoden angewendet werden, die durch Abgleichung einer Vielzahl von sensiblen oder auch nicht sensiblen Daten zu Persönlichkeitsprofilen führen, die gemäss der Rechtsprechung des Bundesverwaltungsgerichts in Sachen Moneyhouse[1] ebenfalls einen erhöhten Schutz der Betroffenen indizieren. Politische Parteien und Interessengruppen werden als private «Inhaber» von Datensammlungen somit ihrer Gesamtverantwortung etwa für die Beschaffung, Aufbewahrung, Pflege und Weiterverwendung der dort bearbeiteten Daten Rechnung tragen (vgl. Tabelle A). Sie orientieren sich dabei am fundamentalen Prinzip der Transparenz (Ziff. 7). Nur wenn die Parteien und Interessengruppen für die Stimmbürger genügend erkenn- und nachvollziehbar machen, welche Bearbeitungsmethoden sie zur Anwendung bringen, können diese auf Akzeptanz stossen.

Den Parteien und Interessengruppen steht es im Kontext zum politischen Prozess frei, bei der Bearbeitung von Daten Dritte einzusetzen, indem sie den Prozess ganz oder teilweise an solche übertragen oder Daten von Dritten beziehen. Im Rahmen ihrer Gesamtverantwortung als Inhaber machen sie die Einschaltung und die Rollen dieser je nach Umständen ebenfalls als Inhaber oder nur als Auftragsbearbeiter handelnden Dritten transparent. Sie vergewissern sich, dass Letztere ihrerseits die Vorgaben der Datenschutzgesetzgebung einhalten (s. Tabelle A).

3 Öffentliche Register

Die Kantone führen über die Stimmberechtigten ein Register – das Stimmregister. Basis für das Stimmregister bildet die Einwohnerkontrolle. Zu- und wegziehende Personen sind durch die Gesetzgebung über Niederlassung und Aufenthalt verpflichtet, sich bei der Gemeinde unter Vorlage eines amtlichen Dokumentes an- und abzumelden und werden in der Einwohnerkontrolle ein- resp. ausgetragen. Die Einwohnerkontrolle erlaubt es daher, Beginn und Ende der Stimmberechtigung zu bestimmen und im Stimmregister korrekt festzuhalten. Die Stimmregister bilden sowohl Basis für Wahlen und Abstimmungen des Bundes als auch der Kantone und der Gemeinden. Das Bundesrecht gibt vor, dass das Stimmregister den Stimmberechtigten zur Einsicht offensteht. In welcher Form den Stimmberechtigten diese Einsicht gewährt wird (Einsicht vor Ort, Abgabe von Papierlisten, Abgabe in digitaler Form) bestimmen die Kantone. Sie regeln ebenfalls, ob und in welcher Form Einsicht in die Einwohnerkontrolle gewährt wird.

Gewisse Kantone fassen die kommunalen Einwohnerkontrollen zu einem Register aller Einwohnerinnen und Einwohner des Kantons zusammen. Nicht selten werden diese zentralen Register mit weiteren Daten (zum Beispiel E-Mail-Adresse und Handynummer aus der Steuererklärung) angereichert.

[1] BVGer Entscheid A-4232/2015 vom 18. April 2017

Im Rahmen ihrer Gesamtverantwortung als Inhaber von staatlichen Datensammlungen haben sich die für die öffentlichen Register zuständigen Gemeinwesen zu vergewissern, dass die dort bearbeiteten Daten sicher aufbewahrt und nur soweit rechtlich zulässig an Dritte weitergegeben werden. Sie müssen Gewähr dafür bieten, dass es zu keinen zweckwidrigen Verwendungen oder unkontrollierten Datenabflüssen kommen kann (s. Tabelle B).

Die von den Gemeinwesen zum Schutz dieser zentralen Dateien getroffenen technischen und organisatorischen Massnahmen sind unterschiedlich. Bei den Adress- und Kontaktdaten handelt es sich zwar um Personendaten, die unter die Datenschutzgesetzgebung fallen, jedoch grundsätzlich nicht um besonders schützenswerte.

