



STUDIE PARTEIEN & DATENSCHUTZ

**– Datenschutzpraxis deutscher Parteien und
parteinaher Organisationen –**

September 2009

1. Update

Impressum

Herausgeber und Vertrieb
Xamit Bewertungsgesellschaft mbH
Monschauer Straße 12
40549 Düsseldorf
www.xamit.de

© Xamit Bewertungsgesellschaft mbH 2009

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotodruck oder in einem anderen Verfahren) ohne schriftliche Genehmigung des Herausgebers übersetzt, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Rechtlicher Hinweis

Alle innerhalb der Xamit-Studien genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Inhaltsverzeichnis

1	„DATENSCHUTZ“ EINE GRETCHENFRAGE AN UNSERE PARTEIEN.....	1
2	PARTEIEN UND DATENSCHUTZ.....	3
2.1	Parteien formen den Datenschutz.....	3
2.2	Untersuchte Parteien und Stiftungen.....	5
3	SPENDEN SAMMELN IM INTERNET.....	6
4	DATENSCHUTZ IM INTERNET	12
4.1	Webstatistiken und Nutzerhinweis.....	12
4.2	Einbindung von Kontaktformularen	14
5	DATENSCHUTZVERSTÄNDNIS VON PARTEIEN	17
5.1	Zentrum des Datenschutzes: das Verzeichnissesverzeichnis.....	17
5.2	Verzeichnissesverzeichnis? Haben wir nicht!	19
6	HÄUFIGE IRRTÜMER UND WISSENSLÜCKEN	22
7	FAZIT	26
8	WEITERE STUDIEN VON XAMIT ZUM THEMA DATENSCHUTZ.....	29

1 „Datenschutz“ eine Gretchenfrage an unsere Parteien

Hätte Gretchen aus Goethes „Faust“ in unserer Zeit gelebt, würde sie mit Sicherheit im Internet surfen. Als Surferin wäre sie in Wahlzeiten mit vielen Foren und Spendenaufrufen unserer Parteien in Berührung gekommen. Bestimmt wären dabei sogar persönliche Daten von ihr registriert worden.

Unter diesem Aspekt hätte sie ihre vor 200 Jahren gestellte Frage nach einem Bekenntnis zur Religion vermutlich durch die Frage an die Parteien ersetzt:

„Wie hältst Du es als Partei selber mit dem Datenschutz?“

Basis unserer Untersuchung ist diese „moderne“ Form der Gretchenfrage.

Die CDU/CSU ist für „Datenschutz mit Augenmaß“¹ und sagt weiterhin in ihrem Wahlprogramm zur Bundestagswahl 2009, dass der Bürger darauf vertrauen können muss, „dass seine Daten vor Missbrauch geschützt sind.“² Die Grünen verlangen in ihrem Bundestagswahlprogramm sogar die Verankerung des Datenschutzes als Bürgerrecht im Grundgesetz³ und außerdem, dass derjenige, der Daten sammelt und mit ihnen arbeitet, einen streng geschützten Umgang mit ihnen nachweisen muss.⁴

45% aller Bürger nutzen das Internet, um sich über politische Themen zu informieren. Bei den 18-29 Jährigen sind es 77%.⁵ Deutsche Parteien folgen dem Trend aus den USA und Obamas Wahlkampf 2008, in dem sie zunehmend das Medium des Internet für ihre (Wahlkampf)Zwecke einsetzen. Die Profile namhafter Parteipolitiker findet man in sozialen Netzwerken wie StudiVZ und Facebook, deren Videobotschaften und Fotos bei YouTube oder Flickr. Die Wahlkampfseite der CDU beispielsweise, teAM2009.de, verlinkt auf Flickr, YouTube, Twitter, MeinVZ, StudiVZ, SchülerVZ, MySpace, Facebook, Wer-kennt-wen und CDU TV.

Das Internet spielt im Wahlkampf eine immer wichtigere Rolle

Neben der Selbstdarstellung ist Spendensammeln ein weiterer Fokus der Online-Aktivitäten. Dies bringt zwangsläufig auch eine Speicherung persönlicher Daten von Spendern mit sich. Darüber hinaus hinterlassen Besucher auf Webseiten und in Social Networks wie StudiVZ Datenspuren (z.B. betrachtete Profile oder geschriebene Beiträge), die Begehrlichkeiten wecken.

¹ Bundesvorstand der CDU, Parteivorstand der CSU: Wir haben die Kraft – gemeinsam für unser Land. Regierungsprogramm 2009-2013. 28.06.2009, S. 81.

² Ebd.

³ Bündnis90/Die Grünen: Der grüne Gesellschaftsvertrag. Klima, Arbeit, Gerechtigkeit, Freiheit. 8. -10.05.2009, S. 145.

⁴ Ebd., S. 147.

⁵ BITKOM (2009): BITKOM Pressekonferenz Studie zu E-Democracy. URL: http://www.bitkom.org/files/documents/BITKOM_Praesentation_PK_E-Democracy_19_08_2009_final.pdf. Letzter Zugriff: 2009-08-20.

Die Parteien prägten und prägen das Datenschutzniveau in Deutschland. Über ihre Abgeordneten im Bundestag und in den Landtagen beeinflussen sie die Datenschutzgesetzgebung, wählen die Datenschutzbeauftragten des Bundes und der Länder und beeinflussen die Mittelausstattung der Aufsichtsbehörden über die jeweiligen Haushalte (Kapitel 2).

Mit der vorliegenden Untersuchung versucht Xamit, eine empirische Antwort auf die Frage zu finden, wie ernst die Parteien den Datenschutz in der Praxis wirklich nehmen. Dazu untersuchten wir drei Aspekte:

1. Die Abwicklung von Online-Spenden (siehe Kapitel 3): Welche Möglichkeiten bieten Parteien, online zu spenden? Wie sicher sind diese Verfahren?
2. Den Umgang mit personenbezogenen Daten im Internet (siehe Kapitel 4): Wie legen Parteien ihren Besuchern offen, welche Daten erhoben werden und was mit diesen geschieht?
3. Das Vorhandensein von Grundlage für datenschutzkonformes Handeln (siehe Kapitel 5): Verfügen die Parteien über ein Verzeichnisverzeichnis?

In Kapitel 6 gehen wir auf ausgewählte Antworten ein. Das Fazit zieht Kapitel 7. Eine Erläuterung der wichtigsten Datenschutzbegriffe finden Sie auf Seite 25.

