EUROPÄISCHE
KOMMISSION

Brüssel, den 12.9.2018
COM(2018) 638 final

Freie und faire Wahlen

LEITFADEN

Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen

Ein Beitrag der Europäischen Kommission zum Treffen der Führungsspitzen in Salzburg am 19./20. September 2018

LEITFADEN DER KOMMISSION ZUR ANWENDUNG DES EU-DATENSCHUTZRECHTS IM ZUSAMMENHANG MIT WAHLEN

Die Kommunikation mit der Wählerschaft ist die Grundlage jedes demokratischen Prozesses. Für politische Parteien ist es gängige Praxis, ihre Kommunikation auf die spezifischen Interessen der Wähler zuzuschneiden. Es ist daher nur logisch, dass an Wahlen beteiligte Akteure ausloten, inwieweit sie zugängliche Daten nutzbar machen können, um neue Stimmen zu gewinnen. Der Durchbruch der digitalen Tools und Online-Plattformen hat viele neue Möglichkeiten eröffnet, politische Debatten mit den Bürgerinnen und Bürgern zu führen.

Wie der Fall Cambridge Analytica unlängst gezeigt hat, ist es jedoch etwas ganz anderes, wenn auf der Grundlage der unrechtmäßigen Verarbeitung personenbezogener Daten Mikrotargeting-Techniken für Wahlzwecke entwickelt werden. Der Fall macht deutlich, welche Herausforderungen mit modernen Technologien verbunden sind, und zeigt auch, dass der Datenschutz im Wahlkontext von besonderer Bedeutung ist. Mikrotargeting-Techniken sind zu einem ernstzunehmenden Anliegen geworden, nicht nur für den Einzelnen, sondern auch für das Funktionieren unserer Demokratien, da sie eine ernsthafte Bedrohung für ein faires, demokratisches Wahlverfahren darstellen und das Potenzial haben, die Führung offener Debatten, Fairness und Transparenz zu untergraben, die in einer Demokratie unerlässlich sind. Die Kommission ist der Auffassung, dass dieses Anliegen dringend angegangen werden muss, um das Vertrauen der Öffentlichkeit in die Fairness der Wahlverfahren wiederherzustellen.

Die ersten Berichte der britischen Datenschutzbehörde (Information Commissioner's Office) über die Verwendung von Datenanalysen in politischen Kampagnen[1] und die Stellungnahme des Europäischen Datenschutzbeauftragten zu Online-Manipulation und personenbezogenen Daten[2] haben bestätigt, dass das ursprünglich für kommerzielle Zwecke entwickelte Mikrotargeting zunehmend auch das Wahlverhalten beeinflusst.

In Bezug auf die allgemeinere Frage des Datenschutzes im Zusammenhang mit Wahlen sind mehrere Datenschutzbehörden tätig geworden[3].

Seit dem 25. Mai 2018 gilt die Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung)[4] unmittelbar in der gesamten Europäischen

[1] Berichte der britischen Datenschutzbehörde (Information Commissioner's Office) vom 10. Juli 2018: „Investigation into the use of data analytics in political campaigns – Investigation update" (Untersuchung der Verwendung von Datenanalysen in politischen Kampagnen – neueste Ergebnisse) und „Democracy Disrupted? Personal information and political influence" (Das Ende der Demokratie? Personenbezogene Daten und politische Einflussnahme).

[2] Nur auf Englisch verfügbar: Https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 „Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" veröffentlicht im Amtsblatt Nr. 71 der italienischen Datenschutzbehörde vom 26.3.2014 [doc. web n. 3013267];
https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux "Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?" veröffentlicht von der Commission Nationale de l'informatique et des libertés (französische Datenschutzbehörde) am 8.11.2016;
https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf „Guidance on political campaigning" der britischen Datenschutzbehörde Information Commissioner's Office [20170426].

Union. Sie stellt der Union die Instrumente bereit, die für den Umgang mit Fällen von widerrechtlicher Nutzung personenbezogener Daten im Wahlkontext erforderlich sind. Um die Integrität der demokratischen Ordnung aber tatsächlich schützen zu können, bedarf es der konsequenten und einheitlichen Anwendung dieser Vorschriften. Da die Verordnung anlässlich der bevorstehenden Wahl zum Europäischen Parlament zum ersten Mal auf europäischer Ebene zur Anwendung kommen wird, ist es wichtig, für sämtliche an der Wahl beteiligten Akteure – d. h. für nationale Wahlbehörden, politische Parteien, Informationsbroker und Datenanalysten, Social-Media-Plattformen und Online-Werbenetzwerke – einen klaren Rahmen vorzugeben. Ziel dieses Leitfadens ist es daher, die für Wahlen relevanten Datenschutzverpflichtungen hervorzuheben. Die nationalen Datenschutzbehörden, deren Aufgabe die Durchsetzung der Datenschutz-Grundverordnung ist, müssen ihre erweiterten Befugnisse in vollem Maße nutzen, um mögliche Verstöße, insbesondere beim Mikrotargeting von Wählerinnen und Wählern, zu ahnden.

1. Der Datenschutzrahmen der Europäischen Union

Der Schutz personenbezogener Daten ist ein Grundrecht, das in der Charta der Grundrechte der Europäischen Union (Artikel 8) und in den Verträgen (Artikel 16 AEUV) verankert ist. Die Datenschutz-Grundverordnung baut darauf auf und bietet einen starken Datenschutzrahmen, der der Union bei Fällen von Missbrauch personenbezogener Daten künftig eine bessere Handhabe bietet und alle Akteure in Bezug auf die Verarbeitung personenbezogener Daten stärker in die Verantwortung nimmt.

