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 15. Dezember 2022[1]

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

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

[1] Diese Aktualisierung ersetzt die Version vom 1. Juni 2019

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

Inhaltsverzeichnis

1 Worum geht es?

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.

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 Bürgerinnen und Bürger 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 - und dass die Verantwortlichen daher höhere Anforderungen für die zulässige Bearbeitung erfüllen muss.

2 Zuständige Aufsichtsbehörden und anwendbares Recht

Soweit 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 Bearbeitungen von Personendaten 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.

Auf Bundesebene treten am 1. September 2023 – also kurz vor den eidgenössischen Erneuerungswahlen - das totalrevidierte Datenschutzgesetz vom 25. September 2020 und die Vollzugsverordnungen zu diesem Erlass in Kraft. Nähere Informationen dazu können unserer Publikation «Das neue Datenschutzgesetz aus Sicht des EDÖB» entnommen werden. Auch diverse kantonale Datenschutzgesetze werden zurzeit revidiert (s. dazu auch die nachfolgende Ziff. 8.1).

3 Adressaten und Zweck des Leitfadens

Der Leitfaden richtet sich an alle politischen Parteien sowie an weitere Akteure der politischen Meinungsbildung.

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 soll den Adressaten eine Auslegungshilfe zum anwendbaren Datenschutzrecht von Bund und Kantonen bieten, um beurteilen zu können, welche Bearbeitungsmethoden im Kontext der politischen Willensbildung im digitalen Raum aus Sicht der Datenschutzbehörden datenschutzrechtlich zulässig sind; bzw. welche Voraussetzungen erfüllt werden müssen.

Der Leitfaden will die Akteure der politischen Meinungsbildung dazu anhalten, die digitalen Bearbeitungsmethoden für die wählende und stimmende Bevölkerung erkenn- und nachvollziehbar zu machen. Von diesem datenschutzrechtlichen Anspruch auf Transparenz abzugrenzen gilt es den in der öffentlichen Diskussion unter dem Schlagwort der sog. «Fake News» thematisierten Wahrheitsgehalt von Sachinhalten, der weder Gegenstand der Datenschutzgesetzgebung ist noch Thema dieses Leitfadens sein kann. Ebenso bleibt die Thematik des E-Votings hier ausgeklammert.

4 Akteure

4.1 Politische Parteien und Interessengruppen

Die Datenbearbeitungen 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.

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.

Politische Parteien und Interessengruppen werden als «Verantwortliche» oder «private Inhaber oder Inhaberin von Datensammlungen» somit ihrer Gesamtverantwortung etwa für die Beschaffung, Aufbewahrung, Pflege und Weiterverwendung der dort bearbeiteten Daten Rechnung tragen (vgl. Tabelle A).

4.2 Verantwortliche oder Auftragsbearbeitende

Bearbeitungen von Personendaten können gemäss der Datenschutzgesetzgebung in zwei verschiedenen Rollen stattfinden: als Verantwortliche oder Verantwortlicher (im aktuellen Bundesgesetz auch «Inhaber der Datensammlung») oder als Auftrags(daten)bearbeitende. Verantwortliche oder Verantwortlicher ist eine private Person oder ein Behördenorgan, die oder das alleine oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (s. Tabelle A). Auftragsbearbeiter ist eine private Person oder ein Behördenorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet (s. Tabelle C). Der Verantwortliche bzw. die Verantwortlichen bleiben für die Einhaltung der Datenschutzbestimmungen zuständig – oder eben verantwortlich – auch wenn die Personendatenbearbeitung einem Dritten (Auftragsbearbeitende) übertragen wird. Auch möglich ist eine gemeinsame Verantwortlichkeit mehrerer Datenbearbeiter.

Bsp: Wählerin A besucht die Webseite einer Partei und sieht sich das Parteiprogramm an, ohne der Partei beizutreten. Die Partei möchte über soziale Medien gezielt Wählerinnen und Wähler ansprechen, die die Webseite der Partei besucht haben, ohne der Partei beizutreten, d. h. Wählerinnen wie A.