Mit der vorliegenden Studie dokumentiert Xamit, wie Parteien Datenschutz praktisch leben. Lassen Sie sich überraschen!

2 Parteien und Datenschutz

Kapitel 2.1 zeigt auf, wie Parteien sowohl die Datenschutzgesetze als auch die Kontrollen durch die Aufsichtsbehörden maßgeblich prägen. Welche Institutionen wir in der vorliegenden Studie befragt haben, beschreibt Kapitel 2.2.

2.1 Parteien formen den Datenschutz

Auf den ersten Blick erscheint der Einfluss von Parteien auf den Datenschutz in Deutschland gering. Doch der Eindruck täuscht (Abbildung 1): Abgeordnete des Bundestags und der Landtage gehören fast ausnahmslos einer Partei an und sind damit auch der Partei- und Fraktionsdisziplin unterworfen. Sowohl Bundestag als auch Landtage erlassen – vereinfacht dargestellt – Gesetze mit Datenschutzbezug. Diese Gesetze bestimmen das Datenschutzniveau, das der Gesetzgeber wünscht.

Parteien prägen das Datenschutzniveau in Deutschland

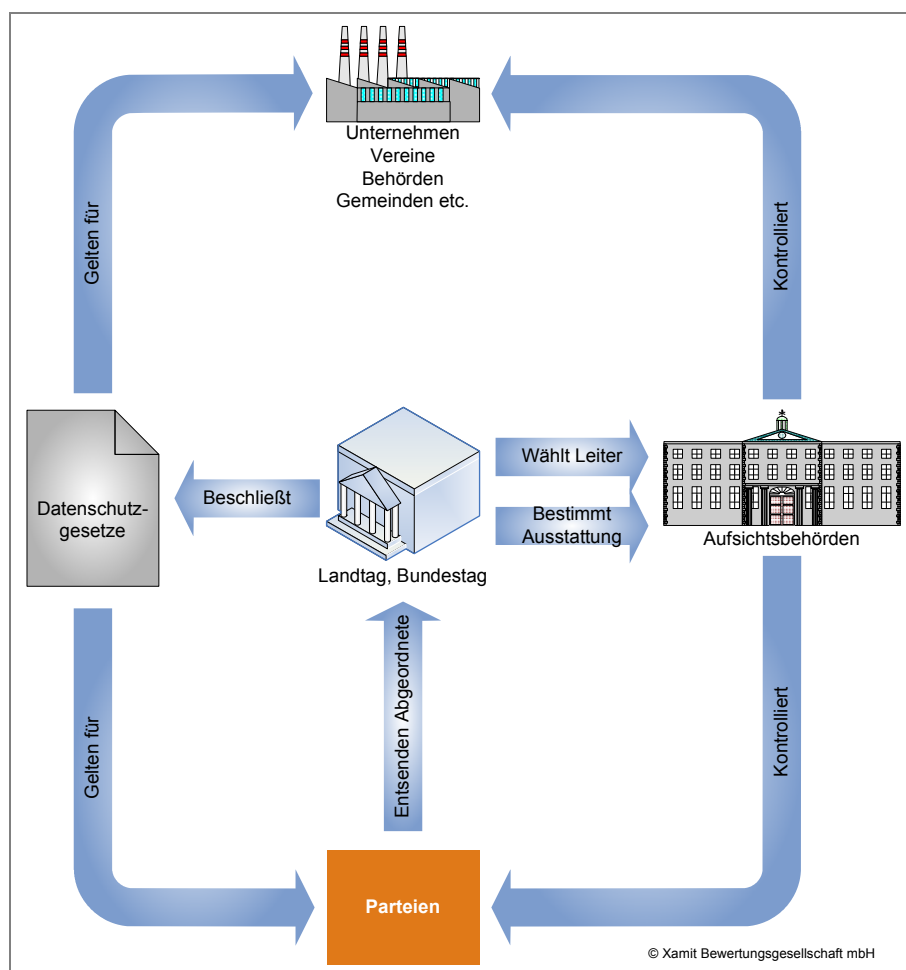


Abbildung 1: Parteien beeinflussen Gesetze und Aufsichtsbehörden (vereinfachte Darstellung, Ablauf ist bundeslandabhängig)

Um den Datenschutzgesetzen Nachdruck zu verleihen, überwachen Aufsichtsbehörden die Ministerien, Gemeinden, Unternehmen, Vereine und natürlich auch die Parteien. Die Ausstattung der Aufsichtsbehörden legen Bundestag und Landtage durch die Mittelausstattung fest. Je geringer diese ausfällt, desto weniger Kontrollen der Gesetze sind faktisch möglich. Etliche Gesetzesverstöße bleiben so ungeahndet. Die Einflussnahme der Parteien ist sogar noch unmittelbarer. Der Bundesdatenschutzbeauftragte und die Landesdatenschutzbeauftragten werden auf Zeit von den zuständigen Parlamenten gewählt und sind als Leiter der jeweiligen Aufsichtsbehörde für die Datenschutzkontrolle von Ministerien, Behörden und anderen öffentlichen Einrichtungen verantwortlich. In einigen Bundesländern kontrollieren die Landesdatenschutzbeauftragten auch nicht-öffentliche Stellen, wie Parteien, privatwirtschaftliche Unternehmen und Vereine. Wenn Datenschutzbeauftragte zu engagiert die Datenschutzbelange von Bürgern vertreten, können sie dadurch ihre Wiederwahl gefährden.⁶

Über ihre Abgeordneten bestimmen Parteien also einerseits die Datenschutzgesetzgebung mit und legen andererseits das Kontrollniveau der Aufsichtsbehörden fest.

⁶ Vgl. die Debatte um die Wiederwahl von Dr. Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) in Heise Online (2009): Debatte um Datenschutzposten in Schleswig Holstein. URL: <http://www.heise.de/newsticker/meldung/print/135605>. Letzter Zugriff: 2009-08-07.

