Datenschutz im Wahlkampf

Tipps zum richtigen Umgang mit personenbezogenen Daten März 2017

A. Allgemeine Grundsätze

1. Was sind personenbezogene Daten ? (§ 3a BDSG)
Alle Einzelangaben über persönliche oder sachliche Verhältnisse einer Person, d.h. alle Informationen, die eine Verbindung zu einem bestimmten Menschen haben.

Besonders schutzbedürftig sind die sogenannten sensiblen Daten (§ 3 Abs. 9 BDSG). Zu diesen „besondere Arten personenbezogener Daten" zählen Gesundheitsdaten, Informationen über ethnische Herkunft oder über eine politische, religiöse, gewerkschaftliche oder sexuelle Orientierung. Ihre Verarbeitung ist an strengere Voraussetzungen gebunden als die Verarbeitung sonstiger personenbezogener Daten.

2. Grundsatz der Datenvermeidung & Datensparsamkeit (§ 3a BDSG)
→ Daten nur Sammeln und Behalten, wenn unbedingt notwendig für den Verwendungszweck (d.h. für die beabsichtigte Nutzung)

3. Erhebung beim Betroffenen und Informationspflichten (§ 4 BDSG + § 33 BDSG)
Daten sind direkt bei der Person, um die es geht, einzusammeln. Sie muss über den Vorgang informiert werden (§ 33 BDSG: „...die/der Betroffene ist zu Speicherung, Art der Daten, Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und zur Identität der verantwortlichen Stelle zu benachrichtigen"). Ausnahmen gibt es nur, wenn eine Rechtsvorschrift diese vorsieht oder die direkte Erhebung bei der Person unverhältnismäßigen Aufwand erfordert.

> <u>Beispiel:</u>
> Daten über die Parteizugehörigkeit, Telefonnummer etc. eines Betroffenen dürfen nicht bei Nachbarn erfragt werden.
> Sie müssen direkt bei der betroffenen Person erfragt werden.

4. Einwilligung (§ 4a BDSG)
Die Zustimmung zur Verarbeitung der die eigene Person betreffenden Daten muss auf freier Entscheidung des Betroffenen beruhen. Es darf kein Über-/Unterordnungsverhältnis vorliegen, sonst ist die Freiwilligkeit problematisch (etwa bei Arbeitnehmer/Arbeitgeber-Situation).

Wenn Personendaten zum Zweck des Wahlkampfes verarbeitet werden, dann muss der Betreffende darüber informiert sein und dieser Verarbeitung/Speicherung zustimmen.

Es braucht ausnahmsweise keine persönliche Zustimmung, wenn die zu sammelnden Daten bereits öffentlich/allgemein zugänglich sind (z.B. Telefonbuch; Internet) – diese Ausnahme gilt aber nicht, wenn die Daten nicht allgemein veröffentlich sind (z.B. auf öffentlicher website), sondern nur für einen bestimmten Zweck.

Beispiel:
Ein Handwerker gibt auf seiner homepage die Adresse seines Betriebes an

- Wahlwerbung darf per Post ohne besondere Einwilligung zugesandt werden

Gegenbeispiel:
Eine Bürgerin sucht per Aushang nach vermisstem Haustier und gibt Adresse an.

- Keine Wahlwerbung ohne Nachfrage zulässig; da Adresse nur für konkret eingegrenzten Zweck öffentlich gemacht

5. Datengeheimnis (§ 5 BDSG)

Die mit der Verwaltung von Personendaten Betrauten (z.B. Wahlkampfhelfende, die Adresslisten erstellen) müssen auf das sogenannte Datengeheimnis verpflichtet werden. Sie müssen die erlangten Personendaten geheim halten und dürfen z.B. nicht Adresslisten, die die Partei zusammengestellt hat, für eigene Zwecke verwenden oder mitnehmen.
Dies sollte schriftlich festgehalten werden um diese Verpflichtung ggfs. nachweisen zu können. Dazu können Vordrucke genutzt werden, durch welche Betraute auf das Datengeheimnis und zum Geheimhaltung (im Wahlkampf anzuraten) verpflichtet werden.

6. Notwendigkeit eines Beauftragten für Datenschutz/Meldepflicht (§ 4d, 4f BDSG)

Sofern mehr als 9 Personen mit der automatisierten Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten betraut sind, ist dies der Datenschutzaufsichtsbehörde des jeweiligen Bundeslandes zu melden oder ein Beauftragter für den Datenschutz zu bestellen.