Zu diesem Zweck hat die Partei ein so genanntes Tracking-Pixel auf ihrer Webseite eingefügt, das von den sozialen Medien ausgelesen wird. Ein Tracking-Pixel ist ein Plugin, das eine Webseite-Besitzerin oder ein Webseite-Besitzer in seine Webseite integrieren kann. Wenn eine Wählerin die Webseite besucht, stellt der Browser der Wählerin automatisch eine Verbindung zu den Servern der sozialen Medien her und sendet eine Reihe von Informationen über die Wählerin an die sozialen Medien. Auf diese Weise können die sozialen Medien in der Regel den Besuch von Einzelnen auf der Webseite überwachen. Dies geschieht z. B., um den Wählerinnen einer bestimmten Werbezielgruppe in den sozialen Medien hinzuzufügen. Daher sieht A, nachdem sie die Webseite der Partei verlassen und die sozialen Medien besucht hat, in den sozialen Medien Werbung für die Partei.

Die Partei und die sozialen Medien sind gemeinsame Verantwortliche.

Befindet sich die Auftragsbearbeiterin oder der Auftragsbearbeiter in einem aus datenschutzrechtlicher Sicht unsicherem Drittland, sind besondere Massnahmen zu treffen. Eine solche Konstellation liegt etwa vor, wenn Personendaten auf einem US- amerikanischem Server gespeichert werden. Weitere Informationen dazu sind auf der Webseite des EDÖB (Link: Übermittlung ins Ausland (admin.ch)) publiziert.

4.3 Öffentliche Register

Die Gemeinden 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.

Im Rahmen ihrer Gesamtverantwortung als Inhaberin 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 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 die Gesuchstellerin oder den Gesuchsteller herausgeben. Gemeindeeinwohnerinnen oder 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.

4.4 Datenanalyse-Unternehmen

Datenanalyse-Unternehmen können als Beauftragte oder Beauftragter 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. Webseite-Analyse, Crawler-Agenturen).

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

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

4.5 Datenhändler

Professionelle Adresshändlerinnen und Adresshändler sowie Anbieterinnen 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. Weitere 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 Inhaberinnen oder Inhaber (vgl. Hinweise in Tabelle A) oder als Auftragsbearbeitende (vgl. Tabelle C).

4.6 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 Drittanbieterinnen oder Drittanbieter ihre Leistungen und Daten Interessierten zur Verfügung.
Soweit private Datenplattformen personenbezogene Daten im Kontext mit dem politischen Prozess als gesamtverantwortliche Inhaberinnen oder Inhaber bearbeiten, sind die Hinweise in Tabelle A und Tabelle D zu beachten. Soweit sie solche Daten als Auftragsbearbeiterin oder als Auftragsbearbeiter bearbeiten oder weitergeben, gibt Tabelle C entsprechende Hinweise.

4.7 Einzelpersonen

Adressatin oder 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 Leserinnen oder 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 Nutzerinnen und Nutzern austauschen, akkumulieren nicht nur die Betreiberinnen oder Betreiber der Netzwerke, sondern auch deren Kundschaft grosse Mengen von Adress-, Text-, Ton- und Bilddaten, die sich auf deren Familien, Freundinnen und Freunde sowie Bekannte beziehen und Rückschlüsse auf Weltanschauung und politische Präferenzen zulassen. Solche Informationen werden mit den damit verbundenen Benutzerinnenkonten oder Benutzerkonten in den Rechenzentren der Plattform- Betreiberinnen und Betreiber und zum Teil auch auf den Smartphones und übrigen Rechner der Benutzerinnen oder 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 Inhaberinnen oder Inhaber von Datensammlungen tragen daher auch die einzelnen Adressatinnen und 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.

5 Personendaten im Kontext von Wahlen und Abstimmungen

5.1 Personendaten

Als Personendaten gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. 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 Beeinflussung der Stimmberechtigten durch sog. «Fake News» nicht Gegenstand des Datenschutzrechts ist. Soweit sich nachweislich unrichtige Sachinhalte nachteilig auf die Persönlichkeit und Ehre einzelner Personen auswirken, verweisen wir auf die einschlägigen Bestimmungen des Zivilrechts und des Strafgesetzbuches (so namentlich Art. 28 ZGB sowie 173 ff. und Art. 261bis StGB).

5.2 Besonders schützenswerte Personendaten und Persönlichkeitsprofile

Daten, die Rückschlüsse auf politische oder weltanschauliche Ansichten zulassen, gelten als besonders schützenswert, sodass das Gesetz an deren Bearbeitung besondere Anforderungen stellt. 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 wiederum durch das Gesetz besonders geschützt sind.

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[2] ebenfalls einen erhöhten Schutz der Betroffenen indizieren.