Die Verordnung garantiert den Bürgerinnen und Bürgern in der Union zusätzliche und stärkere Rechte, die in Bezug auf Wahlen besonders wichtig sind. Die in den letzten 20 Jahren in der Union geltende Datenschutzregelung litt insbesondere unter der uneinheitlichen Anwendung der Vorschriften in den Mitgliedstaaten, dem Fehlen jeglicher formeller Mechanismen für die Zusammenarbeit zwischen den nationalen Datenschutzbehörden und deren eingeschränkten Durchsetzungsbefugnissen. Mit der Datenschutz-Grundverordnung wurden diese Mängel behoben: Ausgehend von den bewährten Datenschutzgrundsätzen wurden Schlüsselbegriffe – wie der Begriff der Einwilligung – vereinheitlicht, das Recht der Bürgerinnen und Bürger, über die Verarbeitung ihrer Daten informiert zu werden, gestärkt, die Bedingungen festgelegt, unter denen personenbezogene Daten übermittelt werden dürfen, Vorschriften für Fälle von Datenschutzverletzungen eingeführt, ein Mechanismus für die Zusammenarbeit zwischen den Datenschutzbehörden in grenzüberschreitenden Fällen geschaffen und die Durchsetzungsbefugnisse der Datenschutzbehörden ausgebaut. Bei Verstößen gegen die EU-Datenschutzvorschriften sind die Datenschutzbehörden befugt, diese Fälle zu untersuchen (z. B. durch Anforderung von Auskünften, Durchführung von Vor-Ort-Prüfungen in den Geschäftsräumen der Verantwortlichen und Auftragsverarbeitern) und eine Änderung der Vorgehensweisen zu verlangen (z. B. durch das Aussprechen von Verwarnungen und Verweisen oder die Anordnung einer befristeten oder endgültigen

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Aussetzung der Verarbeitung). Sie sind ferner befugt, Geldbußen in Höhe von bis zu 20 Mio. EUR oder – im Falle von Unternehmen – von bis zu 4 % des weltweiten Umsatzes zu verhängen[5]. Bei der Entscheidung über die Verhängung von Geldbußen und deren Betrag haben die Datenschutzbehörden die Umstände des Einzelfalls und Faktoren wie Art, Umfang oder Zweck der Verarbeitung, Zahl der betroffenen Personen und Ausmaß des von ihnen erlittenen Schadens zu berücksichtigen[6]. Im Wahlkontext ist es wahrscheinlich, dass die Verstöße beträchtlich und die betroffenen Personen sehr zahlreich sind. Daher könnten insbesondere angesichts der Bedeutung des Vertrauens der Bürger in die demokratischen Prozesse sehr hohe Geldbußen verhängt werden.

Der neu eingerichtete Europäische Datenschutzausschuss, in dem alle nationalen Datenschutzbehörden sowie der Europäische Datenschutzbeauftragte vertreten sind, spielt eine Schlüsselrolle bei der Anwendung der Datenschutz-Grundverordnung, indem er Leitlinien, Empfehlungen und Dokumente zu bewährten Verfahren veröffentlicht[7]. Als mit der Durchsetzung der Datenschutz-Grundverordnung betraute Instanzen und direkte Ansprechpartner für alle Beteiligten obliegt es den nationalen Datenschutzbehörden, zusätzliche Rechtssicherheit bezüglich der Auslegung der Verordnung zu schaffen. Die Kommission unterstützt diese Arbeit nach Kräften.

Die Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[8]) ergänzt den Datenschutzrahmen der Union und ist im Zusammenhang mit Wahlen von Bedeutung, da sie Bestimmungen über die elektronische Übermittlung unerbetener Nachrichten, auch zum Zwecke der Direktwerbung, enthält. Die Datenschutzrichtlinie für elektronische Kommunikation enthält auch Vorschriften über die Speicherung von Informationen auf Endgeräten wie Smartphones oder Computern und über den Zugang zu bereits gespeicherten Informationen, z. B. Cookies, mit denen das Online-Verhalten eines Nutzers verfolgt werden kann. Der Vorschlag der Kommission für eine Verordnung über Privatsphäre und elektronische Kommunikation[9], über den derzeit verhandelt wird, beruht auf denselben Grundsätzen wie die Datenschutzrichtlinie für elektronische Kommunikation. Mit der neuen Verordnung soll der Anwendungsbereich über die herkömmlichen Telekommunikationsbetreiber hinaus auf internetgestützte elektronische Kommunikationsdienste ausgeweitet werden.

[5] Leitfaden der Kommission zur Datenschutz-Grundverordnung: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de.
[6] Artikel 83 der Datenschutz-Grundverordnung.
[7] Der Europäische Datenschutzbeauftragte gibt ebenfalls Stellungnahmen ab.
[8] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).
[9] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017) 10 final).