7. Zulässigkeit des Datenumgangs nach Interessenabwägung (§ 28 BDSG)

Auch ohne eine Einwilligung der betroffenen Person kann die Verwendung der sie betreffenden Daten zulässig sein: Wenn die Verwendung zur Abwicklung eines Vertrages oder Geschäftsverhältnisses notwendig ist, wenn die Daten aus allgemein zugänglichen Quellen stammen (s.o.) oder wenn es zur Wahrung berechtigter Interessen der datenverwendenden Stelle (hier: der wahlkämpfenden Organisation) erforderlich ist.

Bei einer Interessenabwägung muss die politische Partei ihr Interesse, persönliche Daten für Wahlwerbung zu verwenden mit dem Interesse der Bürgerin/des Bürgers, keine Wahlwerbung zu erhalten, in einen Vergleich setzen. Werden dabei Gründe ersichtlich, dass die Interessen der Person überwiegen, dürfen die Daten nicht verwendet werden, ohne die Person um Erlaubnis zu fragen.

8. Rechte der betroffenen Person
(§ 33 Benachrichtigung / § 34 Auskunft / § 35 Berichtigung, Löschung, Sperrung)

Betroffene haben Anspruch auf Auskunft über die zu ihnen gespeicherten Daten (Welche Daten sind gespeichert und woher kommen sie ?) und zum Zweck der Speicherung (Warum und wofür wurden diese Daten gespeichert ?).
Es müssen also Maßnahmen getroffen werde, um solche Anfragen bearbeiten zu können und die notwendigen Löschungen durchführen zu können. Dies mag bei kleinen Kampagnen einfach sein, kann jedoch bei großen Datenbanken einen nicht unerheblichen Aufwand erzeugen.

9. Zweckbindung (§ 28 Abs.2 BDSG)

Bei der Erhebung personenbezogener Daten muss für diese ein konkreter Erhebungszweck festgelegt werden. Eine Nutzung außerhalb dieses Erhebungszweckes ist nur bei schon öffentlichen Daten zulässig, oder wenn keine Betroffeneninteressen dieser zweckfremden Nutzung entgegenstehen. Die Betroffeneninteressen sind meist höher zu gewichten, was der Absicht entgegensteht, die erhaltenen Daten ohne Einwilligung zu anderen als den ursprünglich vorgesehenen zu verwenden.

> Beispiel: Interessenten haben nur der Aufnahme der Kontaktdaten in die Adressdatei eines Ortsverbandes/Kreisverbandes zugestimmt, da sie über lokale/regionale politische Initiativen informiert werden wollen.
>
> - Weiterleitung der Kontaktdaten in eine zentrale Adressdatei auf Bundesebene zur beabsichtigten Ansprache zu anderen Themen ist dann zunächst unzulässig; es müsste eine Einwilligung eingeholt werden, oder man müsste im Rahmen einer Interessenabwägung (s.o.) zu dem – in der Beispiel-Konstellation möglichen – Ergebnis kommen, dass keine Interessen der Interessenten entgegenstehen.

10. Besonderheiten bei Minderjährigen

Ob Minderjährige ihre Datenschutzrechte schon alleine ausüben dürfen, hängt von ihrer Einsichtsfähigkeit ab. Dabei kommt es auf den Einzelfall an. Bei Internetkommunikation sind Alter und Einsichtsfähigkeit häufig gleichwohl schlecht einschätzbar. Datenschutzbehörden gehen jedenfalls davon aus, das unter 14 Jahren keine wirksame Einwilligung erteilt werden kann.
Nach dem ab Mai 2018 anzuwendenden Regelungen der EU-Datenschutz-Grundverordnung gilt eine absolute Untergrenze von 13 Jahren, unter der keine datenschutzbezogenen Erklärungen ohne Zustimmung der Erziehungsberechtigten gültig sind (Art. 8 Abs. 1 Satz 1 DSGV). Zwischen 13 und 16 Jahren sind eigenständige Zustimmungen der Kinder/Jugendlichen nur möglich, wenn die Dienstleistung sich nicht direkt an Kinder richtet – was wohl bei Wahlkampf-Angeboten wie politischen newslettern der Fall sein dürfte.