6 Bearbeitungsgrundsätze

Jede Akteurin und jeder Akteur, der im Kontext von Wahlen und Abstimmungen Personendaten bearbeitet, hat die allgemeinen Bearbeitungsgrundsätze der Datenschutzgesetzgebung zu beachten. Für öffentliche Organe gilt zudem das Legalitätsprinzip, wonach sich jede Bearbeitung von Personendaten auf eine genügende gesetzliche Grundlage stützen muss.

6.1 Treu und Glauben und Transparenz

Die Akteurinnen und Akteure müssen die Bearbeitung von Personendaten zunächst nach Treu und Glauben vornehmen. Dies bedeutet, dass sie die Daten nicht in einer Art erheben und bearbeiten dürfen, mit der die betroffenen Personen aus den Umständen heraus nicht rechnen mussten und mit der sie vermutlich nicht einverstanden gewesen wären.

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

Der Grundsatz der Transparenz verlangt, 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 der Datenbearbeiterin oder des Datenbearbeiters und – bei einer Weitergabe der Daten an Dritte – die Kategorien von möglichen Datenempfängern. Auch die Beschaffung von Personendaten bei Dritten wie beispielsweise Datenhändlerinnen oder Datenhändlern muss für die betroffenen Personen erkennbar sein. Nur so wird für die Stimmberechtigten nachvollziehbar, aufgrund welcher digitaler Bearbeitungsmethoden und Technologien sie angesprochen und politisch beeinflusst werden. Nur wenn die Parteien und Interessengruppen für die Stimmbürgerinnen und Stimmbürger genügend erkenn- und nachvollziehbar machen, welche Bearbeitungsmethoden sie zur Anwendung bringen, können sie sich auf deren Akzeptanz berufen.

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 und allfällige besondere Vorschriften über die Informationspflicht halten.

6.2 Verhältnismässigkeit

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 Rechte der betroffenen Personen gewahrt werden. Die Datenbearbeitung muss für die betroffenen Personen sowohl hinsichtlich ihres Zwecks als auch hinsichtlich ihrer Mittel zumutbar sein.

6.3 Zweckbindungsgrundsatz

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.

6.4 Korrektheit der Daten

Wer über eine Datensammlung verfügt, hat sich auch über die Richtigkeit der darin enthaltenen Daten, soweit diese eine Personenrelevanz aufweisen, zu vergewissern. Die Datenbearbeiterin oder 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.

6.5 Datensicherheit

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 die Inhaberin oder der Inhaber einer Datensammlung, sondern jede Datenbearbeiterin sowie 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 Persönlichkeitsverletzung und Rechtfertigungsgründe

7.1 Persönlichkeitsverletzung

Wer als private Verantwortliche oder privater Verantwortlicher Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Eine Persönlichkeitsverletzung liegt beispielsweise dann vor, wenn ein Bearbeitungsgrundsatz verletzt wird (vgl. Ziff. 6), Personendaten gegen den ausdrücklichen Willen bearbeitet werden oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgegeben werden.

> *Bsp.: Eine politische Partei versendet einen Newsletter an Personen, die diesen abonniert haben. Diese Datenbearbeitung verletzt die Persönlichkeit der betroffenen Personen nicht. Sobald sich eine Person vom Newsletter abmeldet, würde eine weitere Zustellung deren Persönlichkeit verletzen, da die damit verbundene Datenbearbeitung gegen den ausdrücklichen Willen erfolgen würde.*

> *Bsp.: Ein selbständig tätiger Anwalt kandidiert für ein politisches Amt und verschickt an seinen Klientenstamm Wahlwerbung. Es gibt keinen übereinstimmenden Zweck zwischen anwaltschaftlicher Beratung und Wahlwerbung in eigener Sache. Es gibt auch keine logische Verbindung zwischen den beiden Zwecken. Ausserdem entspricht die Zweckänderung der Bearbeitung nicht den berechtigten Erwartungen der Klienten. Der Anwalt darf die Kontaktdaten seiner Kunden deshalb nicht ohne vorgängige Einholung einer Einwilligung für die Bearbeitungen im politischen Kontext verwenden.*

Eine Persönlichkeitsverletzung ist nicht widerrechtlich, wenn sie durch die Einwilligung der Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch ein Gesetz gerechtfertigt ist. Nachfolgend wird nicht mehr auf die gesetzliche Grundlage als Rechtfertigungsgrund eingegangen (Beispiele dafür finden sich in Ziff. 4.3).