2.2 Untersuchte Parteien und Stiftungen

Um den Umgang von Parteien mit dem Datenschutz zu untersuchen, betrachten wir verschiedene Parteiorganisationen und bekannte parteinahe Stiftungen. Denn Parteien sind mit Stiftungen und anderen parteinahen Organisationen durch vielfältige personelle Verflechtungen verbunden und profitieren von deren Arbeit. Neben der Bundesebene untersuchten wir auch die Landesverbände von Brandenburg, Nordrhein-Westfalen, Saarland, Sachsen und Thüringen. Parteinahe Organisationen, wie die „Mittelstands- und Wirtschaftsvereinigung der CDU/CSU“, die von zwei Parteien getragen werden, rechneten wir der größeren Partei zu. Damit ergibt sich folgende Teilnahme (Tabelle 1 und Tabelle 2):

Tabelle 1: Teilnehmende Organisationen nach Parteizugehörigkeit

Partei	Anzahl Organisationen
SPD	10
CDU	13
CSU	2
FDP	9
Die Grünen	7
Die Linke	7
Gesamt	48

Tabelle 2: Teilnehmende Organisationen nach Organisationstyp

Organisationstyp	Anzahl Organisationen
Bundespartei	6
Landespartei	25
Stiftung	11
Parteinahe Vereinigung	6
Gesamt	48

3 Spenden sammeln im Internet

Online-Spenden stellen im aktuellen Bundestagswahlkampf 2009 eine wichtige Säule in den Online-Auftritten der Parteien dar. Neben reinen Geldspenden bieten Parteien an, Plakate für sie zu spenden. Hierbei bezahlt der Spender dafür, dass ein Plakat für eine gewählte Zeitspanne an einem, i.d.R. vom Spender gewünschten, Ort aufgestellt wird.

Bei Online-Spenden werden sensible persönliche Daten im Internet übertragen

Online-Spenden setzen voraus, dass sensible Daten, wie Kontonummern oder Kreditkartennummern, im Internet übertragen werden. Für die Erstellung der Spendenquittung sind außerdem die Daten des Spenders notwendig. Deshalb eignen sich Online-Spenden gut, um zu untersuchen, wie verantwortungsvoll Parteien mit den ihnen anvertrauten Daten umgehen. Parteien können also bereits beim Spendensammeln belegen, ob sie Datenschutz ernst nehmen.

Wir haben uns bei der Analyse auf die Bundesebene der sechs großen Parteien CDU, CSU, Die Linke, FDP, Grüne und SPD und deren Angebot, online zu spenden, beschränkt.

Klassische Spendenverfahren, wie Überweisung oder Scheck, betrachten wir hier nicht, da sie außerhalb des Internets stattfinden. Das von der SPD aktuell angebotene Spendentelefon bleibt ebenfalls unberücksichtigt.

Neben der Online-Spende gibt es signifikante Unterschiede, wie die Parteien die Adressdaten der Spender erheben: die FDP fragt bspw., ob der Spender Deutscher ist, die CDU verlangt die exakte Staatsbürgerschaft. Auf eine dedizierte Betrachtung, inwieweit die Verfahren der Parteien auch konform mit den Anforderungen an Parteispenden sind (siehe Gesetz über die politischen Parteien (PartG)), verzichten wir an dieser Stelle.

Tabelle 3 zeigt die zum Zeitpunkt der Erhebung angebotenen Möglichkeiten der Online-Spenden, die wir auf den Webseiten der Parteien gefunden haben. Drei Parteien offerieren die Bezahlung mit Kreditkarte, vier durch Lastschriftinzug und drei durch den Bezahlendienst PayPal.

Tabelle 3: Möglichkeiten online zu spenden⁷

Partei	Kreditkarte	Lastschrift	PayPal
SPD	✓	✓	
CDU	✓		
CSU			✓
FDP	✓	✓	✓
Die Grünen		✓	
Die Linke		✓	✓
Gesamt	3	4	3

Die drei Bezahlmethoden unterscheiden sich danach, wie viele Dritt-Unternehmen mit der Abwicklung beauftragt werden (Abbildung 2). Eine Erlaubnis zum Lastschrifteinzug übermittelt die Partei oder Ihr technischer Dienstleister direkt an die Bank des Spenders zur Ausführung. Sowohl bei Kreditkartenzahlungen wie auch bei PayPal wird ein weiteres Unternehmen einbezogen. Wer sein PayPal-Konto mittels Kreditkarte ausgleicht, bezieht sogar zwei Unternehmen mit ein. Zahlungen via PayPal werden immer über die USA abgewickelt. Dies kann – je nach Unternehmen – auch bei Kreditkartenzahlungen der Fall sein. Damit können US-Behörden Einblick in Spenden an deutsche Parteien erhalten. PayPal ist eine Tochter von eBay. Wer mit PayPal zahlt, vertraut seine Daten letztlich eBay an. Keine der untersuchten Parteien weist bei der Bezahlung mittels PayPal auf die Datenübermittlung in die USA hin!

Bei Zahlungen über PayPal können US-Behörden Einblick in Spenden an deutsche Parteien erhalten.

Solange eine Partei mehrere Möglichkeiten der Bezahlung anbietet, hat ein Online-Spender eine Wahlmöglichkeit gemäß seiner Datenschutzinteressen. Vorausgesetzt er kennt und versteht die genannten Zahlungswege. Die CSU bietet durch die Beschränkung auf PayPal keine Auswahlmöglichkeit bei der Online-Spende.

