Datenschutz im Europa-Wahlkampf

Tipps zum richtigen Umgang mit personenbezogenen Daten
Frühjahr 2019

---

1. Was sind personenbezogene Daten ? (Artikel 4 Nr. 1 DSGVO)

Alle Informationen, die sich auf eine konkret identifizierbare natürliche Person beziehen, z.B. auch mittels Zuordnung zu einem Namen, zu Standortdaten oder zu einer Online-Kennung.

Besonders schutzbedürftig sind die sogenannten sensiblen Daten (Artikel 9 Absatz 1 DSGVO). Ihre Verarbeitung ist an strengere Voraussetzungen gebunden als die Verarbeitung sonstiger personenbezogener Daten. Zu diesen „besondere Arten personenbezogener Daten" zählen (unter anderen) Daten, aus denen die Hautfarbe und die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, Gesundheitsdaten oder Daten zum Sexualleben.

2. Datenminimierung und Zweckbindung (Artikel 5 Absatz 1 lit. c DSGVO)

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

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. In diesem Fall dürfen die Kontaktdaten nicht in einer zentralen Adressdatei auf Bundesebene gelangen, dafür wäre eine weitere Einwilligung erforderlich.

3. Erhebung von Daten und Informationspflichten (Artikel 13 + Artikel 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.

Sie müssen direkt bei der betroffenen Person erfragt werden.

4. Unter welche Voraussetzungen dürfen personenbezogene Daten verarbeitet werden? (Artikel 6 DSGVO)

Die Erhebung und Verarbeitung von personenbezogenen Daten zu Zwecken des Wahlkampfes bedarf regelmäßig einer Einwilligung. Eine Datenverarbeitung aufgrund eines berechtigten Interesses kann ausnahmsweise in Betracht kommen:

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. Mit diesem berechtigten Interesse können Parteien auch die Wählerdaten von den Einwohnermeldeämtern beziehen.

Der zeitliche Rahmen ist hier auf die sechs Monate vor und den Monat nach der Wahl beschränkt; danach müssen die Daten gelöscht werden. Stammen die Daten jedoch 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.

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

Einwilligung (Artikel 7 DSGVO)

Liegt kein „Berechtigtes Interesse“ vor, bedarf es einer Einwilligung: Die betroffenen Personen müssen über die Verarbeitung ihrer Daten zum Zweck des Wahlkampfes informiert werden, und müssen dieser zustimmen (Einwilligung).

Die Einwilligung kann jederzeit widerrufen werden; darüber muss die Person informiert werden.

Die Einwilligung in die Datenverarbeitung muss die betroffene Person freiwillig geben.

Wahlwerbung per email und Telefon erfordert stets die Einwilligung.

5. 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. nicht Adresslisten, die die Partei zusammengestellt hat, für eigene Zwecke verwenden oder mitnehmen.

Die Schriftform dient dem Nachweis, denn die Datenschutzgrundverordnung sieht eine Rechenschaftspflicht für die Rechtmäßigkeit der Datenverarbeitung vor.

6. Rechte der betroffenen Person

(Artikel 12 bis 22 DSGVO)

Nach der Datenschutzgrundverordnung 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 Anspruch auf Berichtigung und Löschung.

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 Datenschutzgrundverordnung 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.

7. 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. Dies bedeutet, dass etwa IP-Adressen und andere Personendaten nicht ohne Zustimmung

der Nutzerinnen und Nutzer aufgezeichnet und analysiert und insbesondere nicht an Dritte übermittelt werden dürfen. Aufsichtsbehörden empfehlen 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:

- Cookies dürfen nur mit Zustimmung der Nutzer gesetzt werden, so dass eine entsprechende Einwilligung einzuholen ist.
- Das Internetangebot muss zudem über die Datenverarbeitung informieren und damit eine Datenschutzerklärung enthalten.
- Weiterhin muss ein deutlicher Hinweis auf das Impressum erfolgen.