7.2 Überwiegende private oder öffentliche Interessen

Eine Persönlichkeitsverletzung kann mit überwiegenden privaten oder öffentlichen Interessen gerechtfertigt werden. Ob die privaten oder öffentlichen Interessen überwiegen, hängt von der Interessenabwägung im Einzelfall ab. So muss beurteilt werden, wie schwer die Persönlichkeitsverletzung oder die potenziellen Persönlichkeitsverletzungen tatsächlich wiegen und ob die hinter der Datenbearbeitung

stehenden privaten oder öffentlichen Interessen demgegenüber als so schwerwiegend einzustufen sind, dass es objektiv gerechtfertigt und für die Betroffenen zumutbar erscheint, dass der Persönlichkeitsschutz hinter diesen zurückzutreten hat.

Datenbearbeitungen im politischen Kontext können für sich ein legitimes privates oder gar öffentliches Interesse in Anspruch nehmen, und die politischen Rechte werden durch die Verfassung garantiert. Inwieweit dieses Interesse dem Persönlichkeitsschutz vorgeht und damit als überwiegend zu qualifizieren ist, hängt insbesondere davon ab, welche Daten dabei bearbeitet werden und auf welche Weise dies geschieht.

> *Bsp.: Eine politische Partei kauft bei einem Adresshändler einen Adressstamm ein, der ursprünglich zu Marketingzwecken erhoben wurde. Sie verwendet diese Adressen anschliessend für den Versand von Abstimmungsempfehlungen. Auch wenn hier eine Verletzung des Zweckbindungsprinzips anzunehmen ist, dürfte die damit einhergehende Persönlichkeitsverletzung als gering einzustufen sein, so dass sie regelmässig durch das überwiegende Interesse der Partei gerechtfertigt sein wird.*

7.3 Einwilligung

Liegt kein überwiegendes Interesse vor oder möchte sich ein Datenbearbeiter nicht dem Risiko aussetzen, dass ein solches in einem Rechtsstreit keinen Bestand hat, muss eine die Persönlichkeit der Betroffenen verletzende Datenbearbeitung durch die Einwilligung der Betroffenen gerechtfertigt werden. Einwilligungen müssen selbstbestimmt und informiert erfolgen.

Selbstbestimmt ist die Einwilligung, wenn die Betroffenen hinsichtlich der Aktivierung oder Deaktivierung 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, welche die Leserin oder den Leser auf die jeweils relevanten Passagen der einschlägigen Bearbeitungsreglemente und Datenschutzbestimmungen führen. Zur fairen Information gehört im politischen Kontext insbesondere, dass die Betroffenen nicht mit irreführenden oder falschen Angaben zu Absenderinnen und Absendern sowie 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“).

7.4 Ausdrückliche Einwilligung

Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die (selbstbestimmte und informierte) Einwilligung zudem ausdrücklich erfolgen. Für eine ausdrückliche Einwilligung ist eine aktive Zustimmungshandlung der Betroffenen notwendig. Eine ausdrückliche Einwilligung liegt namentlich dann vor, wenn sich die betroffenen Personen auf der Webseite einer Akterin oder 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 Akteurinnen und 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.

8 Der Prozess der Datenbearbeitung im politischen Kontext

Datenbearbeitungen durch private Verantwortliche sind nach Schweizer Recht ohne weiteres zulässig, sofern dabei die Persönlichkeit der Betroffenen nicht verletzt wird. Kommt es zu Verletzungen, muss für diese ein Rechtfertigungsgrund bestehen (vgl. zum Ganzen Ziff. 7). Die Rechtmässigkeit muss dabei über den gesamten Prozess der Datenbearbeitung gegeben sein. Zur Veranschaulichung, was dies im politischen Kontext bedeutet, lässt sich dieser Prozess funktional in die Beschaffung, Analyse, die Zuweisung von Informationen sowie die Ansprache der Betroffenen aufteilen.

8.1 Beschaffung von Personendaten

Werden Personendaten direkt bei der betroffenen Person selbst beschafft, kann der Beschaffungsprozess so ausgestalten werden, dass dabei die Persönlichkeitsrechte der Betroffenen gewahrt werden (vgl. dazu auch die Ausführungen unter Ziff. 7 vorstehend). In diesem Zusammenhang zentral ist die Einhaltung der Transparenz und der Zweckbindung sowie die Informationspflicht bei der Beschaffung besonders schützenswerter Personendaten und der Erstellung von Persönlichkeitsprofilen. Demzufolge müssen die Betroffenen insbesondere darüber informiert werden, welche Daten zu welchen Zwecken und auf welche Art und Weise bearbeitet werden. Nach Inkrafttreten des neuen Datenschutzgesetzes im September 2023 wird die Informationspflicht auch für die Beschaffung nicht besonders schützenswerter Personendaten gelten (vgl. hierzu die Publikation «Das neue Datenschutzgesetz aus Sicht des EDÖB»).