2. Wichtigste Pflichten der einzelnen Akteure

Die Datenschutz-Grundverordnung betrifft alle Akteure, die im Zusammenhang mit Wahlen aktiv sind, wie europäische und nationale politische Parteien (im Folgenden: „politische Parteien“), europäische und nationale politische Stiftungen (im Folgenden: „Stiftungen“), Plattformen, Anbieter von Datenanalysen und die für Wahlverfahren zuständigen Behörden. Diese dürfen personenbezogene Daten (z. B. Namen und Adressen) nur auf rechtmäßige Weise, nach Treu und Glauben und in nachvollziehbarer Weise für ganz bestimmte Zwecke verarbeiten. Sie können diese Daten nicht in einer Weise weiterverwenden, die mit den Zwecken, für die die Daten ursprünglich erhoben wurden, nicht vereinbar ist. Die Verarbeitung zu journalistischen Zwecken fällt prinzipiell ebenfalls in den Anwendungsbereich der Datenschutz-Grundverordnung, für sie können jedoch aufgrund der Bedeutung der Freiheit der Meinungsäußerung und der Informationsfreiheit in einer demokratischen Gesellschaft gemäß den nationalen Rechtsvorschriften Abweichungen oder Ausnahmen vorgesehen werden[10].

Der Begriff der personenbezogenen Daten ist umfassend auszulegen. Personenbezogene Daten sind alle Informationen, die eine bestimmte oder bestimmbare natürliche Person betreffen. Daten, die im Rahmen einer Wahl verarbeitet werden, umfassen häufig besondere Kategorien personenbezogener Daten („sensible Daten“), wie politische Meinungen, Gewerkschaftszugehörigkeit, ethnische Herkunft, Sexualleben usw., für die strengere Schutzvorschriften gelten[11]. Darüber hinaus können Datenanalysen aus Datensätzen mit nichtsensiblen Daten „sensible Daten“ (z. B. politische Meinungen, aber auch religiöse Überzeugungen oder die sexuelle Ausrichtung) ableiten. Die Verarbeitung dieser abgeleiteten Daten fällt ebenfalls in den Anwendungsbereich der Datenschutz-Grundverordnung und sollte daher im Einklang mit allen Datenschutzbestimmungen erfolgen.

Zusammenfassend ist festzustellen, dass praktisch alle wahlbezogenen Datenverarbeitungsvorgänge unter die Datenschutz-Grundverordnung fallen.

Um den an den Wahlen beteiligten Akteuren ein klares Bild zu verschaffen, werden in den folgenden Abschnitten unter Berücksichtigung der ersten Erkenntnisse aus dem Fall „Cambridge Analytica“ die Datenschutzverpflichtungen hervorgehoben, die im Zusammenhang mit Wahlen von besonderer Bedeutung sind. Sie sind im Anhang zusammengefasst.

2.1 Verantwortliche und Auftragsverarbeiter

Der Begriff der Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen sowie der gemeinsam für die Datenverarbeitung Verantwortlichen ist eine zentrale Komponente der Datenschutz-Grundverordnung. Für die Datenverarbeitung verantwortlich ist die Organisation, die allein oder in Zusammenarbeit mit anderen entscheidet, warum und wie die personenbezogenen Daten verarbeitet werden. Auftragsverarbeiter verarbeiten

[10] Artikel 85 Absatz 2 der Datenschutz-Grundverordnung.
[11] Article 9(1) General Data Protection Regulation.

personenbezogene Daten nur im Auftrag und auf Anweisung des Verantwortlichen (wobei ihr Arbeitsverhältnis in einem Vertrag oder einem anderen verbindlichen Rechtsakt festgelegt ist). Die Verantwortlichen müssen von Anfang an den Risiken angemessene Maßnahmen treffen, den Datenschutz durch geeignete Technikgestaltung umsetzen und nachweisen können, dass sie die Bestimmungen der Datenschutz-Grundverordnung (Grundsatz der Rechenschaftspflicht) einhalten.

Ob die Rolle des Verantwortlichen oder die des Auftragsverarbeiters vorliegt, muss in jedem Einzelfall geprüft werden. Bei Wahlen können eine Reihe von Akteuren für die Datenerarbeitung verantwortlich sein: In den meisten Fällen sind politische Parteien, einzelne Kandidaten und Stiftungen für die Datenverarbeitung verantwortlich. Je nachdem, in welchem Umfang sie für die jeweilige Datenverarbeitung verantwortlich sind, können auch Plattformen und Anbieter von Datenanalysen (gemeinsam) Verantwortliche oder Auftragsverarbeiter sein.[12] In Bezug auf die Wählerverzeichnisse gelten die nationalen Wahlbehörden als verantwortlich.

Wenn sich die Verarbeitungstätigkeiten von Unternehmen mit Sitz außerhalb der Union auf das Anbieten von Waren und Dienstleistungen für natürliche Personen in der Union oder die Überwachung ihres Verhaltens in der Union beziehen, müssen auch diese Unternehmen die Datenschutz-Grundverordnung einhalten. Dies trifft auf eine Reihe von Plattformen und Anbieter von Datenanalysen zu.

2.2 Grundsätze, Rechtmäßigkeit der Verarbeitung und besondere Auflagen für „sensible Daten“

An den Wahlen beteiligte Akteure können personenbezogene Daten, auch aus öffentlichen Quellen, nur im Einklang mit den für die Verarbeitung personenbezogener Daten geltenden Grundsätzen und in den in der Datenschutz-Grundverordnung eindeutig festgelegten begrenzten begründeten Fällen verarbeiten.[13] Die wichtigsten Gründe für eine rechtmäßige Datenverarbeitung bei Wahlen sind die Einwilligung einer Person, die Erfüllung einer rechtlichen Verpflichtung nach Unions- oder nationalem Recht, die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, und das berechtigte Interesse eines der Akteure. Wahlakteure können sich jedoch nur dann auf ein berechtigtes Interesse berufen, wenn die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Personen nicht überwiegen.