Das kantonale Recht kann vorsehen, dass die Einwohnerkontrollen der Gemeinden auf Gesuch von interessierten Privaten, Parteien oder anderen Dritten hin Adressdaten von Einwohnern nach bestimmten Kriterien geordnet (d.h. mittels Listen, z. B. Jungbürger) bekannt geben dürfen. In der Regel dürfen diese Listen vom Gesuchsteller nur für bestimmte, häufig ideelle Zwecke verwendet werden und nicht an Dritte weitergegeben werden. Die zuständige Stelle der Gemeinde prüft, ob die gesetzlichen Voraussetzungen für eine Bekanntgabe gegeben sind und kann anschliessend die Daten an den Gesuchsteller herausgeben. Gemeindeeinwohner, die ihre Personendaten in der Einwohnerkontrolle schützen wollen, haben in der Regel die Möglichkeit, ihre Daten für eine Listenbekanntgabe oder generell für eine Weitergabe an Dritte zu sperren. Dies setzt voraus, dass die Gemeinde die betroffenen Personen über die Bedingungen und das Ausmass der Bekanntgabe und die Sperrmöglichkeiten informiert. Spezifische Sperrmöglichkeiten für politische Werbung werden bislang von den Behörden kaum angeboten. In der Praxis wird versucht, mit geeigneten Massnahmen dafür zu sorgen, dass die in der Einwohnerkontrolle oder im Stimmregister gegeben Schutzmassnahmen wie beispielsweise das Sperrecht in der Einwohnerkontrolle nicht durch eine Einsicht in das jeweils andere Register unterlaufen werden.

4 Prozess der Datenbearbeitung

Als Datenbearbeitung gilt gemäss Legaldefinition jeder Umgang mit Daten, unabhängig von den angewandten Mitteln und Verfahren. Zur Veranschaulichung lässt sich dieser Prozess im Kontext von Wahlen und Abstimmungen funktional in die Beschaffung, Analyse sowie die Zuweisung von Informationen aufteilen.

4.1 Beschaffung

Die Parteien und Interessengruppen können für die Datenbearbeitung im politischen Prozess zunächst auf selbst beschaffte Datenbestände wie Mitgliederadressen, E-Mail-Adresslisten von Newsletter-Abonnenten und ähnliche Informationen zurückgreifen. Oft werden diese eigenen Daten durch Informationen ergänzt, welche die Parteien und Interessengruppen durch Unterschriftensammlungen oder mittels persönlicher Ansprache der Bevölkerung an Ständen, bei Hausbesuchen oder über Telefonate erlangen. Bei diesen direkten Kontakten können neben den Kontaktdaten der angesprochenen Personen individuelle politische Präferenzen und weitere für die Parteien oder Interessengruppen relevante Informationen nachgefragt werden. Zusätzlich können die Parteien und Interessengruppen Daten aus öffentlich zugänglichen Quellen wie Telefonverzeichnissen oder öffentlichen Registern beschaffen.

Sie können im Internet Portale oder statistische Webseiten mit Hilfe von Web-Mining zur Datenbeschaffung nutzen, damit Dritte beauftragen oder die entsprechenden Informationen käuflich erwerben. Web-

Crawler-Dienste können Inhalte von Webseiten oder E-Mailadressen systematisch suchen und die gewünschten Informationen beschaffen. Eine weitere mögliche Datenquelle sind Datenplattformen.

Die beschafften Daten werden von den Parteien oder Interessengruppen zusammengetragen und können mithilfe einer Kampagnen-Software bewirtschaftet werden. Aufgebaut in etwa wie ein flexibles Content Management System (CMS) verbinden solche Anwendungen alle gängigen sozialen Netzwerke zu einem System, welches die Interaktionen mit bestimmten Personengruppen erlaubt. Einmal im Besitz einer E-Mail-Adresse, können die Parteien und Interessengruppen über eine bestimmte Funktion («Social Match») in den sozialen Netzwerken nach der zugehörigen Person suchen und ihre Datensammlung mit den zugehörigen Informationen anreichern (vgl. Ziff. 7).

Die Kampagnen-Software unterstützt die Partei oder die Interessengruppe anschliessend bei der Planung und Durchführung von Aktionen und erlaubt es, das Potenzial der eigenen Datensammlung mit den Möglichkeiten von sozialen Netzwerken zu verbinden, indem sich die Analyse- und Selektionsmöglichkeiten der sozialen Netzwerke zentral innerhalb der Software nutzen lassen.

Bei jeder Form der Beschaffung von Daten für politische Zwecke beachten die Verantwortlichen insbesondere den Grundsatz der Transparenz (Ziff. 7). Bei der Beschaffung von Informationen wie weltanschauliche oder politischen Ansichten ist zu beachten, dass diese einem qualifizierten gesetzlichen Schutz (Ziff. 7) unterstehen.

4.2 Analyse

Im Sinne von «Big Data» werden im E-Commerce-Bereich über einen längeren Zeitraum grosse Mengen von heterogenen Daten bearbeitet, die zu Analysezwecken aggregiert und zusammengetragen werden. Mithilfe von leistungsstarken Computersystemen und Analysemethoden können Daten ausgewertet und die Interessen einzelner oder kleiner Gruppen ähnlich denkender Personen identifiziert werden. Mithilfe von statistischen Modellen können Vorhersagen getroffen werden, welche Produkte oder Dienstleistungen für welche Profilgruppen von bestehenden oder neuen Kunden geeignet sind («Predictive Analytics»). Die bestehenden oder potentiellen Kunden werden dann mit den für ihr Profil zugeschnittenen Werbebotschaften beworben oder erhalten beispielsweise in einem Onlineshop für sie passende Produkteempfehlungen.