⁷ Zeitpunkt der Erhebung 10. bis 17. August 2009 über die Webseiten der Parteien

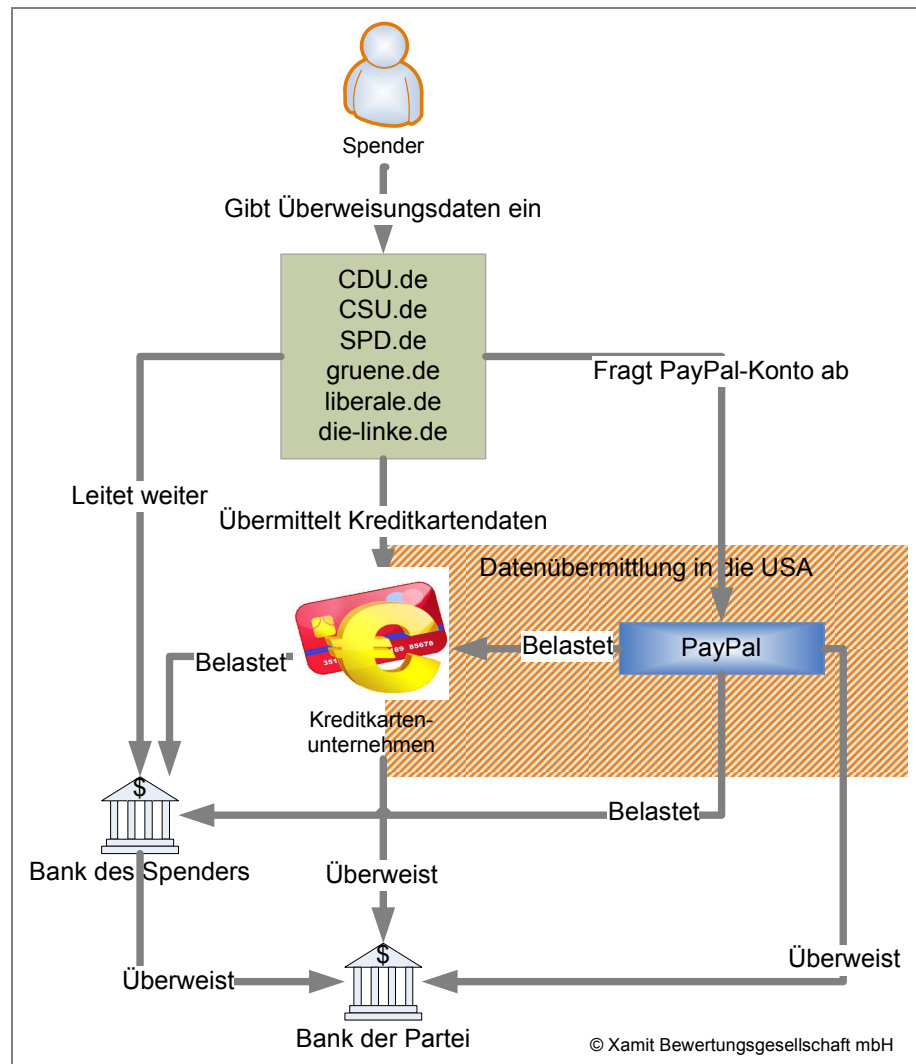


Abbildung 2: Datenströme bei Online-Spenden (vereinfacht dargestellt)

Unverschlüsselte Daten lassen sich leicht ausspähen

Wenn sensible Daten, wie Kontodaten oder Kreditkartennummern, online übermittelt werden, sollten diese verschlüsselt werden. Unverschlüsselte Daten lassen sich leicht ausspähen. Wer die Kreditkartendaten ausspäht, kann ohne weiteres auf Kosten des Spenders einkaufen gehen oder dessen Konto räumen. Parteien,

- denen das Wohlergehen ihrer Spender am Herzen liegt und
- die gesetzeskonform (siehe § 9 Anlage BDSG) handeln wollen,

Vor Phishing-Angriffen können erweiterte Zertifikate schützen

verschlüsseln die übertragenen Daten z.B. mit SSL. Eine Verschlüsselung sichert jedoch nur den Transport der Daten ab. Sie kann nicht garantieren, dass der Empfänger authentisch ist. Für einen besseren Schutz vor Phishing-Angriffen wurden erweiterte Zertifikate („EV-SSL-Zertifikat“) eingeführt, die in der Adresszeile des Browsers den Namen des Zertifikatsinhabers oft grün hinterlegt anzeigen. Stimmt der Inhaber deutlich nicht mit der Webseite überein, ist Vorsicht geboten.

Tabelle 4 zeigt, welche Parteien verschlüsseln und welche ein erweitertes Zertifikat verwenden.

Tabelle 4: Verschlüsselte Übertragung der Bezahlenden

Partei	Kreditkarte Lastschrift	Verschlüsselte Übertragung	Erweitertes Zertifikat
SPD	✓	(✓)	
CDU	✓	✓	✓
CSU	-/-	-/-	-/-
FDP	✓	✓	
Die Grünen	✓	✓	✓
Die Linke	✓	✓	
Gesamt	5	5	2

Die Grünen und die CDU handeln vorbildlich, indem sie verschlüsseln und dem Spender mit Hilfe eines erweiterten Zertifikats anzeigen, dass die Webpräsenz authentisch ist. Die FDP und die Linke verschlüsseln zwar, verzichten aber auf eine Authentizitätsanzeige. Die Linke überträgt zudem Daten für Plakatspenden unverschlüsselt und gefährdet so ihre Spender. Die CSU überlässt die Absicherung PayPal.

Nur CDU und Grüne handeln beim Übertragen der Daten im Internet vorbildlich

Die SPD verhält sich höchstem Maße unverantwortlich gegenüber ihren Spendern. Dem technischen Laien verspricht sie eine Sicherung nach dem Stand der Technik. Eine dem Stand der Technik entsprechende Sicherung ist eine SSL-verschlüsselte Datenübertragung. Diese scheint aber nicht aufgebaut zu werden (Abbildung 3), tatsächlich werden die Daten für den Spender unsichtbar verschlüsselt übermittelt. Allerdings nicht an die SPD. Weil die SPD die Spendenzahlung über einen externen Dienstleister abwickeln will, ohne dessen Identität offenzulegen, bindet sie die Webseiten des Dienstleisters per „iFrame“ ein. Ein Spender merkt deshalb nicht, dass seine Finanzdaten gar nicht an die SPD übermittelt werden, sondern an die „infin – Ingenieurgesellschaft für Informationstechnologien mbH & Co. KG“. Diese Technik wird sonst von Kriminellen eingesetzt, um Finanzdaten auszuspähen, während der Besucher glaubt auf seiner Bankseite zu sein.

Die SPD setzt eine Technik ein, die auch von Kriminellen benutzt wird, um Finanzdaten auszuspähen

Für Plakatspenden gibt die SPD den Dienstleister an. Die SSL-Verschlüsselung bleibt aber auch hier verborgen, da die gleiche Technik wie bei den allgemeinen Spenden angewendet wird. Spender haben deshalb auch hier keine Möglichkeit, die Identität der empfangenden Webseite zu überprüfen. Nicht nur Banken und die meisten Onlineshops, sondern auch die CDU und Die Grünen sind hier beim Thema Datensicherheit deutlich weiter.

