STIFTUNG DATENSCHUTZ

Datenschutz im Wahlkampf

Tipps zum richtigen Umgang mit personenbezogenen Daten *Wahlsaison 2022*

Wählen Sie Datenschutz!

Frederick Richter
Vorstand Stiftung Datenschutz

Die Unverfälschtheit der Ergebnisse freier Wahlen erscheint in der heutigen Zeit als besonders hohes Gut. Die zweifelsfreie demokratische Willensbildung muss gerade im Zeitalter von „fake news“ und social bots geschützt werden.

Ebenso wichtig ist es natürlich aus Sicht des Datenschutzes, dass alle Beteiligten beim Kampf um die Stimmen der Wählerinnen und Wähler deren Bürgerrechte wahren und mit den auf sie bezogenen Daten behutsam umgehen.

Wir wünschen Ihnen einen erfolgreichen Wahlkampf!

Was sind personenbezogene Daten?

(Art. 4 Nr. 1 DSGVO)

Alle Informationen, die sich auf eine konkrete, natürliche Person beziehen oder beziehen lassen, zum Beispiel Namen oder E-Mail-Adressen.

Daten, aus denen politische Meinungen, religiöse und weltanschauliche Überzeugungen, die Zugehörigkeit zu Gewerkschaften, Informationen zur Gesundheit, zum Sexualleben, zur Hautfarbe und ethnischen Herkunft hervorgehen, sind besonders geschützt (besondere Arten von personenbezogenen Daten, Art. 9 Abs. 2 DSGVO) und dürfen nur unter strengen Voraussetzungen verarbeitet werden.

Datenminimierung und Zweckbindung

(Art. 5 Absatz 1 lit. c DSGVO)

Personenbezogene Daten sollten nur dann erhoben und gespeichert werden, wenn es für die beabsichtigte Nutzung, also für den Verwendungszweck, unbedingt notwendig ist.

Personenbezogene Daten dürfen auch nur für zuvor festgelegte, eindeutige und legitime Zwecke erhoben werden

Beispiel *Interessenten haben der Aufnahme der ihrer Kontaktdaten in die Adressdatei eines Ortsverbandes zugestimmt, sie möchten über lokale politische Initiativen informiert werden. In diesem Fall dürfen die Kontaktdaten nicht in einer zentralen Adressdatei auf Bundesebene gelangen, dafür wäre eine weitere Einwilligung erforderlich. Daher sollten Formulare zur Datenerhebung unterschiedliche Einwilligungsmöglichkeiten enthalten, die von den Interessentinnen und Interessenten angekreuzt werden können.*

Erhebung von Daten und Informationspflichten

(Art. 13 & Art. 14 DSGVO)

Daten sollten direkt bei der Person, um die es geht, erhoben werden. In jedem Fall muss sie über die Datenerhebung informiert werden. Eine Informationspflicht besteht auch dann, wenn die Daten aus öffentlich zugänglichen Quellen stammen.

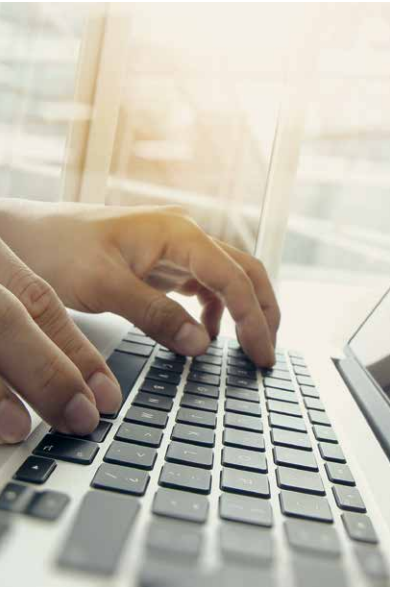
Beispiel *Daten über die Parteizugehörigkeit, Telefonnummer etc. eines Betroffenen dürfen nicht bei Nachbarn erfragt werden.*

Unter welche Voraussetzungen dürfen personenbezogene Daten verarbeitet werden?

(Artikel 6 DSGVO)

Wenn personenbezogene Daten für Wahlkampfzwecke erhoben werden sollen, müssen die betroffenen Personen dem zustimmen.