11. Besonderheiten für Abgeordnete und Wahlkampfhelfer

Im Datenschutzrecht gelten unterschiedliche Regelungen für öffentliche und private Stellen. Öffentliche Stellen sind hauptsächlich Behörden (was Abgeordnete und ihre Büros nicht sind). Auch sind MdB-Büros keine anderweitig öffentlich-rechtlich organisierte Einrichtungen wie etwa Körperschaften, Anstalten oder Stiftungen; sie nehmen keine hoheitlichen Aufgaben der öffentlichen Verwaltung wahr. Bundestagsabgeordnete sind auch keine sogenannten „Beliehenen", d.h. Privatsubjekte, die hoheitlicher Funktionen übernehmen, wie etwa Schornsteinfeger.

Mitglieder des Deutschen Bundestages sind datenschutzrechtlich als nichtöffentliche Stellen zu betrachten, für die das Datenschutzrecht Anwendung normale findet, sobald sie Daten nicht zu privat-persönlichen Zwecken, sondern für politische Zwecke verarbeiten oder nutzen.

Gegebenenfalls können Sonderregelungen wie etwa Datenschutzordnungen eines Landtages zu beachten sein. Dabei können Abgeordnete als Personen mit öffentlich-rechtlicher Funktion betrachtet werden. Innerhalb dieser Funktionen kann der Abgeordnete als Organ einer öffentlichen Stelle (etwa Bundestag oder Landtag) handeln und dann ausnahmsweise den Regelungen zu öffentlichen Stellen unterfallen. Beispiele wären etwa Ausschusssitzungen oder Petitionsvorgänge, bei der personenbezogene Daten in den Erkenntnisraum des Abgeordneten gelangen.

> 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 („Haushaltsausnahme", § 1 Abs. 2 Nr. 3 BDSG)
>
> → wenn Daten für Wahlkampfzwecke gesammelt oder genutzt werden, so wird der private Bereich verlassen und das gesamte private Datenschutzrecht findet Anwendung; um im Bereich der Ausnahme zu bleiben, müsste der private Datenumgang mit allen Bestandteilen und während der gesamten Dauer ausschließlich für persönliche oder familiäre Tätigkeiten erfolgen.

> 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.

Auch unter den neuen europäischen Vorgaben dient eine Verarbeitung von personenbezogenen Daten allein dann der Ausübung persönlicher oder familiärer Tätigkeiten, wenn sie ohne jeden Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird (ErwGr. 18 DSGVO). Als persönliche oder familiäre Tätigkeiten könnten auch das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netzwerke und Online-Tätigkeiten im Rahmen solcher Tätigkeiten gelten. 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.

12. 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 werden dürfen (zumindest wenn es sich um komplette IP Adressen handelt).

Exkurs: Aufgeweicht wurde diese Praxis durch die Entscheidung des EuGH aus 2016 in der Rechtssache C-582/14 (MdL (Piraten) Patrick Breyer vs. Bundesrepublik Deutschland).
Der EuGH stellte zunächst fest, dass IP-Adressen auch dann personenbezogenen Daten sind, wenn eine Feststellung der Identität des Nutzers nur auf Umwegen (etwa durch Anzeige und der damit verbundenen Anfrage an den Netzanbieter) möglich ist.

Der EuGH schränkte dann die eingangs erwähnte Regel der nur eingeschränkt zulässigen Nutzer-Verfolgung ein. Eine Speicherung müsse nicht immer auf die für die Nutzung der website unverzichtbaren Daten beschränkt sein. Es müsse vielmehr eine Interessenabwägung stattfinden, bei der die Interessen des Webseitenanbieters (etwa zur Abwehr von Angriffen auf die Webseite) mit den Interessen der Nutzer abgewogen werden müssen.

- Trotzdem ist zu empfehlen (zumindest wenn keine umfangreichen Angriffe auf die Webseite abzusehen sind), dass weiterhin eine Anonymisierung der IP-Adressen der die website Nutzenden vorgenommen wird, um Probleme früh zu vermeiden.
- Viele der modernen Webtraffic-Tools bieten die Möglichkeit datenschutzgerechter Analyse der Besucherströme und eine unnötige Speicherung komplett zu verhindern.