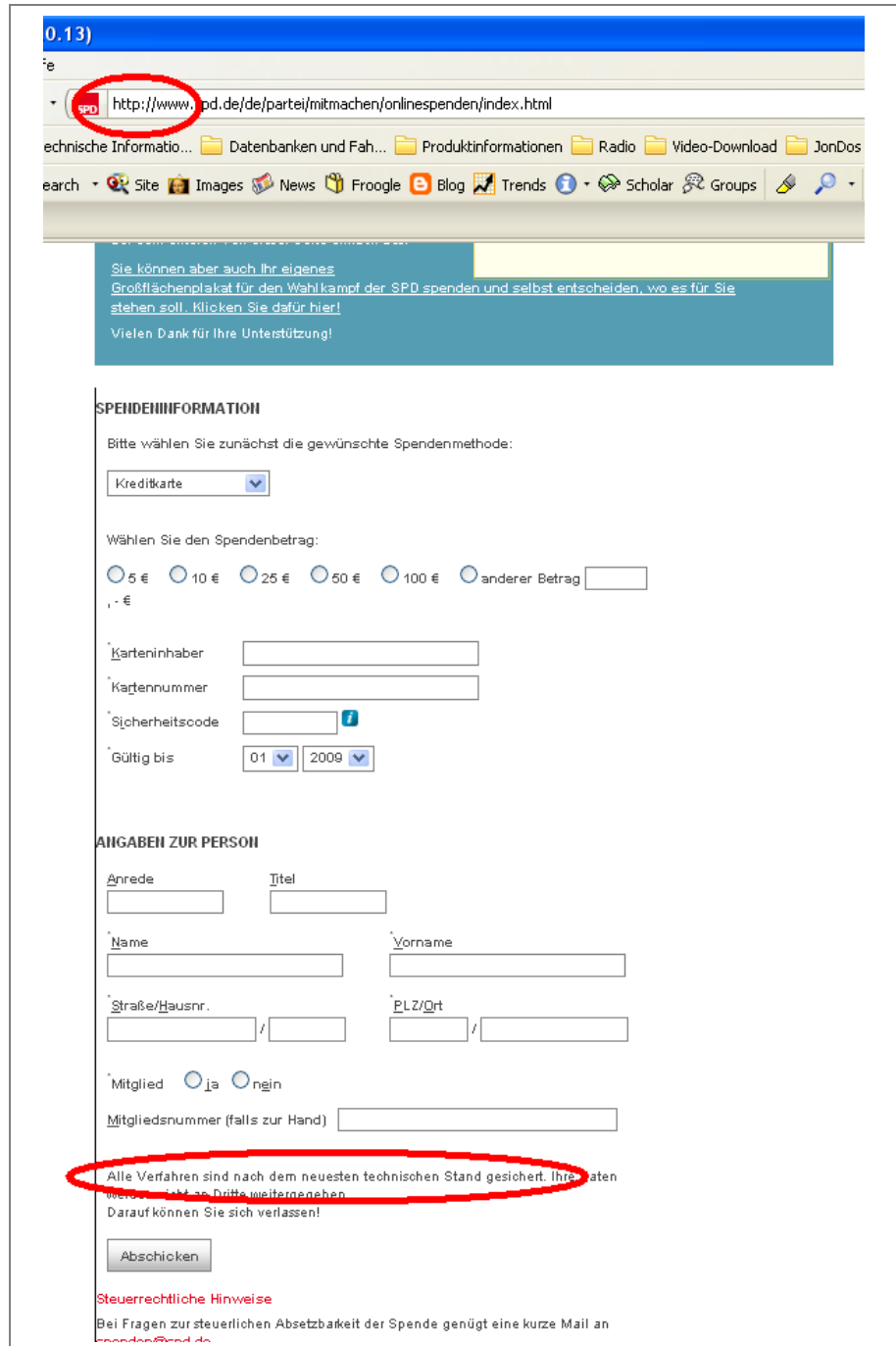


Abbildung 3: Gebrochenes Versprechen einer sicheren Datenübertragung⁸

SPD verweist auf nicht mehr existierende Gesetze

Die Datenschutzerklärung für Plakatspenden rundet dann das Bild vom Datenschutz der SPD ab: In ihrer aktuellen Datenschutzerklärung verweist die SPD im Abschnitt „4. Sonstiges“ auf das nicht mehr existente Teledienststedatenschutzgesetz (TDDSG) (Abbildung 4). Bereits 2007 ersetzte der Bundestag aber unter maßgeblicher Betei-

⁸ URL: <http://www.spd.de/de/partei/mitmachen/onlinespenden/index.html>. Letzter Zugriff: 2009-08-19.

ligung der mitregierenden SPD das TDDSG durch das Telemediengesetz (TMG).

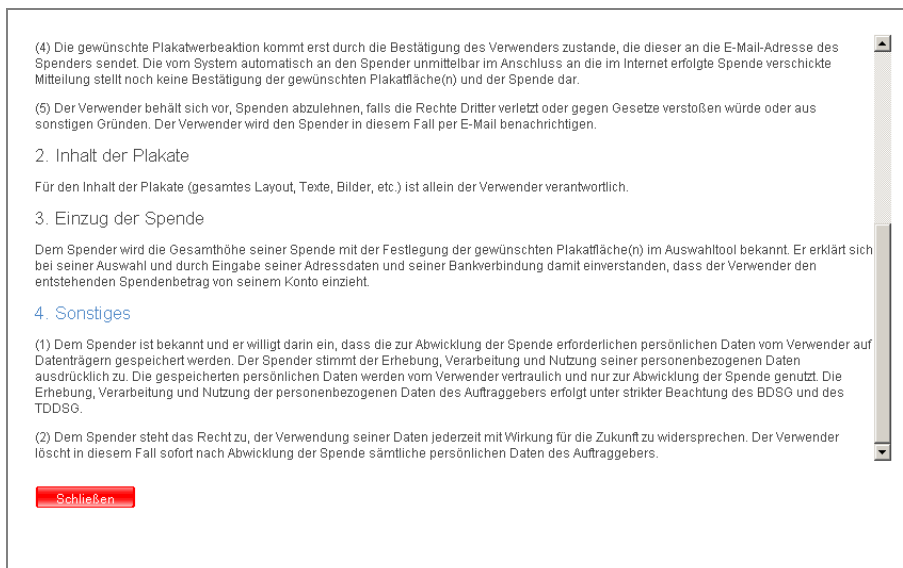


Abbildung 4: SPD-Datenschutzerklärung seit 2007 veraltet⁹

⁹ URL: https://contrast-plakatshop.de/bund/Doing_support/hinweis.php#datenschutz. Letzter Zugriff: 2009-08-19.