Werden darüber hinaus auch die übrigen Bearbeitungsgrundsätze eingehalten und sollen weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile Dritten bekannt gegeben werden, wird die Persönlichkeit der Betroffenen nicht verletzt, so dass für die Datenbearbeitung kein Rechtfertigungsgrund bestehen muss.

Bsp.: Eine Partei ergänzt die im Rahmen des Newsletterversandes erhobenen Datenbestände durch Informationen, welche durch Unterschriftensammlungen oder mittels persönlicher Ansprache der Bevölkerung an Ständen, bei Hausbesuchen oder über Telefonate erlangt werden. Zusätzlich werden Daten aus öffentlich zugänglichen Quellen wie Telefonverzeichnissen oder öffentlichen Registern beschafft. Die Partei beschafft die Daten grösstenteils bei den betroffenen Personen selbst. Sie soll diese somit bei der Beschaffung darüber informieren, dass sie die Daten für eine persönliche Ansprache nutzen und gegeben falls mit weiteren öffentlich zugänglichen Daten ergänzen wird.

Bei Unsicherheit darüber, ob mit der Datenbearbeitung Persönlichkeitsrechte verletzt werden, empfiehlt es sich, eine Einwilligung der Betroffenen einzuholen, zumal dies in derartigen Konstellationen ohne grossen Aufwand möglich ist.

Sobald die Personendaten bei Dritten beschafft werden, können die Persönlichkeitsrechte der Betroffenen ungleich schwieriger gewahrt werden. Gerade bei der Bearbeitung von Daten über einer Grosszahl von Betroffenen dürfte beispielsweise die Einhaltung des Transparenzgrundsatzes nur unzureichend möglich oder mit grossem Aufwand verbunden sein. Dementsprechend sollte in solchen Konstellationen oder falls geplant ist, besonders schützenswerte Personendaten oder Persönlichkeitsprofile an Dritte bekannt zu geben, ein Rechtfertigungsgrund gegeben sein.

Bsp.: Eine politische Interessengruppe beschafft Personendaten mit Hilfe von Web-Mining aus Webseiten und Internetportalen, beauftragt Dritte damit oder erwirbt die entsprechenden Informationen käuflich. Dazu kommen Web-Crawler-Dienste zum Einsatz, welche Inhalte von Webseiten oder E-Mail-Adressen systematisch durchsuchen und die gewünschten Informationen beschaffen. Die Einhaltung des Transparenzgrundsatzes oder gar eine aktive Information der Betroffenen dürften hier faktisch nicht möglich sein. Auch das Zweckbindungsprinzip könnte auf diese Weise verletzt werden. Dementsprechend muss für derartige Datenbearbeitungen ein überwiegendes Interesse gegeben sein. Beruhen die Beschaffungen auf krassen Rechtsverletzungen, wie z.B. bei Crawler-Diensten, die sich über die Nutzungsbedingungen sozialer Netzwerke hinwegsetzen, stösst die Berufung auf überwiegende Interessen indessen an ihre Grenze.

An die Grenze des noch Rechtfertigbaren stossen kann auch die Bewirtschaftung der zusammengetragenen Daten mit Hilfe einer Kampagnen-Software. 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, kann die Interessengruppe 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). Diese Datenbearbeitung greift unter Umständen stark in die Persönlichkeitsrechte der Betroffenen ein, so dass eine Rechtfertigung durch ein überwiegendes Interesse oft nicht mehr möglich ist. In diesem Fall muss die Einwilligung der Betroffenen eingeholt werden.

8.2 Analyse

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. 5) ausführlich zu dieser Thematik geäussert. Der qualifizierte Schutz gilt auch für die Bearbeitung von sensiblen Daten wie weltanschaulichen oder politischen Ansichten, welche der Gesetzgeber einem besonderen Schutz unterstellt hat (Ziff. 5.2).

Soweit ersichtlich bestehen keine gesetzlichen Grundlagen, welche einem öffentlichen Organ personenbezogene politische Analysen erlauben würden.