Die Datenschutzaufsichtsbehörden empfehlen dazu weitere Maßnahmen:

- Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Widersprüche sind wirksam umzusetzen.
- pseudonymisierte Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.
- personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

13. Weitergabe von Nutzerdaten zur Drittdatenverarbeitung

Häufig werden Personendaten auf Webseiten an Dritte weitergegeben, ohne dass der Nutzer dieser Weitergabe explizit zugestimmt hat - etwa wenn Datenanalysetools wie *Google Analytics* oder Zahlungsdienstleister wie *Paypal* auf den eigenen Webseiten eingebunden sind.

Es handelt sich um eine Datenübermittlung an Dritte, welche im Allgemeinen hohen Ansprüchen genügen muss. Besonders die meist fehlende Einwilligung und der kaum mögliche Nachweis, dass Betroffeneninteressen durch die Übertragung an Dritte nicht berührt werden, führen dazu, dass der Einsatz von Drittanbietersoftware (bzw. Scripts auf den Webseiten) zu weitreichenden Problemen und Verstößen gegen das Datenschutzrecht führt. Dies trifft auch zu, wenn eigene Webseiten auf Plattformen wie Facebook oder Google genutzt werden.
So ist es besonders problematisch, dass datenschutzrechtlich zweifelhafte und in den vergangenen Jahren häufig datenschutzrechtlich negativ aufgefallene Plattformen genutzt werden und durchaus kritische Personendaten wie die politische Ausrichtung mit Dritten geteilt werden. Meist wird dies über die AGB bzw. die Datenschutzerklärungen der Plattformanbieter gerechtfertigt und rechtlich abgesichert, jedoch werden auch diese häufig von Datenschutzaufsichtsbehörden bemängelt und sind häufig mit dem BDGS nicht vereinbar.

Aus Sicht des Wahlkämpfers ist zwar durchaus verständlich, dass weitverbreitete Plattformen wie Facebook genutzt werden müssen 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.

14. Datenverschlüsselung

Nach § 9 BDSG müssen technische und organisatorische Maßnahmen zum Schutz gesammelter Daten ergriffen werden. Das gilt für alle Daten, die sich auf Personen beziehen; es gibt nach dem Gesetz also grundsätzlich keine „belanglosen Daten“. Gleichwohl wird an dieser Stelle etwas abgestuft: Der für Schutz und Sicherung der Daten zu betreibende Aufwand ist am Schutzbedarf auszurichten. Für besonders sensible Daten muss daher 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 Transportverschlüsselung eingesetzt werden, um Verstößen und Mahnungen aus dem Weg zu gehen.
>
> - Am liebsten ist Datenschützern natürlich im Allgemeinen der umfassende Einsatz des https-Protokolls auf allen Webseiten der wahlkämpfenden Stelle, auch wenn umstritten ist, ob das nach dem geltenden Recht zwingend erforderlich ist. Es sollte hier auf Nummer sicher gegangen werden – zumal Aufwand und Kosten sich in Grenzen halten und ein sicherheitsbewusstes Image belegt wird.

15. 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).

Datenschutzrechtlich interessant ist in diesem Bereich vor allem, wie an die verwendeten Datensätze (mail-Adressen) gelangt wurde und ob/wie die Betroffenen darüber informiert werden. Dies ist aber eher eine theoretische Betrachtung, da für den Versender allein schon der unaufgeforderte Versand von Mails zu weitreichenden Problemen im Wettbewerbsrecht /Lauterkeitsrecht führen würde. Die Nutzung von Mailadressen, bei denen die Nutzer offensichtlich nicht zu deren Einsatz für Wahlmails zugestimmt haben (fehlerhafte Interessenabwägung + Verstoß gegen Zweckbindungsgrundsatz) macht ein solches Wahlwerbemittel dann nur noch „rechtswidriger“.

Dies muss gleichwohl nicht bedeuten, dass gar keine Wahlwerbemails verschickt werden könnten. Die Inhaber der Mail-Adressen müssen dem Empfang jedoch vorher zugestimmt haben und die Zweckbindung gewahrt werden.

Beispiel: Wenn mail-Adressen vom einem Interessenten für Information zum Kandidat A eingeholt wurden, so können sie nicht ohne weiteres von und für Kandidat B genutzt werden. Es muss zumindest eine Interessenabwägung durchgeführt werden.

- Wenn der Zweck, zudem ein Bürger seine mail-Adresse hergab, weit gefasst war (etwa „Wahlkampfinformation Partei A"), besteht mehr Freiheit, da die im Bespiel aufgeführten Kandidaten im Zweifel beide umfasst sind.
- 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 sollte 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.