Berechtigte Interessen (Artikel 6 Absatz 1f DSGVO)

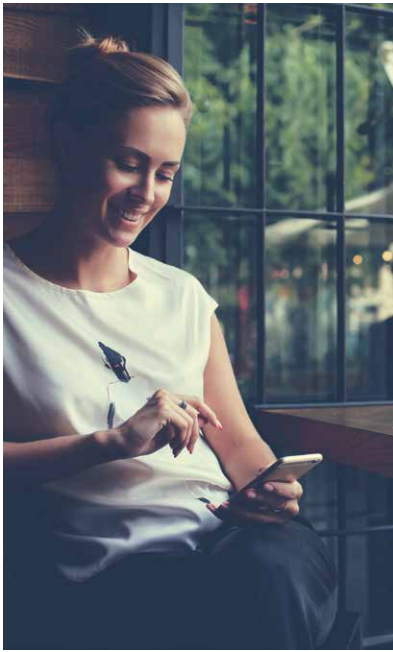


Die Datenverarbeitung kann auch zulässig sein, wenn der Verarbeiter, also hier die Wahlkämpfer, ein berechtigtes Interesse nachweisen können, doch das ist meist schwierig. Denkbar wäre dies aber für Wahlwerbung durch Briefpost. Das Bundesmeldegesetz erlaubt es Parteien, Wählerdaten von den Einwohnermeldeämtern zu beziehen. Diese Daten dürfen nur für die Wahlwerbung und ausschließlich in den sechs Monaten vor und einen Monat nach der Wahl genutzt werden; danach sind sie zu löschen.

Zu beachten ist

Stammen die Daten aus öffentlich zugänglichen Quellen, wie Adressverzeichnissen, müssen die Betroffenen über die Quelle und über ihre Möglichkeit zum Widerspruch informiert werden. Soziale Netzwerke sind in diesem Sinne keine öffentlichen Quellen; hier sollten keine personenbezogenen Daten erhoben werden.

Stammen die Kontaktdaten von der Webseite der betroffenen Person (z.B. Unternehmens-Homepage), darf für die Versendung der Wahlwerbung nur die Postanschrift verwendet werden, da die Nutzung der E-Mail-Adresse stets einer ausdrücklichen Einwilligung bedarf.



Einwilligung (Artikel 7 DSGVO)

Liegt kein „berechtigtes Interesse" vor, bedarf es für die Datenverarbeitung der Einwilligung der betroffenen Person: Sie muss darüber informiert werden, dass ihre Daten für Wahlkampfzwecke verarbeitet werden, und sie muss dem freiwillig zustimmen. Diese Einwilligung kann jederzeit widerrufen werden; darüber muss die Person ebenfalls informiert werden. Wichtig ist die Dokumentation der jeweiligen Einwilligung, um nachweisen zu können, auf welcher Grundlage personenbezogene Daten verarbeitet werden.

Wahlwerbung per E-Mail und Telefon erfordert stets eine freiwillige, informierte Einwilligung.

Auch die Veröffentlichung von Personenfotos auf der Webseite bedarf im Regelfall der Einwilligung der abgebildeten Person. Nur im Ausnahmefall kann die Veröffentlichung auch ohne Einwilligung erlaubt sein (z.B. Fotografien, die auf öffentlichen Veranstaltungen gemacht wurden, um einen repräsentativen Gesamteindruck der Veranstaltung zu vermitteln).

Verpflichtung zur Wahrung der Vertraulichkeit

Es wird empfohlen, die Personen, die mit personenbezogenen Daten umgehen, (z.B. Wahlkampfhelfende, die Adresslisten erstellen) schriftlich auf das Datengeheimnis zu verpflichten. Sie müssen die erlangten Personendaten geheim halten und dürfen z.B. Adressen, die die Partei erhoben hat, keinesfalls für eigene Zwecke verwenden oder mitnehmen. Die Schriftform dient dem Nachweis, denn die Datenschutz-Grundverordnung sieht eine Rechenschaftspflicht für die Rechtmäßigkeit der Datenverarbeitung vor.