Darüber hinaus muss die Speicherung von Informationen oder der Zugang zu bereits gespeicherten Informationen auf dem Endgerät (Computer, Smartphone usw.) im Einklang mit den Anforderungen der Datenschutzrichtlinie für elektronische Kommunikation hinsichtlich des Schutzes von Endgeräten stehen, was bedeutet, dass die betreffende Person ihre Einwilligung geben müsste.

[12] In der kürzlich ergangenen Rechtsprechung des Gerichtshofs der Europäischen Union (Rechtssache Zeugen Jehovas, C-25/17, Urteil vom 10. Juli 2018) wurde klargestellt, dass eine Organisation, die auf die Erhebung und Verarbeitung personenbezogener Daten „Einfluss nimmt“, unter bestimmten Umständen als für die Verarbeitung Verantwortlicher angesehen werden kann.
[13] Artikel 5 und 6 der Datenschutz-Grundverordnung.

Wenn als Rechtsgrundlage die Einwilligung verwendet wird, muss diese nach der Datenschutz-Grundverordnung durch eine eindeutige bestätigende Handlung sowie freiwillig und in informierter Weise erfolgen.[14]

In den Wahlprozess involvierte Behörden verarbeiten personenbezogene Daten, um einer rechtlichen Verpflichtung oder der Wahrnehmung einer öffentlichen Aufgabe nachzukommen. Sonstige im Wahlprozess tätige Akteure können Daten auf der Grundlage der Einwilligung oder des berechtigten Interesses verarbeiten.[15] Auch politische Parteien und Stiftungen können Daten auf der Grundlage des öffentlichen Interesses verarbeiten, wenn dies im nationalen Recht vorgesehen ist.[16]

Behörden dürfen bestimmte Informationen über Personen, die in den Wählerverzeichnissen oder in den Melderegistern enthalten sind, nur dann an politische Parteien weitergeben, wenn dies nach dem Recht des jeweiligen Mitgliedstaats ausdrücklich zulässig ist, und nur zweckgebunden für die Zwecke der Werbung im Wahlkontext (z. B. Name und Anschrift).

Die Datenverarbeitung bei Wahlen betrifft häufig „sensible Daten". Die Verarbeitung solcher Daten, einschließlich der abgeleiteten „sensiblen Daten", ist grundsätzlich verboten, es sei denn, eine der in der Datenschutz-Grundverordnung genannten besonderen Begründungen trifft zu.[17] Die Verarbeitung „sensibler Daten" erfordert spezifische, strengere Auflagen: Die betroffene Person muss ihre ausdrückliche Einwilligung gegeben[18] oder die betroffenen Daten öffentlich gemacht haben.[19] Politische Parteien und Stiftungen können auch „sensible Daten" verarbeiten, wenn auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats ein erhebliches öffentliches Interesse besteht und geeignete Garantien vorhanden sind.[20] Die Datenschutz-Grundverordnung sieht ferner vor, dass die politischen Parteien und Stiftungen „sensible Daten" verarbeiten können, sofern sie sich ausschließlich auf ihre Mitglieder oder ehemaligen Mitglieder oder auf Personen beziehen, die regelmäßige Kontakte mit ihnen unterhalten; allerdings dürfen diese nur innerhalb der politischen Partei oder Stiftung offengelegt werden.[21] Diese spezielle Bestimmung kann jedoch nicht von einer politischen Partei dazu verwendet werden, Daten von potenziellen Mitgliedern oder Wählern zu verarbeiten.

Der Zweck der Datenverarbeitung sollte zum Zeitpunkt der Datenerhebung festgelegt werden (Grundsatz der Zweckbindung).[22] Daten, die zu einem bestimmten Zweck erhoben werden,

[14] Artikel 7 sowie Artikel 4 Absatz 11 der Datenschutz-Grundverordnung.
[15] Unter der Maßgabe, dass die Rechte und Freiheiten der betroffenen Personen nicht ernsthaft beeinträchtigt werden.
[16] Siehe Erwägungsgrund 56 der Datenschutz-Grundverordnung: „Wenn es in einem Mitgliedstaat das Funktionieren des demokratischen Systems erfordert, dass die politischen Parteien im Zusammenhang mit Wahlen personenbezogene Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern geeignete Garantien vorgesehen werden."
[17] Artikel 9 der Datenschutz-Grundverordnung.
[18] Artikel 9 Absatz 2 Buchstabe a der Datenschutz-Grundverordnung.
[19] Artikel 9 Absatz 2 Buchstabe e der Datenschutz-Grundverordnung.
[20] Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung.
[21] Artikel 9 Absatz 2 Buchstabe d der Datenschutz-Grundverordnung. Politische Parteien oder Stiftungen können die Daten über ihre Mitglieder oder ehemaligen Mitglieder oder Personen, die regelmäßige Kontakte mit ihnen unterhalten, nicht ohne die Einwilligung der betroffenen Person an Dritte weitergeben.
[22] Artikel 5 Absatz 1 Buchstabe b der Datenschutz-Grundverordnung.

dürfen nur für einen Zweck weiterverarbeitet werden, der damit vereinbar ist. Andernfalls muss eine neue, in der Datenschutz-Grundverordnung vorgesehene Rechtsgrundlage, etwa die Einwilligung, vorhanden sein, um die Daten für einen anderen Zweck zu verarbeiten. So dürfen insbesondere Daten, die von Lifestyle-Informationsbrokern oder Plattformen zu kommerziellen Zwecken erhoben werden, nicht im Zusammenhang mit Wahlen weiterverarbeitet werden.