8.3 Zuweisung von Informationen

Unter der Annahme, dass die Personen einer gemeinsamen Profilgruppe auf bestimmte Botschaften besonders stark reagieren, wird beabsichtigt, den einzelnen Gruppen gezielt Informationen über E-Mail-Verteiler oder auf sozialen Medien zu vermitteln. 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.

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 politische Freundin/Freund oder Gegnerin/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 Gegnerinnen und Gegner – zu versenden.

8.4 Ansprache der Betroffenen

Oft ist die Zustellung einer politischen Mitteilung die erste Gelegenheit, bei der die Betroffenen Kenntnis über die erfolgten Datenbearbeitungen erlangen (vgl. Ziff. 8.1 – 8.3). Dies insbesondere dann, wenn die Bearbeitung auf einem überwiegenden Interesse beruht. Deswegen ist mit der Zustellung der politischen Botschaft die Information an die Betroffenen nachzuholen. Diesen ist mitzuteilen, wer für die erhaltene Mitteilung verantwortlich ist, wo weiterführende Informationen zu den damit verbundenen Datenbearbeitungen erhältlich sind und wie die Betroffenenrechte geltend gemacht werden können. Die Betroffenen sollen möglichst verständlich über die erfolgten Datenbearbeitungen (vgl. Ziff. 8.1 – 8.3) informiert werden, damit der Kontext der politischen Botschaft verstanden wird und richtig eingeordnet werden kann. Zudem muss eine rasche und einfache Widerspruchsmöglichkeit angeboten werden.

8.5 Einholung einer gültigen Einwilligung

Für die Voraussetzungen einer gültigen Einwilligung siehe die Ausführungen in Ziffer 7.3 und 7.4 hiervor.

8.6 Betroffenenrechte

Die Verantwortlichen sind verpflichtet, die datenschutzrechtlichen Betroffenenrechte einfach sicherzustellen. So hat jede betroffene Person das Recht, bei der Inhaberin oder dem Inhaber einer Datensammlung Auskunft zu den über sie bearbeiteten Daten zu verlangen, falsche Personendaten zu berichtigen und Daten löschen zu lassen.

Daher müssen alle Betroffenen in geeigneter Weise ihr Auskunfts-, Berichtigungs- und Löschrecht wahrnehmen können. Dies beginnt damit, dass sie über ihre Rechte informiert werden sowie darüber, wie und wo sie diese geltend machen können. Dafür bietet sich die Webseite des Verantwortlichen und die Ansprache der Betroffenen an. Erfolgen Datenbearbeitungen als gemeinsame Verantwortliche oder werden Dritte als Auftragsbearbeiterinnen oder Auftragsbearbeiter herangezogen, muss für die Betroffenen einfach erkennbar sein, bei welcher Akteurin oder welchem Akteur die Betroffenenrechte geltend gemacht werden können.

Das Ausüben der Rechte muss für die Betroffenen einfach und in der Regel kostenlos möglich sein.

9 Anforderungen an Webseite

Sofern eine Webseite betrieben wird und Personendaten bearbeitet werden, sind aus datenschutzrechtlicher Sicht die Bearbeitungsgrundsätze einzuhalten; öffentliche Organe sind zudem an das Legalitätsprinzip gebunden. Die nachfolgenden Kontrollfragen sollen dabei helfen, die Bearbeitungsgrundsätze in Bezug auf die Webseite einzuhalten:

- Werden Webseiten Besucherinnen und Besucher unübersehbar, einfach zugänglich und in verständlicher Sprache über die verschiedenen eingesetzten Instrumente und den Beschaffungszweck informiert (vgl. Ziff. 6.1)?

- Gibt es für Personen mit weitergehendem Informationsbedürfnis eine mehrstufige Information, d.h. gibt es zusätzlich zu einfach verständlichen, knappen Erklärungen auch technisch detailliertere?

- Können Besucherinnen und Besucher einzeln («granular») wählen, ob bzw. welche der eingesetzten Instrumente des Webtracking sie zulassen wollen?

- Werden bei der Einbindung von Facebook Social Plugins oder ähnlichen Diensten Technologien eingesetzt, welche gewährleisten, dass das Tracking bzw. die Datenübermittlung erst nach einer allfälligen Einwilligung erfolgt (vgl. Ziff. 7.3 und 7.4)?

- Werden Betroffene über ihre Rechte informiert, insbes. über ihr Auskunftsrecht? Wurden die nötigen technologischen und organisatorischen Vorkehrungen getroffen, um Auskunftsbegehren beantworten zu können (vgl. Ziff. 8.6)?