Techniken zur Reichweitenmessung des Internetangebots bedürfen aus datenschutzrechtlicher Sicht der Information über den Einsatz dieser Technik. Die Orientierungshilfe der Aufsichtsbehörden (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf) führt hierzu aus, dass für diesen Zweck keine andauernde Wiedererkennung und stetig umfangreichere Profilbildung sowie keine Weitergabe von Daten an Dritte nötig sind. Nach Auffassung der Aufsichtsbehörden ist die Beeinträchtigung des Nutzers in diesem Falle als gering zu bewerten mit der Folge, dass die Interessenabwägung zugunsten des Verantwortlichen ausfällt. Darüberhinausgehende Profilingmaßnahmen oder die Erstellung von Nutzerprofilen bedürfen allerdings stets der Einwilligung. Die Aufsichtsbehörden verweisen darauf, dass erst wenn der Nutzer seine Einwilligung(en)durch eine aktive Handlung, wie zum Beispiel das Setzen von Häkchen im Banner oder den Klick auf eine Schaltfläche abgegeben hat, die einwilligungsbedürftige Datenverarbeitung tatsächlich (durch technische Maßnahmen sichergestellt) stattfinden darf.

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 zudem die Entscheidung des Europäischen Gerichtshofs, 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.

8. 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.

- ⇨ Hierfür steht das https-Protokoll zur Verfügung.
- ⇨ Auch bei Messengerdiensten ist auf eine verschlüsselte Kommunikation zu achten. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit verweist zudem auf die Verwendung von datenschutzfreundlich ausgestalteten Messenger-Diensten. Sie betont, dass kein Kommunikationspartner dazu gezwungen werden sollte, wider seiner Überzeugung in Datenschutzbedingungen einzuwilligen, nur um z. B. aktuelle Informationen der Abgeordneten zu erhalten. So könnten mehrere Messengerdienste genutzt werden.

9. Wahlkampf-Mails und „Spam-Wahlkampf"

Zum Teil werden im Wahlkampf Email-Aussendungen eingesetzt, im Rahmen derer massenhaft Bürger angeschrieben werden. In Deutschland kann solches recht klar durch gesetzliche Unterlassungsansprüche abgewehrt werden (§ 823 bzw. § 1004 BGB; § 7 UWG).

Es gilt, dass die Inhaber der Mail-Adressen dem Empfang vorher zu~~ge~~stimmen müssen und die Zweckbindung gewahrt wird.

Einwilligungen, die vor dem 25. Mai 2018 eingeholt wurden, gelten fort, wenn sie den Bedingungen der Datenschutzgrundverordnung genügen. Es muss daher auch unter altem Recht eine freiwillige Einwilligung vorgelegen haben und eine Information über die Datenverarbeitung erfolgt sein. Entsprechendes gilt für die jederzeitige Widerrufsmöglichkeit der Einwilligung.

- ➢ 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 Mails betreffende Informationen zur Abmeldung und Löschung der Personendaten bei der verantwortlichen Stelle besitzen.
- ➢ Zu beachten ist: Öffentliche 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-Mail Adresse verkoppelt werden, denn das schließt u.U. die Freiwilligkeit aus.
- Eine Authentifizierung des Nutzers bei Eintragung einer Mail-adresse in 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, da dies wiederum Problem mit vorgenannten Regelung zum Spamversand macht.

Bei Versendung der Mail ist dringend darauf zu achten, den Adressverteiler in "blind copy" (BCC) zu setzen.

10. 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.

11. Besonderheiten für Abgeordnete und Wahlkampfhelfer

Insgesamt ist umstritten, inwieweit Abgeordnete als öffentliche Stellen eingeordnet werden können. Gemäß der Auffassung der 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), die die Vorgaben der Datenschutzgrundverordnung beachten müssen (https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/HandreichungDSGVOFuerAbgeordnete.pdf?__blob=publicationFile&v=2) . 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.