Sofern die politischen Parteien und Stiftungen nicht mit der gebotenen Sorgfalt vorgehen und sich vergewissern, dass die Daten rechtmäßig erhoben wurden, können sie keine derartigen Daten von einem Dritten verwenden.

2.3 Transparenzanforderungen

Der Fall „Cambridge Analytica“ hat gezeigt, wie wichtig es ist, gegen Undurchsichtigkeit vorzugehen und die betroffenen Personen ordnungsgemäß zu informieren. Die Menschen wissen oft nicht, wer ihre personenbezogenen Daten verarbeitet und für welche Zwecke. Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffenen Personen über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet werden.[23] In der Datenschutz-Grundverordnung werden die diesbezüglichen Pflichten der für die Verarbeitung Verantwortlichen genauer dargelegt. Sie müssen die betroffenen Personen über die wichtigsten Aspekte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten informieren, darunter:

- die Identität des für die Verarbeitung Verantwortlichen,
- die Zwecke der Verarbeitung,
- die Empfänger ihrer personenbezogenen Daten,
- die Quelle der Daten, wenn diese nicht direkt bei der Person erhoben wurden,
- das Bestehen einer automatisierten Entscheidungsfindung und
- alle weiteren Informationen, die für eine faire und transparente Verarbeitung erforderlich sind.[24]

Darüber hinaus schreibt die Datenschutz-Grundverordnung vor, dass die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden.[25] So würde beispielsweise ein kurzer, undurchsichtiger Vermerk zum Datenschutz, der in kleiner Schrift in den Wahlunterlagen aufgeführt ist, die Transparenzanforderungen nicht erfüllen.

Nach den vorläufigen Erkenntnissen waren unvollständige Informationen über den Zweck, zu dem die Daten erhoben wurden, eine zentrale Unzulänglichkeit im Fall „Cambridge Analytica“, die auch die Gültigkeit der Einwilligung der betroffenen Personen infrage stellte. Alle Organisationen, die personenbezogene Daten im Zusammenhang mit Wahlen verarbeiten, müssen dafür Sorge tragen, dass die betroffenen Personen vor ihrer Einwilligung

[23] Artikel 5 Absatz 1 Buchstabe a der Datenschutz-Grundverordnung.
[24] Artikel 13 und 14 der Datenschutz-Grundverordnung.
[25] Leitlinien des Europäischen Datenschutzausschusses zur Transparenz.

oder bevor der für die Verarbeitung Verantwortliche damit beginnt, die Daten auf einer anderen Rechtsgrundlage zu verarbeiten, in vollem Umfang verstehen, wie und zu welchem Zweck ihre personenbezogenen Daten verwendet werden.

Die Informationen müssen den einzelnen Personen in jeder Phase der Verarbeitung, d. h. nicht nur bei der Datenerhebung, mitgeteilt werden.

Insbesondere wenn politische Parteien Daten verarbeiten, die sie von Dritten (z. B. von Wählerverzeichnissen, Informationsbrokern, Datenanalysten und anderen Quellen) erhalten haben, müssen sie den betroffenen Personen in der Regel mitteilen und erläutern, wie sie diese Daten kombinieren und nutzen, um eine faire Verarbeitung zu gewährleisten.[26]

2.4 Profiling, automatisierte Entscheidungsfindung und Mikrotargeting

Profiling ist eine Art der automatisierten Datenverarbeitung, die dazu dient, Aspekte in Bezug auf persönliche Vorlieben, Interessen, wirtschaftliche Lage usw. zu analysieren oder vorherzusagen.[27] Profiling kann dazu verwendet werden, Personen durch Mikrotargeting gezielt anzusprechen, d. h. personenbezogene Daten (z. B. den Suchverlauf im Internet) zu analysieren, um dadurch die besonderen Interessen einer bestimmten Zielgruppe oder Einzelperson zu ermitteln und ihre Handlungen beeinflussen zu können. Mikrotargeting kann dazu verwendet werden, einer Einzelperson oder einer Gruppe von Personen über einen Online-Dienst, z. B. soziale Medien, eine personalisierte Nachricht darzubieten.

Der Fall „Cambridge Analytica“ hat die besonderen Herausforderungen aufgezeigt, die sich durch Mikrotargeting-Methoden in den sozialen Medien ergeben. Organisationen können die von den Nutzern dieser Medien erhobenen Daten auswerten, um Wählerprofile zu erstellen. So können diese Organisationen möglicherweise Wähler ausfindig machen, die leichter beeinflussbar sind, und damit Einfluss auf die Wahlergebnisse nehmen.