Profilbildung im politischen Kontext zielt darauf ab, dass sich jede Profilgruppe nicht nur in ihren gemeinsamen Interessen von anderen Gruppen unterscheidet, sondern dass sich auch die Personen innerhalb dieser Gruppen stärker in ihren politischen Positionen und Vorstellungen ähneln als Personen aus verschieden Gruppen.

Die Segmentierung der Personen basierend auf ihren demografischen, ideologischen, sozioökonomischen und psychischen Eigenschaften sowie verschiedenen Methoden der künstlichen Intelligenz wird zur Vorhersage ihres Verhaltens verwendet. Diese Profile können dazu verwendet werden, die betroffenen Personen gezielt mit politischen Botschaften anzusprechen.

Bereits bei der Zusammenstellung von Daten ist durch die Inhaber dieser Datensammlung zu beachten, dass eine Vielzahl von sensiblen – sprich besonders schützenswerten – oder an sich unsensiblen Daten

sich zu Persönlichkeitsprofilen im Sinne des Datenschutzgesetzes verdichten können. Diese unterstehen einem qualifizierten bzw. höheren gesetzlichem Schutz. Das Bundesverwaltungsgericht hat sich im Moneyhouse-Urteil (Ziff. 2) ausführlich zu dieser Thematik geäussert. Der qualifizierte Schutz gilt auch für die Bearbeitung von sensiblen Daten wie weltanschauliche oder politischen Ansichten, welche der Gesetzgeber einem besonderen Schutz unterstellt hat (Ziff. 7).

4.3 Zuweisung von Informationen

Unter der Annahme, dass die Personen einer gemeinsamen Profilgruppe auf bestimmte Botschaften besonders stark reagieren, sollen den einzelnen Gruppen gezielt Informationen über E-Mail-Verteiler oder auf sozialen Medien vermittelt werden. Mit diesem Vorgehen suchen Parteien und Interessengruppen die politische Meinungsbildung im Vorfeld von Abstimmungen und Wahlen zu beeinflussen. Beim sog. «Microtargeting» werden nicht nur Botschaften oder Inhalte, sondern auch die Art und Weise der Ansprache individualisiert. Dies setzt voraus, dass die Kenntnis über die Zielpersonen auf Basis der gesammelten Daten so genau ist, dass für sie passende politischen Botschaften über ihre bevorzugten Kommunikationskanäle vermittelt werden können.

«Microtargeting» kann die angestrebte beeinflussende Wirkung insbesondere bei Abstimmungen entfalten, da dort erfahrungsgemäss eine grössere Menge der Stimmberechtigten noch keine gefestigte Meinung zu einem bestimmten Thema hat. Bei Proporzwahlen wie den Nationalratswahlen wird demgegenüber oft ein gefestigtes, auf Tradition und Gewohnheit basierendes Wahlverhalten beobachtet. Wieder anders kann es sich bei Ständeratswahlen verhalten, wenn Kandidaten parteiübergreifend gefördert werden.

Personalisiert zugewiesene Botschaften im politischen Kontext müssen nicht immer darauf abzielen, das Wahl- oder Abstimmungsverhalten inhaltlich zu beeinflussen. Vielmehr können sie darauf hinwirken, bereits die Wahrnehmung der politischen Rechte zu fördern oder zu hemmen, je nachdem, ob die ausgewerteten Daten der Adressaten, diese eher als politischen Freund oder Gegner ausweisen. Eine weitere Möglichkeit besteht darin, zwar nur zur Wahrnehmung des Stimm- und Wahlrechts aufzurufen, diese Botschaften dann aber selektiv – unter Weglassung vermuteter politischer Gegner – zu versenden.

5 Weitere Akteure der Datenbearbeitung

5.1 Datenhändler

Professionelle Adresshändler und Anbieter ähnlicher Dienstleistungen beschaffen Informationen aller Art, die sie systematisch und soweit möglich strukturiert, nach personenbezogenen Merkmalen erschlossen bearbeiten und vermarkten. Die angebotenen Daten stammen aus einer Vielzahl von Anträgen, Registrierungen, Bestellungen und Erklärungen, die im Kontext mit Bestellungen von Waren und Dienstleistungen, Geschäftsbedingung oder Wettbewerben ausgefüllt werden. Auch behördlich publizierte Informationen wie Statistiken zu Wahlergebnissen oder Arbeitslosenquoten und öffentliche Bekanntmachungen, Handelsregister und Schuldnerverzeichnisse werden als Datenquellen genutzt. Wei-

tere Daten werden mittels Umfragen bei Konsumenten erhoben oder durch Auswertung allgemein zugänglicher Quellen gesammelt. Mittels Kombination von Daten aus unterschiedlichen Quellen reichern diese professionellen Anbieter zum Beispiel Privatadressen mit diversen Zusatzinformationen an wie zum Konsumverhalten, zur Soziodemografie oder zur Wohn- und Lebenssituation.