Rechte der betroffenen Person

(Artikel 12 bis 22 DSGVO)

Nach der Datenschutz-Grundverordnung stehen den Betroffenen umfangreiche Informations-und Auskunftsrechte zu: Welche Daten sind gespeichert und woher stammen sie? Warum, wofür und wie langen werden Daten gespeichert? Werden die Daten an weitere Personen übermittelt? Wo kann man sich beschweren? Besteht ein Widerrufs- oder Widerspruchsrecht? Auf das Widerspruchsrecht muss spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich sowie in einer verständlichen und von anderen Informationen getrennten Form hingewiesen werden. Die Ausübung dieses Rechts führt zu einem sofortigen Verarbeitungsstopp. Darüber hinaus haben Betroffene An-

spruch auf Berichtigung und Löschung ihrer Daten.

Insgesamt *müssen Maßnahmen getroffen und geeignete Prozesse vorgehalten werden, um die Anfragen der Betroffenen fristgerecht und korrekt bearbeiten zu können. Dies mag bei kleinen Kampagnen einfach sein, kann jedoch bei großen Datenbanken einen nicht unerheblichen Aufwand erzeugen. Die Datenschutz-Grundverordnung verlangt ausdrücklich, dass der Verantwortliche den betroffenen Personen die Ausübung ihrer Rechte erleichtern muss. Auf Anträge des Betroffenen muss innerhalb eines Monats geantwortet werden. Gründe für eine eventuelle Fristverlängerung müssen ebenfalls in der Monatsfrist mitgeteilt werden, so dass in jedem Fall schnell reagiert werden muss. Anderenfalls droht ein Bußgeld.*

Nutzerverfolgung auf eigenen Webseiten

Nutzer von Internetangeboten dürfen auch im Wahlkampf auf Webseiten nicht über die für die Nutzung der Seite notwendige Datenerhebung hinausverfolgt („getrackt“) werden. Zu beachten ist: Wenn eine Webseite aufgerufen wird, wird immer die IP-Adresse des Nutzers für den Verbindungaufbau der Seite, also die technische Verbindung zum Anzeigen der Inhalte verwendet. Diese IP-Adresse darf ohne Zustimmung der Nutzerinnen und Nutzer nicht – ebenso wenig wie andere Personendaten – dauerhaft gespeichert, ausgelesen oder anderweitig verwendet werden, insbesondere nicht an Dritte übermittelt werden. Es wird empfohlen im Rahmen der Geolokalisierung das letzte Oktett der IP-Adresse durch Nullen oder xxx. zu ersetzen. Nicht ausreichend ist jedoch die Bildung eines Hashwerts, da hier die Rückführung auf die ursprüngliche IP-Adresse ohne unverhältnismäßigen Aufwand möglich sei.

Grundsätzlich gilt:

- *Auch Cookies sind personenbezogene Daten und dürfen nur mit Zustimmung der Nutzer gesetzt werden, so dass eine entsprechende Einwilligung einzuholen ist (Ausnahme: Cookies sind aus technischen Gründen erforderlich).*
- *Das Internetangebot muss zudem über die Datenverarbeitung informieren und damit eine Datenschutzerklärung enthalten.*
- *Weiterhin muss ein deutlicher Hinweis auf das Impressum erfolgen. Darin ist auch ein Verantwortlicher für journalistisch-redaktionelle Inhalte zu benennen, wenn etwa Pressemitteilungen oder sonstige aktuelle Informationen veröffentlicht werden.*

Techniken zur Reichweitenmessung des Internetangebots bedürfen aus datenschutzrechtlicher Sicht der Information über den Einsatz dieser Technik. Analyse-Tools, die Daten über das Nutzungsverhalten an Dritte weitergeben, bedürfen einer Einwilligung. Dies ist stets der Fall, wenn sich der Dienstleister, der das Tool anbietet, die Verwendung der Daten für eigene Zwecke vorbehält. Bei der Einwilligung ist außerdem auf die Freiwilligkeit zu achten. Wichtig ist, dass der Nutzer seine Einwilligung(en)durch eine aktive Handlung erteilen kann, wie zum Beispiel durch das Setzen von Häkchen im Banner oder durch den Klick auf eine Schaltfläche.