Für diese Datenverarbeitung gelten alle allgemeinen Grundsätze und Vorschriften der Datenschutz-Grundverordnung, wie z. B. die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz und Zweckbindung. Die betroffenen Personen sind sich sehr oft nicht darüber im Klaren, dass sie einem Profiling unterzogen werden: Sie verstehen nicht, warum sie nach ihren letzten Suchanfragen bestimmte, offensichtlich damit zusammenhängende Werbeanzeigen erhalten, oder warum sie personalisierte Nachrichten von verschiedenen Organisationen erhalten. Die Datenschutz-Grundverordnung verpflichtet alle für die Verarbeitung Verantwortlichen, z. B. politische Parteien oder Datenanalysten, die Personen über den Einsatz solcher Techniken und deren Folgen zu informieren.[28]

Die Datenschutz-Grundverordnung erkennt an, dass die automatisierte Entscheidungsfindung, einschließlich Profiling, ernste Folgen haben kann. Sie sieht vor, dass eine Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie

[26] Artikel 14 der Datenschutz-Grundverordnung.
[27] Siehe Begriffsbestimmung in Artikel 4 Absatz 4 der Datenschutz-Grundverordnung.
[28] Artikel 13 Absatz 2 der Datenschutz-Grundverordnung.

in ähnlicher Weise erheblich beeinträchtigt, es sei denn, die Verarbeitung erfolgt unter strengen Auflagen, etwa wenn die betreffende Person ihre ausdrückliche Einwilligung gegeben hat oder wenn das Unionsrecht bzw. das Recht des Mitgliedstaats entsprechende Garantien vorsieht.[29]

Mikrotargeting-Methoden im Wahlkontext fallen in diese Kategorie, wenn sie ausreichend große Auswirkungen auf den Einzelnen haben. Der Europäische Datenschutzausschuss hat festgestellt, dass dies der Fall ist, wenn die Entscheidung das Potenzial hat, die Umstände, das Verhalten oder die Entscheidungen des Einzelnen erheblich zu beeinflussen oder längere oder dauerhafte Auswirkungen auf den Einzelnen zu haben.[30] Der Ausschuss war der Ansicht, dass gezielte Online-Werbung unter bestimmten Umständen das Potenzial hat, Personen erheblich zu beeinflussen, etwa wenn die Werbung eingreifenden Charakter hat oder ermittelte Schwächen des Einzelnen ausnutzt. Angesichts der Bedeutung, die der Ausübung des demokratischen Rechts auf Stimmabgabe zukommt, könnten z. B. personalisierte Mitteilungen, die dazu führen können, dass eine Person davon abgehalten wird, ihre Stimme abzugeben, oder eine bestimmte Wahl trifft, für das Kriterium der erheblichen Auswirkung infrage kommen.

Im Wahlkontext müssen die für die Verarbeitung Verantwortlichen dafür Sorge tragen, dass jede Verarbeitung, die auf solche Techniken zurückgreift, im Einklang mit den oben genannten Grundsätzen steht und die strengen Auflagen der Datenschutz-Grundverordnung einhält.

2.5 Sicherheit und Richtigkeit der personenbezogenen Daten

Angesichts des Volumens der betroffenen Datensätze und der Tatsache, dass diese häufig „sensible Daten“ enthalten, ist die Datensicherheit im Zusammenhang mit Wahlen von besonderer Bedeutung. Nach der Datenschutz-Grundverordnung müssen Betreiber, die personenbezogene Daten verarbeiten (sowohl für die Verarbeitung Verantwortliche als auch Auftragsverarbeiter), geeignete technische und organisatorische Maßnahmen ergreifen, um ein Schutzniveau zu gewährleisten, das den mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der Personen angemessen ist.[31]

Nach der Datenschutz-Grundverordnung müssen die für die Verarbeitung Verantwortlichen der zuständigen Aufsichtsbehörde unverzüglich und spätestens binnen 72 Stunden Verletzungen des Schutzes personenbezogener Daten melden. Wenn davon auszugehen ist, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat, muss der für die Verarbeitung

[29] Artikel 22 der Datenschutz-Grundverordnung.
[30] Leitlinien des Europäischen Datenschutzausschusses zu automatisierten Entscheidungsfindungen, WP251rev.01, zuletzt überarbeitet und angenommen am 6. Februar 2018.
[31] Artikel 32 der Datenschutz-Grundverordnung.

Verantwortliche auch die von der Verletzung betroffenen Personen unverzüglich davon in Kenntnis setzen.[32]

Politische Parteien und andere am Wahlprozess beteiligte Akteure müssen besonders darauf achten, dass bei Massendatensätzen und bei Daten aus unterschiedlichen, heterogenen Quellen die Richtigkeit der personenbezogenen Daten gewährleistet ist. Unrichtige Daten müssen unverzüglich gelöscht oder berichtigt und erforderlichenfalls aktualisiert werden.

2.6 Datenschutz-Folgenabschätzung

Mit der Datenschutz-Grundverordnung wird ein neues Instrument zur Risikobewertung vor Beginn der Datenverarbeitung eingeführt: die Datenschutz-Folgenabschätzung. Sie ist immer dann notwendig, wenn die Verarbeitung ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge haben könnte.[33] Dies ist im Wahlkontext der Fall, wenn ein für die Verarbeitung Verantwortlicher systematisch und eingehend persönliche Aspekte einer Person (einschließlich Profiling), die sich erheblich auf die Person auswirken, bewertet, und wenn der für die Verarbeitung Verantwortliche in großem Umfang „sensible Daten“ verarbeitet. Nationale Wahlbehörden müssen im Rahmen der Erfüllung ihrer öffentlichen Aufgaben nicht unbedingt eine Datenschutz-Folgenabschätzung durchführen, wenn bereits eine Datenschutz-Folgenabschätzung im Zusammenhang mit der Annahme der Rechtsvorschriften durchgeführt wurde.