Private Datenhändler bearbeiten personenbezogene Daten im Kontext mit dem politischen Prozess als gesamtverantwortliche Inhaber (vgl. Hinweise in Tabelle A) oder als Auftragsbearbeiter (vgl. Tabelle C).

5.2 Datenanalyse-Unternehmen

Datenanalyse-Unternehmen können als Beauftragte die Bewirtschaftung und Analyse der relevanten Daten der Parteien oder Interessengruppen übernehmen. Dies können beispielsweise Kommunikationsagenturen oder andere Unternehmen sein, die sich auf bestimmte Analyseverfahren spezialisiert haben (z.B. Website-Analyse, Crawler-Agenturen).

Datenanalyse-Unternehmen können gleichzeitig auch Datenhändler sein, die selbständig Informationen aus unterschiedlichen Quellen beschaffen, diese auswerten und dann den interessierten Gruppen gegen Entgelt zur Verfügung stellen.

Private Datenhändler bearbeiten personenbezogene Daten im Kontext mit dem politischen Prozess als gesamtverantwortliche Inhaber (vgl. Hinweise in Tabelle A) oder als Auftragsbearbeiter (vgl. Tabelle C).

5.3 Datenplattformen

Datenplattformen von Suchmaschinenbetreibern wie Google oder virtuelle Begegnung und Kommunikation erleichternde soziale Netzwerke wie Facebook oder Twitter sammeln personenbezogene Attribute wie Namen, Geschlecht und Alter, welche die über ein Konto verfügenden registrierten Nutzer angegeben haben. Dazu kommen umfangreiche automatisch aufgezeichnete Datenspuren, welche sowohl die registrierten als auch alle übrigen Benutzer des Internets beim Besuch von Datenplattformen hinterlassen. Darunter fallen technische Daten wie IP-Adressen oder Gerätenummern sowie Informationen über die mit «Gefällt mir» markierten Seiten, geteilte Botschaften etc. Daneben werden Informationen von externen Webseiten oder Apps gesammelt, die mit den jeweiligen Plattformen auf Grundlage von Werbepartnerschaften verbunden sind.

Andere Plattformen, welche sich auf das Unterschriftensammeln für Abstimmungen spezialisiert haben, sammeln grosse Mengen von Kontaktdaten mit E-Mail-Adressen, Wohnadressen und Angaben über politische Präferenzen. Die Plattformen werden entweder von den Parteien oder Interessengruppen selbst bewirtschaftet oder stellen als Drittanbieter ihre Leistungen und Daten Interessierten zur Verfügung.

Soweit private Datenplattformen personenbezogene Daten im Kontext mit dem politischen Prozess als gesamtverantwortliche Inhaber bearbeiten, sind die Hinweise in Tabelle A und Tabelle D zu beachten. Soweit sie solche Daten als Auftragsbearbeiter bearbeiten oder weitergeben, gibt Tabelle C entsprechende Hinweise.

5.4 Einzelpersonen (Adressaten)

Adressat von Informationen, die zum Zwecke der politischen Meinungsbildung im Vorfeld von Wahlen und Abstimmungen bearbeitet werden, ist die stimm- und wahlberechtigte Bevölkerung. Während politische Werbung über Radio und Fernsehen untersagt ist und Printmedien politische Inserate ohne vorherige Interaktion mit einzelnen Lesern vermitteln, bieten Datenplattformen die Möglichkeit, politische Botschaften gezielt an einzelne Personen oder Gruppen von Personen zu übermitteln. Letztere können die zugespielten Botschaften dann ihrerseits kommentieren und weiterverbreiten. Indem sich auf den grössten Plattformen weltweit Milliarden von Nutzern austauschen, akkumulieren nicht nur die Betreiber der Netzwerke, sondern auch deren Kundschaft grosse Mengen von Adress-, Text-, Ton- und Bilddaten, die sich auf deren Familien, Freunde und Bekannte beziehen und Rückschlüsse auf Weltanschauung und politische Präferenzen zulassen. Solche Informationen werden mit den damit verbundenen Benutzerkonten in den Rechenzentren der Plattformbetreiber und zum Teil auch auf den Smartphones und übrigen Rechner der Benutzer gespeichert. Durch deren gezielte Weitergabe oder öffentliche Verbreitung versetzen sie sich und Dritte in die Lage, die politische Meinungsäusserung sowie das Wahl- oder Stimmverhalten anderer Personen zu beeinflussen. Wie die professionellen Inhaber von Datensammlungen tragen somit auch die einzelnen Adressaten als Privatpersonen eine Bearbeitungsverantwortung für die von ihnen im politischen Kontext bearbeiteten Personendaten (vgl. Tabelle E). Dass sie ihre Verantwortung wahrnehmen können, setzt zunächst voraus, dass sie sich dieser Tatsache überhaupt bewusst werden.