Aus Sicht des Wahlkämpfers ist zwar durchaus verständlich, dass weitverbreitete Plattformen wie Facebook genutzt werden, um eine umfassende Bürgernähe zu gewährleisten, jedoch sollte jenem bewusst sein, dass er seine „Bürgernähe“ in gewisser Weise mit der Privatsphäre seiner Wähler bezahlt. Vorzuziehen sind daher Weiterleitungen auf eigene Webseiten – gerade auch, weil dem Wahlkämpfer so deutlich mehr Kontrolle über die Wahlkampagne eröffnet wird und Datenschutzkonformität erreichbar ist. Besonders zu berücksichtigen ist hier, dass Fanpage-Betreiber und Facebook gemeinsam für den datenschutzkonformen Betrieb einer Facebook-Fanpage verantwortlich sind, da beide über die Zwecke und Mittel der Verarbeitung entscheiden. Daher ist auch aus diesem Grunde Vorsicht und Zurückhaltung bei der Einbindung von Social Media Plattformen geboten.

Sicherheit der Datenverarbeitung

(Artikel 32 DSGVO)

Es müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies schließt auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein. Das gilt für alle Daten, die sich auf Personen beziehen; es gibt also grundsätzlich keine „belanglosen“ Daten.

Für besonders sensible Daten muss auch mehr Aufwand betrieben werden als für normale Personendaten. In die Kategorie der sensiblen Angaben gehören – siehe oben – auch die für Parteien sehr interessante politische Präferenz der Menschen; für die Sicherung dieser Informationen ist erhöhter Aufwand zu betreiben.

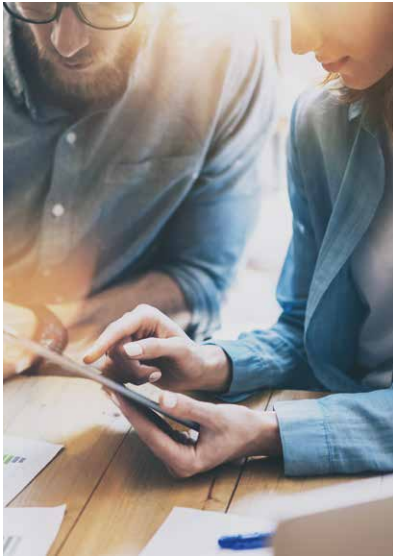
Praxistipp *Bei Kontaktformularen, in denen vom Nutzer personenbezogene Daten eingegeben werden, sollte eine aktuelle und dem Stand der Technik entsprechende Transportverschlüsselung eingesetzt werden, um Verstößen und Mahnungen aus dem Weg zu gehen.*

Auch bei Messengerdiensten ist auf eine verschlüsselte Kommunikation zu achten. Es sollten datenschutzfreundlich ausgestaltete Messengerdienste mit einer Ende-zu-Ende-Verschlüsselung verwendet werden, um aktuelle Informationen bereit zu stellenZusätzlich können die über Messengerdienste verbreiteten Informationen auch auf der Webseite veröffentlicht werden, damit sich niemand gezwungen sind, in die Nutzungsbedingungen eines Messengerdienstes einzuwilligen.

Wahlkampf-Mails und „Spam-Wahlkampf“

- Inhaber der Mail-Adressen müssen dem Empfang von Wahlwerbung vorher zustimmen. Empfehlung: Immer muss beachtet werden, dass für die Betroffenen die einfache Möglichkeit bestehen muss, vorhandene personenbezogene Daten abzufragen und diese ggfs. löschen zu lassen. Dazu gehört auch, dass E-Mails betreffende Informationen zur Abmeldung und Löschung der Personendaten bei der verantwortlichen Stelle besitzen.
- Zu beachten ist: Öffentlich verfügbar E-Mail-Adressen stellen in keinem Fall eine Einwilligung zum unaufgeforderten Versand von Mails dar.
- Bei der Einholung von Einwilligungen ist deren Freiwilligkeit zu beachten. Die Zustimmung zur Datenverwendung darf nicht mit Gegenleistungen für die Preisgabe der E-Mai-Adresse verkoppelt werden, denn das schließt u.U. die Freiwilligkeit aus.

- Eine Authentifizierung des Nutzers bei Eintragung einer Mail-adresse in ein Online Formular ist anzuraten. Es muss gewährleistet werden, dass der Übermittler der Mailadresse deren wirklicher Inhaber ist. Im Allgemeinen trägt der Werbende dabei das Risiko und muss seine Systeme so halten, dass eine missbräuchliche Nutzung verhindert werden kann.