Die von den verschiedenen Akteuren im Zusammenhang mit Wahlen durchzuführenden Folgenabschätzungen sollten die notwendigen Elemente enthalten, um den mit einer solchen Verarbeitung verbundenen Risiken zu begegnen; dazu zählen insbesondere die Rechtmäßigkeit der Verarbeitung, auch für Datensätze von Dritten, und die Transparenzanforderungen.

3. Rechte des Einzelnen

Die Datenschutz-Grundverordnung räumt natürlichen Personen zusätzliche und stärkere Rechte ein, die im Zusammenhang mit Wahlen besonders wichtig sind:

- das Recht auf Auskunft zu ihren personenbezogenen Daten;
- das Recht, die Löschung ihrer personenbezogenen Daten zu beantragen, wenn die Verarbeitung auf Einwilligung beruht und diese Einwilligung widerrufen wird, die Daten nicht mehr benötigt werden oder die Verarbeitung rechtswidrig ist; und
- das Recht, unrichtige, ungenaue oder unvollständige personenbezogene Daten berichtigen zu lassen.

[32] Artikel 33 und 34 der Datenschutz-Grundverordnung; Leitlinien des Europäischen Datenschutzausschusses zur Meldung von Verletzungen des Schutzes personenbezogener Daten.
[33] Artikel 35 und 36 der Datenschutz-Grundverordnung; Leitlinien des Europäischen Datenschutzausschusses zur Datenschutz-Folgenabschätzung.

Natürliche Personen haben auch das Recht, Widerspruch gegen die Verarbeitung (z. B. die Weitergabe von Daten aus Wählerverzeichnissen an politische Parteien) einzulegen, wenn die Verarbeitung ihrer Daten auf „berechtigtem Interesse“ oder „öffentlichem Interesse“ beruht.

Natürliche Personen haben das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung ihrer personenbezogenen Daten beruhenden Entscheidung unterworfen zu werden. In diesen Fällen kann die Person das Eingreifen einer natürlichen Person erwirken und hat das Recht, ihren eigenen Standpunkt darzulegen und die Entscheidung anzufechten.

Damit der Einzelne diese Rechte wahrnehmen kann, müssen alle beteiligten Akteure die erforderlichen Instrumente und Vorrichtungen bereitstellen. Die Datenschutz-Grundverordnung sieht die Möglichkeit vor, Verhaltensregeln aufzustellen, die die Anwendung der Verordnung in bestimmten Bereichen, u. a. auch für Wahlen, festlegen und von einer Datenschutzbehörde genehmigt werden.

Ferner räumt die Datenschutz-Grundverordnung natürlichen Personen das Recht ein, Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen. Natürliche Personen haben außerdem das Recht, eine Nichtregierungsorganisation mit der Einreichung einer Beschwerde in ihrem Namen zu beauftragen.[34] In bestimmten Mitgliedstaaten kann eine Nichtregierungsorganisation nach nationalem Recht auch ohne Auftrag einer natürlichen Person eine Beschwerde einreichen. Angesichts der großen Zahl potenziell betroffener Personen ist dies im Wahlkontext besonders relevant.

[34] Artikel 80 Absatz 1 der Datenschutz-Grundverordnung.

Zentrale Datenschutzfragen im Wahlkontext[35]

Politische Parteien und Stiftungen	Politische Parteien und Stiftungen gelten als Verantwortliche • Zweckbindung einhalten, Daten nur zu Zwecken weiterverarbeiten, die mit dem ursprünglichen Zweck vereinbar sind (z. B. beim Austausch von Daten mit Plattformen) • zutreffende Rechtsgrundlage für die Verarbeitung wählen (auch für abgeleitete Daten): Einwilligung, berechtigtes Interesse, Aufgabe im öffentlichen Interesse (falls gesetzlich vorgesehen), besondere Auflagen für „sensible Daten“ (z. B. politische Meinung) • Datenschutz-Folgenabschätzung durchführen • betroffene Personen über jeden Verarbeitungszweck aufklären (Transparenzanforderungen), entweder bei der Erhebung von Daten oder bei der Erlangung der Daten von Dritten • Richtigkeit der Daten gewährleisten, insbesondere bei Daten aus verschiedenen Quellen und bei abgeleiteten Daten • prüfen, ob die von Dritten erlangten Daten rechtmäßig erhoben wurden und zu welchen Zwecken (z. B.: ob die betroffenen Personen in Kenntnis der Sachlage ihre Einwilligung für einen bestimmten Zweck gegeben haben) • spezifische Risiken des Profiling berücksichtigen und geeignete Garantien vorsehen • bei der Verwendung der automatisierten Entscheidungsfindung besondere Auflagen einhalten (z. B. ausdrückliche Einwilligung einholen und geeignete Garantien umsetzen) • alle Personen, die Zugang zu den Daten haben, eindeutig identifizieren • sichere Verarbeitung durch technische und organisatorische Maßnahmen gewährleisten; Datenschutzverletzungen melden • Verpflichtungen in Verträgen oder anderen verbindlichen Rechtsakten mit Auftragsverarbeitern (z. B. Anbietern von Datenanalysen) klären • Daten löschen, sobald sie für den ursprünglichen Zweck, für den sie erhoben wurden, nicht mehr benötigt werden
Informationsbroker und Anbieter von	Informationsbroker und Anbieter von Datenanalysen sind je nachdem, in welchem Umfang sie die Kontrolle über die Verarbeitung