- Werden beim vorgenommenen Tracking nur Daten gesammelt, die für die beabsichtigte Nutzung notwendig sind (vgl. Ziff. 6.1 und 6.3)?

- Wurden für Webtracking und Webanalyse Lösungen gewählt, welche eine Verwendung durch Dritte zu deren Zwecken ausschliessen, z.B. durch Einsatz von Analyse-Tools, welche beim Dateninhaber oder Dateninhaberin selbst installiert sind oder die IP-Adresse kürzen (vgl. Ziff. 6.3)?

- Soweit Dritte beauftragt werden: Werden die Betroffenen darüber informiert? Werden die beauftragten Dritten angehalten nachzuweisen, dass sie organisatorische und technische Massnahmen zur Datensicherheit ergriffen haben und werden diese kontrolliert (vgl. Ziff. 4.2 und 6.5)?

- Wird ein allfälliger Datentransfer (z.B. Kontaktformular) verschlüsselt?

- Werden die betroffenen Personen über eine allfällige Weiterverwendung ihrer E-Mail-Adressen wie z.B. für «Social Matching» vorab informiert und wird dafür eine separate Einwilligung eingeholt (vgl. Ziff. 6.1; 7.3 und 7.4)?

10 Praxisbeispiele

Beispiel 1

Eine politische Partei wirbt als Verein an Veranstaltungen und auf ihrer Webseite um Mitglieder. Dort bietet sie den Besuchenden die Möglichkeit, sich gegen Angabe ihrer E-Mail-Adresse für den Newsletter zu abonnieren. Der Verein beabsichtigt, alle so erhaltenen E-Mail-Adressen den Betreibern eines sozialen Mediums zur Verfügung zu stellen und so die Targeting- und Verstärkungstechniken dieses Mediums zu nutzen, um seine politische Werbung gezielt an Personen mit ähnlichem Persönlichkeitsprofil zu adressieren.

Es gibt keine offensichtliche logische Verbindung zwischen dem Zweck, den Besuchenden aktuelle Informationen der Partei mit generellen Inhalten zuzustellen, und dem zusätzlichen Zweck, gezielt, auf Persönlichkeitsprofile mit weltanschaulichen Aspekten ausgerichtete politische Botschaften zu versenden. Deshalb entspricht der zusätzliche Zweck auch nicht den berechtigten Erwartungen der Empfänger und Empfängerinnen des Newsletters. Der Verein kann keine hinreichenden überwiegenden privaten und öffentlichen Interessen geltend machen, welche die Persönlichkeitsverletzung rechtfertigen könnte.

Der Verein darf die E-Mailadressen somit nicht ohne vorherige Information und Einholen einer ausdrücklichen Einwilligung den Empfängerinnen und Empfängern des Newsletters für den zusätzlichen Zweck der gezielten und personalisierten politischen Werbung verwenden.

Beispiel 2

Eine für eine politische Partei tätige Werbeagentur bietet über soziale Medien einen Berufseignungstest an, der eine psychologische Bewertung umfasst.

Durch das Ausfüllen des Tests fallen bei den Betreiberinnen der sozialen Medien Informationen über die Ausbildung, die berufliche Tätigkeit, den Beschäftigungsstatus, das Alter, Hobbys, sowie die E-Mail-Adresse und Kontakte der Testpersonen an. Die Agentur kauft diese Informationen den Betreiberinnen

der sozialen Medien ab, um die politische Werbung ihrer Auftraggeberin möglichst adressatengerecht zustellen zu können.

Der Einsatz solcher Targeting-Techniken verstösst gegen die Bearbeitungsgrundsätze der Zweckbindung und Bearbeitung nach Treu und Glauben. Weil keine überwiegenden privaten oder öffentlichen Interessen geltend gemacht werden können, müssen die betroffenen Personen als potentielle Wählerinnen und Wähler vor der Beschaffung der erbetenen Informationen darüber informiert werden, dass diese auch zum Zwecke des gezielten politischen Marketings verarbeitet werden und in diese zusätzliche Bearbeitung ausdrücklich einwilligen.