Empfehlung

Es sollte das – mittlerweile sehr verbreitete – sogenannte „Double opt-in Verfahren" eingesetzt werden, bei dem auf die Mailadresse des Nutzers eine Abfragemail gesendet wird, welche ihm mitteilt, dass seine Adresse auf betreffender Webseite für den Newsletter oder Informationsmails eingetragen wurde und dieser dann noch einmal („doppelt") über einen Bestätigungslink zustimmen muss. Dadurch wird überprüft, ob die Aufnahme in den Mail-Verteiler tatsächlich im Interesse des Mailinhabers liegt.
Keinesfalls jedoch sollte die Bestätigungsmail schon einen „werbenden" Charakter haben.
Bei Versendung der Mail ist dringend darauf zu achten, den Adressverteiler in „blind copy" (BCC) zu setzen!

Aufkleber an Briefkästen mit dem Aufdruck „Keine Werbung" müssen bei Wahlwurfsendungen beachtet werden.

Datenpannen

(Artikel 33, 34 DSGVO)

Liegt eine Datenschutzverletzung vor, muss hierüber innerhalb von 72 Stunden eine Meldung erfolgen. Im Falle eines hohen Risikos für die persönlichen Rechte und Freiheiten einer natürlichen Person ist außerdem die betroffene Person unverzüglich über die Verletzung in klarer und einfacher Sprache zu informieren. Die Aufsichtsbehörden stellen auf ihren Webseiten Informationen zur Meldung von Datenschutzverstößen sowie Online-Meldeformulare bereit.

Besonderheiten für Abgeordnete und Wahlkampfhelfer

Gemäß einer Handreichung aus dem Jahre 2018 der damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit handelt es sich bei den **Abgeordneten des Deutschen Bundestages einschließlich der Abgeordnetenbüros** um öffentliche Stellen des Bundes (§ 2 Absatz 1 BDSG zu bewerten), so dass die Vorgaben der Datenschutz-Grundverordnung für Datenverarbeitungen anzuwenden sind. Es muss daher etwa ein Datenschutzbeauftragter benannt und ein Verzeichnis für Verarbeitungstätigkeiten geführt werden. In vielen Fällen werden die Abgeordneten die Verarbeitung personenbezogener Daten nur auf eine ausdrückliche Einwilligung der betroffenen Personen stützen können. Insbesondere, wenn Abgeordnete Anschreiben von Bürger erhalten, die sensible Daten über Dritte enthalten (etwa politische, weltanschauliche Überzeugungen), bedarf es deren ausdrücklicher Einwilligung, die oft fehlen dürfte. Diese Daten sind dann unverzüglich zu löschen. Kontaktdaten hingegen sind meist zur Ausübung des Mandats erforderlich. Aber natürlich gelten auch hier die Betroffenenrechte.

Disclaimer

In den Bundesländern sind mögliche **Bereichsausnahmen** *zu berücksichtigen, die für die Landesparlamente geschaffen wurden.*

In Brandenburg, Sachsen, Rheinland-Pfalz, Mecklenburg-Vorpommern und Thüringen unterliegen der Landtag, Mitglieder und Fraktionen bei der Wahrnehmung parlamentarischer Aufgaben nicht den datenschutzgesetzlichen Bestimmungen der Landesdatenschutzgesetze, sondern einer Datenschutzordnung des Landtags.

Aufgrund der damit verbundenen Unsicherheiten kann sich für die Abgeordneten in diesen Bundesländern eine Nachfrage bei der zuständigen Datenschutzaufsichtsbehörde empfehlen.

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter

7 Tipps für einen *datenschutzgerechten Wahlkampf*

1. Erklären Sie **transparent**, welche personenbezogenen Daten Sie erfassen.
2. Erfassen Sie nur die Daten, die **für den Zweck** auch wirklich **erforderlich** sind.
3. Geben Sie einfache **Hinweise zum Widerspruch**.
4. Verzichten Sie auf **unangeforderte Mails** (Spam).
5. Geben Sie Daten **nicht ohne Zustimmung** weiter – auch nicht an Dienstleister.
6. Wann immer möglich, **verschlüsseln** Sie personenbezogene Daten.
7. Nutzen Sie **nicht alle Tracking-Technologien**, nur weil Sie es können.