6 Allgemein geltende Bearbeitungsgrundsätze

Jeder Akteur, der im Kontext von Wahlen und Abstimmungen Personendaten bearbeitet, hat die allgemeinen Bearbeitungsgrundsätze der Datenschutzgesetzgebung zu beachten:

Als Personendaten gelten dabei alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Daten, die Rückschlüsse auf politische oder weltanschauliche Ansichten zulassen, gelten als besonders schützenswert, sodass deren Bearbeitung durch das Gesetz besonders geschützt ist. Durch die Bearbeitung von an sich unsensiblen Daten können durch weitere Bearbeitungsschritte wie Datenanalysen oder Anreicherungen besonders schützenswerte Personendaten oder Persönlichkeitsprofile entstehen, welche gemäss der Rechtsprechung des Bundesverwaltungsgerichts i.S. Moneyhouse (Ziff. 2) wiederum durch das Gesetz besonders geschützt sind.

Die Bearbeitung von Personendaten muss zunächst nach Treu und Glauben erfolgen. Dies bedeutet, dass die Daten nicht in einer Art erhoben und bearbeitet werden dürfen, mit der die betroffene Person aus den Umständen heraus nicht rechnen musste und mit der sie vermutlich nicht einverstanden gewesen wäre. Dies bedeutet, dass für die betroffenen Personen die Beschaffung und jede Bearbeitung ihrer Daten erkennbar sein müssen. Dies gilt ebenso für den Zweck jeder Datenbearbeitung, die Identität des Datenbearbeiters und – bei einer Weitergabe der Daten an Dritte – die Kategorien von möglichen Datenempfängern. Auch die Beschaffung von Personendaten bei Dritten wie beispielsweise Datenhändlern muss für die betroffenen Personen erkennbar sein.

Die Bearbeitung muss sich weiter hinsichtlich der Menge der bearbeiteten Personendaten und bezüglich ihrer Dauer am Grundsatz der Verhältnismässigkeit ausrichten. Verhältnismässigkeit bedeutet, dass ein

Datenbearbeiter nur diejenigen Daten bearbeiten darf, die geeignet und objektiv gesehen erforderlich sind, um ein (legitimes) Ziel zu erreichen. Dabei müssen bei der Bearbeitung der Daten das verfolgte Ziel und die verwendeten Mittel in einem vernünftigen Verhältnis zueinanderstehen und die Recht der betroffenen Personen gewahrt werden. Die Datenbearbeitung muss für die betroffenen Personen sowohl hinsichtlich ihres Zwecks als auch hinsichtlich ihrer Mittel zumutbar sein.

Nach dem Zweckbindungsgrundsatz dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei deren Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Ohne einen besonderen Rechtfertigungsgrund dürfen die Daten im Nachhinein nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Zweckbindungsgrundsatz gilt insbesondere auch bei der Einbindung von Services oder Applikationen von Dritten (z.B. Newsletter-Services oder Software zur Planung und Verwaltung der Haustürbesuche), welche die Daten nicht ohne Weiteres für eigene Zwecke verwenden dürfen (vgl. auch Ziff. 7).

Wer über eine Datensammlung verfügt, hat sich auch über die Richtigkeit der darin enthaltenen Daten, soweit diese eine Personenrelevanz aufweisen, zu vergewissern. Der Datenbearbeiter hat alle angemessenen Massnahmen zu treffen, damit die Personendaten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Reine Sachdaten, die keine Bezüge zu bestimmten oder bestimmbaren Personen aufweisen, fallen nicht unter die Geltung des Datenschutzrechts, woraus sich ableitet, dass der Wahrheitsgehalt von politischen Sachinhalten und die Problematik der sog. «Fake News» nicht eigentlich Gegenstand des Datenschutzrechts ist.

Schliesslich müssen nach dem Grundsatz der Datensicherheit Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Zum Schutz verpflichtet ist nicht nur der Inhaber einer Datensammlung, sondern jeder Datenbearbeiter und zwar selbst dann, wenn die betreffenden Personendaten keine Datensammlung darstellen. Die Pflicht trifft somit jeden Akteur im Kontext von Wahlen und Abstimmungen, welcher Personendaten bearbeitet. Die spezifischen datenschutzrechtlichen, organisatorischen und technischen Risiken sind abzuschätzen und geeignete Schutzmassnahmen zu treffen. Dies setzt voraus, dass eine interne Dokumentation vorliegt, aus der hervorgeht, wie die genannten Pflichten hinsichtlich der verschiedenen Kategorien von bearbeiteten Daten erfüllt werden.