4 Datenschutz im Internet

Maschinelle
Quellcodeanalyse der
Webpräsenzen

Eine maschinelle Quellcode-Analyse der Webpräsenzen von Parteien und parteinahen Organisationen bildet die Grundlage, um den Umgang mit personenbezogenen Daten im Internet zu untersuchen. Analysiert wurden jeweils maximal 1.000 Webseiten pro Webpräsenz. Hierbei wurde untersucht,

- ob und welche Webstatistiken erstellt werden (Kapitel 4.1) und
- ob Kontaktformulare vorhanden sind (Kapitel 4.2).

Ist eine
Datenschutzerklärung
vorhanden?

In diesem Zusammenhang wurde auch das Vorhandensein von Datenschutzerklärungen geprüft. Dies geschah durch eine Suche nach charakteristischen Worten („Datenschutz“, „Zweck“ usw.) die gewöhnlich in Datenschutzerklärungen auftauchen. Sie bildeten die Entscheidungskriterien dafür, welche Webseiten über eine Datenschutzerklärung verfügen und welche nicht. Die Reihenfolge der Worte ist dabei irrelevant. Welche Regelungen in einer Datenschutzerklärung enthalten waren, blieb aus methodischen Gründen unberücksichtigt.

4.1 Webstatistiken und Nutzerhinweis

Wer eine Webpräsenz betreibt, investiert (viel) Zeit und Geld. Unternehmen und auch Privatpersonen wollen deshalb wissen, ob dieses Geld wirklich produktiv und effizient investiert wird. Eine Erfolgskontrolle von Webseiten ist deshalb für wirtschaftlich arbeitende Organisationen genauso unverzichtbar wie für Unternehmen. Mit Hilfe von Webstatistiken – auch Web Tracking, Web Analytics oder Webcontrolling genannt – messen Unternehmen das Verhalten ihrer Besucher. Entweder erstellt ein externer Dienstleister, Webstatistiken oder der Webseitenbetreiber wertet das Verhalten der Besucher auf seinem Internetangebot intern aus.

Webstatistiken
protokollieren das Verhalten
von Webseiten-Besuchern

Webstatistiken geben aggregierte Informationen über die Besucher von Webseiten wieder. Sie beantworten u.a. folgende Fragen:

- Über welche Wege betreten Besucher die Webpräsenz?
- Wie viele Besucher hat die Webpräsenz?
- Was unternehmen Besucher auf der Webpräsenz?

Jeder Statistikersteller bindet eine charakteristische Zeichenfolge in die überwachten Webseiten ein, um den Seitenaufruf protokollieren zu können. Diese Zeichenfolge ist ebenfalls auf allen überwachten Webseiten identisch. Kommt eine solche Zeichenfolge auf einer Webseite vor, wurde dies als Überwachung durch den zugehörigen Statistikersteller gewertet. Aus methodischen Gründen wurden ledig-

lich diejenigen Statistikersteller berücksichtigt, die eine eigene Datenerhebung durchführen. Logfile-Analysen¹⁰ blieben deshalb außen vor.

Google verlangt in § 8.1 seiner Nutzungsbedingungen¹¹, die Nutzung von Google Analytics an „prominenter“ Stelle des Webauftritts zu dokumentieren. Google legt den Wortlaut dieser Information fest und behält sich auch ein Kontrollrecht vor. Ob die von Google vertraglich vorgeschriebenen Formulierungen auf einer Webpräsenz, die Google Analytics nutzt, vorkommen, untersuchten wir ebenfalls.

Einhaltung der Nutzungsbedingungen wird überprüft

In unseren früheren Untersuchungen hatten wir Google Analytics als Marktführer ausgemacht.¹² In seiner Stellungnahme vom Januar 2009 wertet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) den Einsatz von Google Analytics in Deutschland als nicht mit dem deutschen Datenschutzrecht vereinbar, d.h. die Nutzung von Google Analytics auf deutschen Webpräsenzen sei illegal.¹³ Zu den Gründen zählen

Das ULD beurteilt den Einsatz von Google Analytics als illegal

- die Datenübermittlung in die USA,
- die ewige Datenspeicherung ohne Löschmöglichkeit und
- die Möglichkeit, durch Datenverknüpfung ein Nutzerprofil zu erstellen.

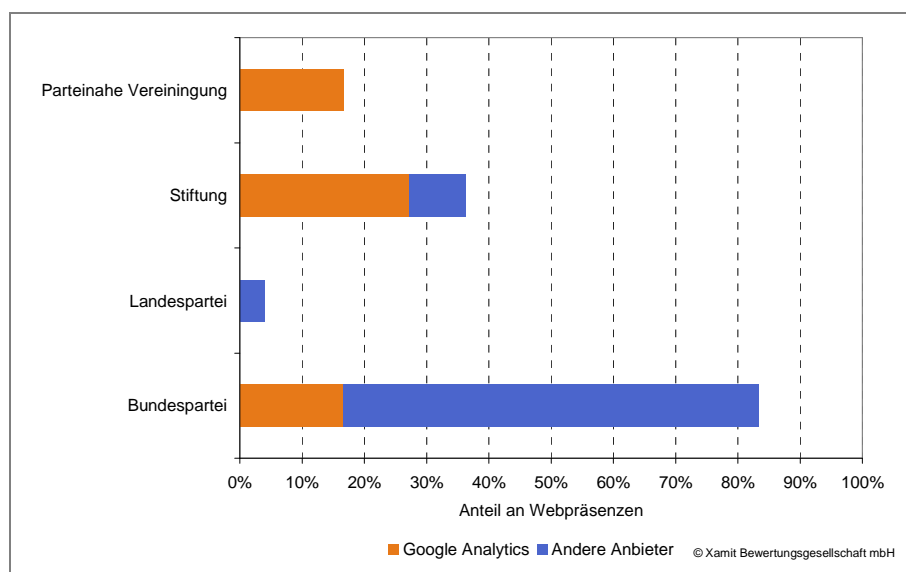


Abbildung 5: Nutzung von Webstatistiken nach Organisationen

¹⁰ Bei jedem Aufruf einer Webseite speichert der Webserver einige Angaben im so genannten Logfile. Anhand der Dateinamen, des Zeitpunkts und auch des Referers kann der Betreiber ein Bewegungsprofil erstellen.

¹¹ Google (2007): Google Analytics Bedingungen. URL: <http://www.google.com/analytics/de-DE/tos.html>. Stand: 2007-10-01.

¹² Xamit (2008): Datenschutzbarometer 2008 - Datenschutz im Internet. URL: <http://www.xamitleistungen.de/studienundtests/index.php>.