[35] Die vorgenannten Informationen sind in keiner Weise erschöpfend. Sie dienen dazu, eine Reihe von zentralen, in der Datenschutz-Grundverordnung vorgesehenen Datenschutzverpflichtungen hervorzuheben, die im Wahlkontext von Bedeutung sind. Sie basieren auf der Annahme, dass die politischen Parteien die Daten selbst erheben (aus öffentlichen Quellen, aus ihrer eigenen Präsenz in den sozialen Medien, direkt von den Wählern usw.) und die Dienste von Informationsbrokern oder Anbietern von Datenanalysen nutzen, um die Wähler über soziale Medien gezielt anzusprechen. Auch Plattformen können für die oben genannten Akteure eine Datenquelle sein. Gegebenenfalls sind auch noch andere Rechtsvorschriften relevant, z. B. die in der Datenschutzrichtlinie für elektronische Kommunikation vorgesehenen Vorschriften über den Versand unerbetener Nachrichten und den Schutz von Endgeräten.

<table>
<tr><td rowspan="3">Datenanalysen</td><td colspan="2">ausüben, entweder (gemeinsam) Verantwortliche oder Auftragsverarbeiter</td></tr>
<tr><td>Für Verantwortliche gilt:</td><td>Für Auftragsverarbeiter gilt:</td></tr>
<tr><td>Zweckbindung einhalten, Daten nur zu Zwecken weiterverarbeiten, die mit dem ursprünglichen Zweck vereinbar sind (insb. beim Austausch von Daten mit Dritten)
zutreffende Rechtsgrundlage für die Verarbeitung wählen: Einwilligung, berechtigtes Interesse. Bei „sensiblen Daten“ ist die Verarbeitung nur möglich, wenn die ausdrückliche Einwilligung vorliegt oder Daten offensichtlich öffentlich gemacht wurden
Datenschutz-Folgenabschätzung durchführen
betroffene Personen über jeden Verarbeitungszweck aufklären (Transparenzanforderungen), insbesondere bei Einwilligung, da die Daten in der Regel an Dritte verkauft werden
bei der Verwendung der automatisierten Entscheidungsfindung besondere Auflagen einhalten (z. B. ausdrückliche Einwilligung einholen und geeignete Garantien umsetzen)
bei der Zusammenlegung verschiedener Datensätze besonders auf die Rechtmäßigkeit der Verarbeitung und auf die Richtigkeit der Daten achten
sichere Verarbeitung durch technische und organisatorische Maßnahmen gewährleisten; Datenschutzverletzungen melden</td><td>Verpflichtungen aus dem Vertrag oder dem mit dem Verantwortlichen geschlossenen anderen Rechtsakt einhalten
sichere Verarbeitung durch technische und organisatorische Maßnahmen gewährleisten
den Verantwortlichen bei der Datenschutz-Folgenabschätzung oder bei der Ausübung der Rechte der betroffenen Personen sowie insofern unterstützen, dass erkannte Datenschutzverletzungen unverzüglich an den Verantwortlichen gemeldet werden</td></tr>
<tr><td></td><td colspan="2">Plattformen sind in der Regel Verantwortliche, soweit die Verarbeitung auf ihren Plattformen betroffen ist, und möglicherweise zusammen mit anderen Organisationen gemeinsam Verantwortliche</td></tr>
<tr><td>Social-Media-Plattformen/Online-Werbenetzwerke</td><td colspan="2">zutreffende Rechtsgrundlage für die Verarbeitung wählen: Vertrag mit natürlichen Personen, Einwilligung, berechtigtes Interesse. Bei „sensiblen Daten“ ist die Verarbeitung nur möglich, wenn die ausdrückliche Einwilligung vorliegt oder Daten offensichtlich</td></tr>
</table>

	öffentlich gemacht wurden • nur Daten verwenden, die für den angegebenen Zweck erforderlich sind • Datenschutz-Folgenabschätzung durchführen • beim Austausch von Mitgliederdaten mit Dritten Rechtmäßigkeit gewährleisten • Transparenzanforderungen einhalten, insbesondere hinsichtlich der Geschäftsbedingungen, wenn die Daten anschließend an Dritte weitergegeben werden usw. • bei der Verwendung der automatisierten Entscheidungsfindung besondere Auflagen einhalten (z. B. ausdrückliche Einwilligung einholen und geeignete Garantien umsetzen) • sichere Verarbeitung durch technische und organisatorische Maßnahmen gewährleisten; Datenschutzverletzungen melden • Kontrollen und Vorrichtungen für Personen bereitstellen, damit diese ihre Rechte wirksam wahrnehmen können, einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung – einschließlich Profiling – unterworfen zu werden
	Nationale Wahlbehörden sind Verantwortliche
Nationale Wahlbehörden	• Rechtsgrundlage der Verarbeitung: rechtliche Verpflichtung oder gesetzlich vorgesehene Aufgabe von öffentlichem Interesse • Datenschutz-Folgenabschätzung durchführen, wenn die Folgen nicht bereits im Gesetz bewertet wurden