7 Anspruch der Stimmberechtigten auf Transparenz

Weiter haben die Akteure die besondere Relevanz des Grundsatzes der Transparenz zu beachten. Dieser verleiht den Stimmberechtigten einen datenschutzrechtlichen Anspruch darauf, nachvollziehen zu können, aufgrund welcher digitaler Bearbeitungsmethoden und Technologien sie angesprochen und politisch beeinflusst werden.

Staatliche Organe, die im Kontext von Wahlen und Abstimmungen Daten zur Verfügung stellen, erfüllen den datenschutzrechtlichen Transparenzanspruch, indem sie sich bei ihrer Aufgabenerfüllung an den Rahmen der öffentlich zugänglichen gesetzlichen Grundlagen halten.

Als Grundlage für die Personendatenbearbeitung durch private Akteure wie Parteien oder Interessengruppen kann alternativ die Einwilligung der betroffenen Personen, ein überwiegendes privates oder öffentliches Interesse vorliegen. In der Praxis kommt im politischen Kontext meist nur die Einwilligung der Betroffenen in Frage. Diese ist nur dann gültig, wenn sie nach angemessener Information und freiwillig erfolgt. Wie dargelegt, werden im politischen Kontext in der Regel personenbezogene Daten über

politische oder weltanschauliche Ansichten bearbeitet, die in die Kategorie der besonders schützenswerten Personendaten fallen. Durch die Verknüpfung der Daten, welche die betroffenen Personen zum Beispiel auf Webseiten und sozialen Plattformen zurücklassen, können Persönlichkeitsprofile entstehen. Liegt weder ein Rechtfertigungsgrund durch Gesetz noch ein überwiegendes privates oder öffentliches Interesse vor, setzt die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen eine ausdrückliche Einwilligung der betroffenen Personen voraus. Im politischen Kontext dürfen Daten über Personen somit bearbeitet werden, wenn diese ausdrücklich, selbstbestimmt und hinreichend informiert in deren Anwendung eingewilligt haben.

Die Akteure des politischen Meinungsbildungsprozesses bearbeiten Daten nur zu den Zwecken, in dem Umfang und mit jenen Methoden, für die eine Einwilligung vorliegt. Eine ausdrückliche Einwilligung liegt namentlich dann vor, wenn sich die betroffenen Personen auf der Webseite eines Akteurs registriert haben und sich ausdrücklich (z.B. durch Setzen eines entsprechenden Häkchens) damit einverstanden erklären, dass ihre hinterlegten Daten entsprechend bearbeitet werden. Erklärungen, mit denen Personen lediglich in genereller Weise Nutzungsbedingungen annehmen, sind hingegen keine ausdrücklichen Einwilligungen. Das gleiche gilt für Äusserungen, mit denen Anliegen und Inhalte der Akteure beispielsweise auf sozialen Plattformen abonniert oder kommentiert werden. Einwilligungen können sich zudem nur auf die eigenen Daten beziehen. Die Bearbeitung der Daten von Drittpersonen setzt wiederum deren Einwilligung voraus.

Selbstbestimmt ist die Einwilligung, wenn die Betroffenen hinsichtlich der Aktivierung oder Desaktivierung einzelner Aspekte und Funktionalitäten der digitalen Applikationen (z.B. durch setzen entsprechender Häkchen) differenziert einwilligen können und dadurch eine echte Wahl haben, nicht nur ob, sondern auch in welchem Mass sie ihre Daten zur Verfügung stellen. Zudem müssen die Betroffenen jederzeit die Möglichkeit haben, ihre Einwilligung zu widerrufen und die Löschung ihrer Daten zu verlangen. Die Erfüllung dieser Ansprüche setzt seitens der Akteure Investitionen in datenschutzfreundliche Technologien voraus.