¹³ Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (2009): Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics. URL: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf. Letzter Zugriff: 2009-08-05.

Bis auf Die Linke nutzen Bundesparteien einen identifizierbaren Webstatistikanbieter (siehe Abbildung 5). Bei Landesparteien und parteinahen Vereinigungen konnte nur bei jeweils einer Webpräsenz ein Webstatistikanbieter entdeckt werden. 27% der Stiftungen verwenden Google Analytics und 9% einen anderen Anbieter.

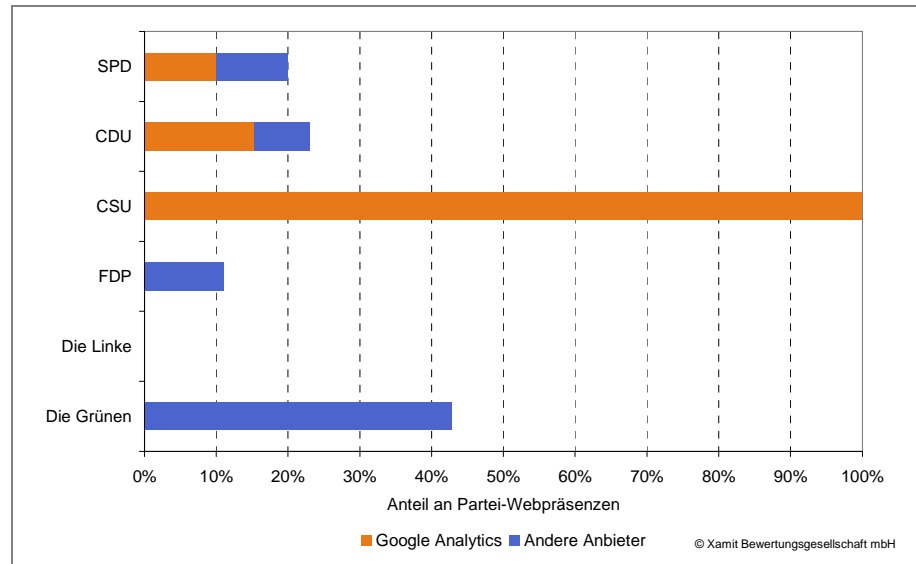


Abbildung 6: Nutzung von Webstatistiken nach Parteien

10% der untersuchten Webpräsenzen von Parteien und parteinahen Organisationen nutzen Google Analytics und 13% einen anderen Anbieter. Alle untersuchten und der CSU zugerechneten Webseiten nutzen Google Analytics (Abbildung 6).

Bis auf eine der CDU zugerechnete Webpräsenz besitzen alle übrigen Webpräsenzen mit Webstatistik eine Datenschutzerklärung.

Zwei Webpräsenzen verstoßen gegen die Nutzungslizenz von Google Analytics

Jeweils eine Webpräsenz mit Google Analytics, die wir der CDU und der CSU zugerechnet haben, verzichtet auf den vorgeschriebenen Passus aus der Lizenzvereinbarung mit Google. Dies ist ein klarer Verstoß gegen die Nutzungslizenz.

Hier zeigt sich ein klarer Trend: auf Bundesebene sind Webstatistiken stark verbreitet, während die Nutzung auf Landesebene stark abnimmt.

4.2 Einbindung von Kontaktformularen

Für jede Webpräsenz wurde untersucht,

- ob Eingabefelder personenbezogene Daten abfragen, z. B. bei Kontaktformularen,
- ob eine Datenschutzerklärung auf der Webpräsenz vorliegt,
- ob die Datenschutzerklärung einfach und mit maximal einem Klick vom Formular aus direkt erreichbar ist.

Dazu untersuchten wir maschinell den Quellcode jeder Webseite daraufhin, ob Formularfelder verwendet werden. Wenn wir ein Formularfeld fanden, analysierten wir seine Umgebung im Quellcode. Tauchten dort einschlägige Begriffe, wie „Vorname“, „Straße“ etc. auf, gingen wir davon aus, dass personenbezogene Daten abgefragt werden. Diese Methode ist nicht hundertprozentig fehlerfrei, doch eine manuelle Überprüfung zufällig ausgewählter Webpräsenzen zeigte nur minimale Fehlzuordnungen. Deshalb können wir auch diese Ergebnisse als ausreichend valide betrachten.

Umfang und Qualität der abgefragten Daten

Lediglich die Bundes-SPD gibt keine Datenschutzerklärung zu ihrem Kontaktformular an (Abbildung 7). Parteinahere Vereinigungen nutzen generell Kontaktformulare ohne Datenschutzerklärung. D.h. sie erläutern Besuchern, die das Kontaktformular verwenden, nicht, wie die erhaltenen Daten verwendet werden.