11 Zusammenfassende Übersicht

A **Parteien und Interessen-gruppen**	Soweit Parteien und Interessengruppen eine Gesamtverantwortung i.S. einer Inhaberin oder eines Inhabers einer ***Datensammlung*** (Verantwortliche oder Verantwortlicher) wahrnehmen (Ziff. 4.1 und 4.2), 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*** **als gemeinsame Verantwortliche** werden angehalten nachzuweisen, dass sie sämtliche datenschutzrechtliche Vorgaben einhalten (Ziff. 6) • ***Beauftragte Dritte*** als Auftragsbearbeitende werden vertraglich verpflichtet, sämtliche datenschutzrechtliche Vorgaben einzuhalten, insbesondere nachzuweisen, dass sie angemessene organisatorische und technische Massnahmen zur Datensicherheit (Ziff. 6.5) ergreifen und die Personendaten nur für die vertraglich vereinbarten Zwecke bearbeiten. • Der Anspruch der Stimmberechtigten auf ***Transparenz*** (Ziff. 6.1 und 9) wird erfüllt durch ***Webseite gestützte Informationen*** über - die Identität der verantwortlichen Inhaberinnen oder Inhaber der Sammlung; - die Kategorien der bearbeiteten Daten; - die Datenbeschaffung mit Hinweis auf Drittquellen; - den aktuellen Zweck und, falls notwendig den, 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. 6.3) und der ***Verhältnismässigkeit*** (Ziff. 6.2), 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. 7.4); • Die ***Datenrichtigkeit*** ist auch bei Einschaltung Dritter gewährleistet und nicht mehr benötigte Daten sind gelöscht (Ziff. 6.4); • 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 die Informationen auf der Webseite des EDÖB (Link: Übermittlung ins Ausland (admin.ch) und mindestens folgende Dokumente: - Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG (Link: PDF Stellungnahme) - Anleitung für die Prüfung von Datenübermittlungen mit Auslandbezug (Link: PDF Anleitung) • 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. 4.3) 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 genügende gesetzliche Grundlage vorliegt oder die Daten vorgängig wirksam 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. 6.5); • den zuständigen Datenschutzbehörden Datenverluste innert umgehend gemeldet werden.
C **Datenhändler und Datenanalyse -Unternehmen**	Soweit private Datenanalyse-Unternehmen (Ziff. 4.4) oder Datenhändler (Ziff. 4.5) Daten im Kontext mit dem politischen Prozess als gesamtverantwortliche ***Inhaberinnen oder Inhaber*** bearbeiten, tragen sie den Hinweisen in Tabelle A Rechnung. Soweit sie als ***Auftragsbearbeiterin oder Auftragsbearbeiter*** tätig sind und Daten im Kontext mit dem politischen Prozess bearbeiten: • halten sie die vertraglich vereinbarten Pflichten des oder der Verantwortlichen ein • vergewissern sie sich vor Vertragsabschluss, dass ihre Auftraggeberin oder ihr Auftraggeber willens und technisch wie organisatorisch in der Lage ist, die erhaltenen Daten gesetztes- und vertragsgemäss weiterzubearbeiten; • beachten sie die Rechtsprechung i.S. Moneyhouse zur profilbildenden Kombination von Daten aus verschiedenen Quellen (Ziff. 5); • stellen sie die Datensicherheit gemäss den vertraglich vereinbarten Pflichten sicher (Ziff. 6.5); • 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 private Datenplattformen (Ziff. 4.6) Informationen im Kontext mit dem politischen Prozess als gesamtverantwortliche Inhaberinnen, Inhaber oder im Auftragsverhältnis bearbeiten, richtet sich die Bearbeitung in aller Regeln nach **allgemeinen Geschäfts- und Nutzungsbedingungen**. • Sie beachten den Anspruch der Stimmberechtigten auf eine ***transparente Datenbearbeitung*** (Ziff. 6.1 und 8.4) und investieren deshalb laufend in ***datenschutzfreundliche Technologien***, 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 ***Inhaberin oder gesamtverantwortlichen Inhaber*** bearbeiten, beachten sie zudem die Hinweise in Tabelle A. Soweit sie Daten im ***Auftragsverhältnis*** bearbeiten, beachten sie die Hinweise in Tabelle C.
E **Einzelpersonen**	Bevor Einzelpersonen politische Inhalte und Äusserungen auf sozialen Netzwerken veröffentlichen, bewerten oder weiterverbreiten, achten sie als Adressatin oder Adressat darauf, die Privatsphäre und andere 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 Freundinnen und Freunde, Familienmitglieder oder andere bestimmbare Personen beziehen, holen sie dafür ***vorgängig*** deren ***ausdrückliche Einwilligung*** ein. Sie vergewissern sich, dass Software auf diese Daten greift, die aus verlässlichen Quellen stammt.