Eine informierte Einwilligung setzt voraus, dass interessierte Personen vor der Registrierung fair und vollständig über die Bearbeitung ihrer Daten und die Funktionsweise der dafür eingesetzten Analysemethoden inklusive automatisierte Programme und künstliche Intelligenz ins Bild gesetzt werden. Zu informieren sind sie auch über ihre Rechte, wie beispielsweise jenes des jederzeitigen Widerrufs. Fair bedeutet, dass die Information sprachlich leicht verständlich, rasch auffindbar und übersichtlich vermittelt wird. Vollständig sind Online-Texte, welche die Zwecke und Wirkungsweisen der digitalen Bearbeitungsmethoden und Technologien in mehreren adressatengerechten Erklärungstiefen zugänglich machen und insbesondere über die Dauer der Bearbeitung und die allfällige Weitergabe der Daten Auskunft geben. Die Kaskade der Informationen beginnt mit einer gut sichtbaren Kurzinformation auf der Registrierungsseite, welche die wichtigsten Punkte der Datenbearbeitung erklärt. Jeder dieser Punkte enthält weiterführende Links, die den Leser auf die jeweils relevanten Passagen der einschlägigen Bearbeitungsreglemente und Datenschutzbestimmungen führen. Zur fairen Information gehört insbesondere im politischen Kontext, dass die Betroffenen nicht mit irreführenden oder falschen Angaben zu Absendern und Quellen getäuscht oder im Falle von Individualkommunikation im Ungewissen darüber gelassen werden, ob sie mit einem menschlichen Wesen oder einem automatisierten Programm interagieren. Weiter muss für sie erkennbar sein, ob eine Online-Zuweisung von Informationen personalisiert oder an jedermann erfolgt. Gegebenenfalls muss aufgrund der Nutzungsbedingungen nachvollziehbar sein, unter Beizug welcher Technologien resp. Verfahren und nach welchen Kriterien personalisierte Zuweisungen erfolgen. Zur vollständigen Information gehören auch Angaben über die Bearbeitung von Daten, die mit Informationen aus sozialen Medien angereichert und ausgewertet werden („Social Match“).

8 Zusammenfassende Übersicht

A **Parteien und Interessengruppen**	Soweit Parteien und Interessengruppen eine Gesamtverantwortung i.S. eines ***Inhabers*** einer ***Datensammlung*** wahrnehmen (Ziff. 2), tragen sie folgenden Hinweisen Rechnung: • Die Bearbeitung erfolgt unabhängig von der Einschaltung Dritter ***rechtmässig*** und unter Einhaltung der allg. Grundsätze des DSG (Ziff. 6). • ***Beauftragte Dritte*** werden angehalten nachzuweisen, dass sie angemessene organisatorische und technische Massnahmen zur Datensicherheit (Ziff. 6) ergreifen. • Der Anspruch der Stimmberechtigten auf ***Transparenz*** (Ziff. 7) wird erfüllt durch ***Website gestützte Informationen*** über - die Identität der verantwortlichen Inhaber der Sammlung; - die Kategorien der bearbeiteten Daten; - die Datenbeschaffung mit Hinweis auf Drittquellen; - den aktuellen Zweck und Rechtfertigungsgrund der Bearbeitung; - die Bearbeitungsmethoden unter Einschluss des Zwecks und der Funktionsweise der zum Einsatz gelangenden Analysemethoden inkl. künstlicher Intelligenz; - die Kategorien allfälliger Datenempfänger; - die Rollen, Pflichten und Verantwortlichkeiten von Datenlieferanten, Datenanalyseunternehmen oder Datenplattformen; - die massgebenden Nutzungsbedingungen Dritter und deren Fundstellen. • Die Bearbeitung erfolgt unter Beachtung der Grundsätze der ***Zweckbindung*** (Ziff. 6) und der ***Verhältnismässigkeit*** (Ziff. 6), wonach eine weitere Bearbeitung stets innerhalb des der Beschaffung zu Grunde liegenden Zweckes und der Dauer bis zur Erreichung dieses Zwecks erfolgt; • Erforderliche ***Einwilligungen*** für die Bearbeitung von Personendaten im Kontext mit dem politischen Prozess werden ***ausdrücklich*** eingeholt (Ziff. 7); • Die ***Datenrichtigkeit*** ist auch bei Einschaltung Dritter gewährleistet und nicht mehr benötigte Daten sind gelöscht (Ziff. 6); • Die datenschutzrechtlichen, organisatorischen und technischen ***Risiken werden abgeschätzt*** und geeignete Schutzmassnahmen getroffen (Ziff. 6). • Es bestehen interne ***Dokumentation***, aus denen hervorgeht, wie die Sicherheit der verschiedenen Kategorien von bearbeiteten Daten gewährleistet wird (Ziff. 6); • Bei der Verwendung von Services oder Applikationen von Dritten (z.B. Newsletter-Services oder die Planung und Verwaltung von Haustürbesuchen) werden die geltenden Vorgaben betreffend die Datenbekanntgabe an Dritte und die Weitergabe von Personendaten ins Ausland eingehalten. (vgl. dazu insbesondere unser Merkblatt