Praxisfrage: Kann ein MdB eine private Sammlung von Bürgerdaten anlegen, für die nicht die Regelungen des Datenschutzrechts gelten ?

→ wenn zu rein persönliche oder familiäre Zwecken Daten gesammelt werden, gelten die Maßgaben des Datenschutzrechts nicht)

→ wenn Daten für Wahlkampfzwecke gesammelt oder genutzt werden, so wird der private Bereich verlassen.

Beispiel: Werden Adressen des persönlichen Freundes- und Bekanntenkreises auch nur einmal für eine Direktwerbeaktion zugunsten eines Dritten zur Verfügung gestellt oder genutzt, so entfällt die Ausnahme. Der konkrete Werbezweck ist dabei unerheblich; eine gewerbliche Produktwerbung fällt genauso darunter wie der Hinweis auf die erwünschte Unterstützung wohltätiger Organisationen oder kommunaler Anliegen. Jegliche nach außen gerichtete, über den persönlichen und familiären Kreis hinaustretende Tätigkeit verlässt den privilegierten Rahmen.

Die Nutzung einer persönlichen Datensammlung für andere Zwecke lässt den privaten Zweck entfallen. Dies gilt auch bei der Einwerbung von Spendengeldern für gemeinnützige Zwecke oder bei der Unterstützung politischer Anliegen.

Auf Landesebene ist zu beachten:

In den Bundesländern sind mögliche Bereichsausnahmen zu berücksichtigen, die für die Landesparlamente geschaffen wurden. So ist in § 2 Absatz 2 Datenschutzgesetz Brandenburg geregelt, dass der Landtag, seine Gremien, seine Mitglieder, die Fraktionen und Gruppen sowie deren Verwaltungen und deren Beschäftigte bei der Wahrnehmung parlamentarischer Aufgaben nicht den datenschutzgesetzlichen Bestimmungen sondern einer Datenschutzordnung des Landtages unterliegen. Diese Geschäftsordnung des Brandenburgischen Landtags berücksichtigt die Grundsätze der DSGVO und greift einzelne Regelungen wieder auf, z.B. das Auskunftsrecht der Betroffenen gemäß § 7 Geschäftsordnung. Allerdings sind keine Regelungen bezüglich eines Datenschutzbeauftragten enthalten, sondern es finden sich Bestimmungen zur Datenschutzkontrolle, die dem Präsidium obliegt.

In den Bundesländern Sachsen und Thüringen ist die Rechtslage ähnlich. So ist in § 2 Absatz 6 Datenschutzgesetz Thüringen geregelt, dass die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag sowie der parlamentarischen Tätigkeit der Abgeordneten einschließlich der Fraktionen nicht den datenschutzgesetzlichen Bestimmungen unterliegt, sondern einer gesonderten Datenschutzordnung des Landtages. Entsprechendes gilt gemäß § 2 Absatz 1 Datenschutzgesetz Sachsen. Allerdings sind in diesen beiden Bundesländern bislang noch keine Geschäftsordnungen verabschiedet worden, sondern es liegen seitens der Fraktionen entsprechende Anträge vor. Im Freistaat Sachsen wurde ein solcher Antrag seitens der CDU-Fraktion und SPD-Fraktion eingebracht (DRUCKSACHE 6/17608, http://edas.landtag.sachsen.de/viewer.aspx?dok_nr=17608&dok_art=Drs&leg_per=6).Im Antrag der Fraktionen DIE LINKE, der SPD und BÜNDNIS 90/DIE GRÜNEN zur Datenschutzordnung des Thüringer Landtags ist darüber hinaus die Aussage zu finden, dass Fraktionen als freiwillige Zusammenschlüsse von Abgeordneten rechtsfähige Vereinigungen

eigener Art und nicht Teil der öffentlichen Verwaltung sind (Drucksache 6/6822, http://www.parldok.thueringen.de/ParlDok/dokument/70117/datenschutzordnung_des_thueringer_landtags.pdf).

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