	«Datenübermittlung ins Ausland kurz erklärt» sowie unsere «Erläuterungen zur Übermittlung von Personendaten ins Ausland»; • Die Auskunftsrechte der betroffenen Personen sowie allfällige Anmeldepflichten für Datensammlungen oder Informationspflichten für die Weitergabe von Personendaten ins Ausland gegenüber den Datenschutzbehörden werden beachtet.
B **Öffentliche Register**	Für den Betrieb von ***Einwohner- und Stimmrechtsregistern*** (Ziff. 3) verantwortliche Behörden stellen sicher, dass • die Datenbearbeitung nicht über ***gesetzliche Regelung*** hinausgeht hinsichtlich Zweck, Inhalt, Umfang und Dauer; • die Weitergabe von personenbezogenen Daten nur soweit erfolgt, als eine ausdrückliche gesetzliche Grundlage vorliegt oder die Daten vorgängig pseudonymisiert worden sind; • den registrierten ***Sperrmöglichkeiten*** zugestanden werden, falls eine Weitergabe ihrer Daten zu Zwecken der politischen Werbung gesetzlich nicht zum vornherein ausgeschlossen ist; • die ***Risiken*** hinsichtlich der technischen und organisatorischen Sicherheit unter Einschluss von Re-Identifikationsgefahren ***abgeschätzt und dokumentiert*** sowie die nötigen Schutzmassnahmen getroffen werden (Ziff. 6); • den zuständigen Datenschutzbehörden Datenverluste innert nützlicher Frist gemeldet werden.
C **Datenhändler und Datenanalyse -Unternehmen**	Soweit private Datenhändler (Ziff. 5.1) oder Datenanalyse-Unternehmen (Ziff. 5.2) Daten im Kontext mit dem politischen Prozess als gesamtverantwortliche ***Inhaber*** bearbeiten, tragen sie den Hinweisen in Tabelle A Rechnung. Soweit sie als ***Auftragsbearbeiter*** tätig sind und Daten im Kontext mit dem politischen Prozess bearbeiten • vergewissern sie sich vor Vertragsabschluss, dass ihr Auftraggeber willens und technisch wie organisatorisch in der Lage ist, die zu vereinbarende Bearbeitung gesetztes- und vertragsgemäss vorzunehmen; • beachten sie die Rechtsprechung i.S. Moneyhouse (Ziff. 2) zur profilbildenden Kombination von Daten aus verschiedenen Quellen (Ziff. 4.2); • stellen sie die Datensicherheit sicher, indem sie die Risiken abschätzen und dokumentieren sowie die nötigen Schutzmassnahmen treffen (Ziff. 6); • unterstützen sie ihren Auftraggeber auf dessen Wunsch bei dessen Risikoerhebungen und melden ihm allfällige Datenverluste. Sie klären in ihren Nutzungsbedingungen oder schriftlichen Vertragsbedingungen darüber auf: • wie, aus welchen Quellen, mit welchen Methoden und zu welchen Zwecken sie die weitergegebenen Daten beschafft haben; • ob und falls ja, zu welchen Zwecken und in welcher Form die betroffenen Personen einer Weitergabe und Weiterbearbeitung der Daten zustimmen konnten.

D **Datenplattformen**	Unabhängig davon ob, Datenplattformen (Ziff. 5.3) Informationen im Kontext mit dem politischen Prozess als gesamtverantwortliche Inhaber oder im Auftragsverhältnis bearbeiten, richtet sich die Bearbeitung in aller Regeln nach **allgemeinen Geschäfts- und Nutzungsbedingungen**. • Sie beachten den Anspruch Stimmberechtigten auf eine ***transparente Datenbearbeitung*** (Ziff. 7) und investieren deshalb laufend in ***datenschutzfreundliche Technologie***, um den Anwendern mehrstufige ***Informationen*** *und* ***echte, benutzerfreundliche digitale Wahlmöglichkeiten*** zu bieten. • Sie benennen gegenüber den zuständigen Datenschutzbehörden hinreichend informierte und autorisierte ***Ansprechpersonen***, die im Fall von Datenverlusten oder anderen datenschutzrelevanten Störfällen mit möglichen Auswirkungen Abstimmungen und Wahlen für Auskünfte verfügbar sind. Soweit Datenplattformen Informationen als gesamtverantwortliche ***Inhaber*** bearbeiten, beachten sie zudem die Hinweise in Tabelle A. Soweit sie Daten im ***Auftragsverhältnis*** bearbeiten, beachten sie zusätzlich Tabelle D.
E **Einzelpersonen**	Bevor Einzelpersonen politische Inhalte und Äusserungen auf sozialen Netzwerken veröffentlichen, bewerten oder weiterverbreiten, achten sie als Adressat darauf, die Privatsphäre und anderen Aspekte der Persönlichkeitsrechte wie die Ehre oder das Familienleben der Betroffenen zu wahren. Bevor sie an Parteien, Interessengruppen, Datenhändler, Datenanalyseunternehmen oder Datenplattformen ***Informationen weitergeben***, die sich auf ihre Freunde, Familienmitglieder oder andere bestimmbare Personen beziehen, holen sie dafür ***vorgängig*** deren ***explizite Einwilligung*** ein. Sie vergewissern sich, dass Software auf diese Daten greift, die aus verlässlichen Quellen stammt.