Viele Besucher bleiben über die Verwendung ihrer Daten im Dunkeln

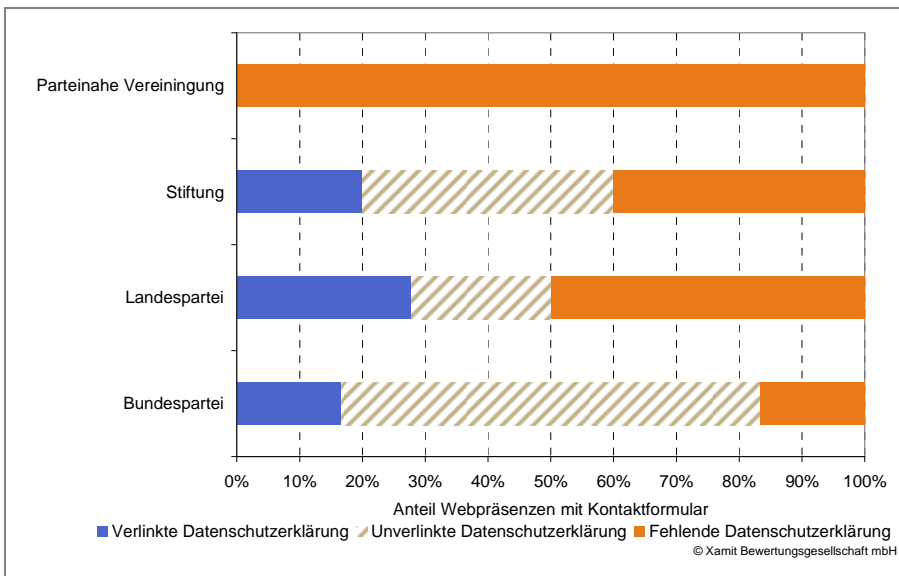


Abbildung 7: Nutzung von Kontaktformularen nach Organisationen

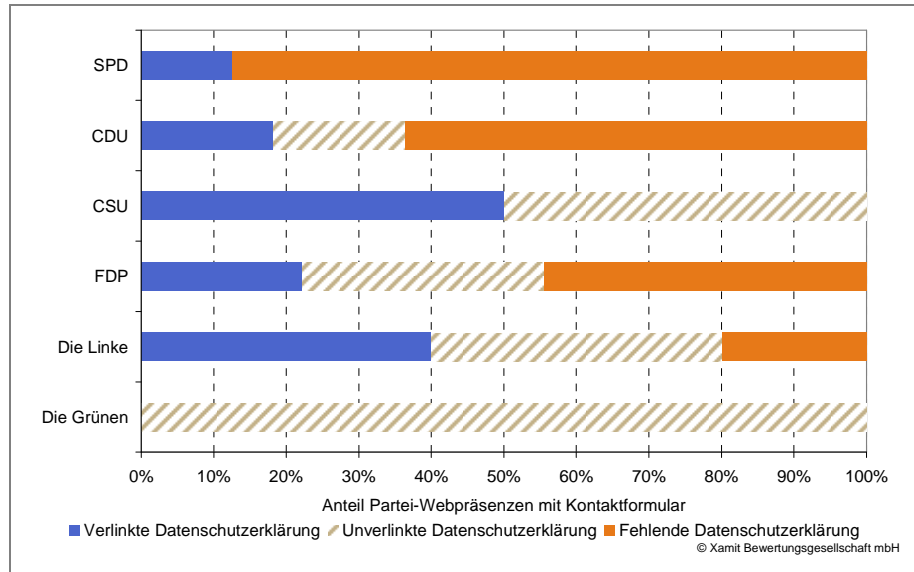


Abbildung 8: Nutzung von Kontaktformularen nach Parteien

Nur CSU und Grüne handeln bei Angabe der Datenschutzerklärung vorbildlich

Insgesamt verfügen 81% der untersuchten Webpräsenzen über ein Kontaktformular oder eine Bestellmöglichkeit für einen E-Mail-Newsletter. 21% der Webpräsenzen mit Kontaktformular verlinken direkt auf die Datenschutzerklärung, weitere 31% verfügen über eine nicht direkt erreichbare Datenschutzerklärung. Die restlichen 49% nutzen das Kontaktformular ohne Datenschutzerklärung. Die Grünen und die CSU sind die einzigen Parteien, die vorbildlich bei Kontaktformularen immer auch eine Datenschutzerklärung vorweisen (Abbildung 8).

5 Datenschutzverständnis von Parteien

Der Gesetzgeber sieht mit dem so genannten Verfahrensverzeichnis ein zentrales Arbeitswerkzeug vor, um Datenschutzrechte sicherzustellen und ihre Einhaltung zu kontrollieren (Kapitel 5.1). Kapitel 5.2 erläutert, wie Parteien mit diesem unverzichtbaren Arbeitsmittel umgehen.

5.1 Zentrum des Datenschutzes: das Verfahrensverzeichnis

Die Kontrolle des Datenschutzes wird durch drei miteinander verbundene Zentren wahrgenommen: Eigenkontrolle, Fremdkontrolle und Selbstkontrolle.

Die Eigenkontrolle verpflichtet die verantwortlichen Stellen zu größtmöglicher Transparenz bei der Datenverarbeitung. Sie schreibt vor, dass Betroffene, wie Interessierte oder Mitglieder, darüber informiert werden sollen, welche Daten über sie zu welchem Zweck verarbeitet werden. Dabei helfen drei Instrumente, die gesetzlich geforderte Transparenz herzustellen:

Eigenkontrolle verpflichtet zu Transparenz

- eine Information über die Datenverarbeitung,
- eine Datenschutzerklärung und
- ein Verfahrensverzeichnis.

Erst diese drei Instrumente zusammen versetzen jeden betroffenen Bürger in die Lage, seine Rechte auszuüben auf

- Auskunft: Wer hat was über mich gespeichert (§ 34 BDSG),
- Berichtigung: Korrektur falscher Angaben (§ 35 BDSG),
- Löschung und Sperrung: Falsche oder überflüssige Angaben (§ 35 BDSG),
- Widerspruch gegen die Datenverarbeitung.

Die Fremdkontrolle bildet das zweite Kontrollzentrum: Staatliche Aufsichtsbehörden kontrollieren, ob Daten ordnungsgemäß verarbeitet werden. Sie gehen auch Beschwerden von betroffenen Bürgern nach.

Fremdkontrolle soll durch staatliche Aufsichtsbehörden gewährleistet werden

Die Selbstkontrolle verpflichtet Unternehmen, Parteien und andere Organisationen, das eigene Handeln auf Datenschutzkonformität hin zu kontrollieren. Das BDSG sieht als betriebliche Kontrollinstanz den betrieblichen Datenschutzbeauftragten¹⁴ oder die Geschäftsleitung vor. Als Arbeitsgrundlage dient ein Verfahrensverzeichnis. Das Verfahrensverzeichnis beschreibt

Das Verfahrensverzeichnis dient als Arbeitsgrundlage der Selbstkontrolle

- den Zweck der Datenverarbeitung,
- die Rechtsgrundlage,

¹⁴ Bei Organisationen in denen mehr als neun Personen personenbezogene Daten automatisiert verarbeiten oder Einsicht in diese Daten haben, muss ein Datenschutzbeauftragter bestellt werden.

- wer die Daten verarbeitet,
- welche Daten verarbeitet werden,
- von wem Daten verarbeitet werden und
- wohin die Daten übermittelt werden.

Das öffentliche
Verfahrensverzeichnis darf
jedermann einsehen – ohne
Angabe von Gründen

Das Verfahrensverzeichnis gibt es in zwei Versionen (vgl. § 4e BDSG): Im öffentlichen Verfahrensverzeichnis stehen allgemeine Informationen darüber, welche Daten zu welchen Zwecken verarbeitet werden. Dieses muss jedermann auf Verlangen zugänglich gemacht (§ 4g Abs. 2 S. 2 BDSG). Das interne Verfahrensverzeichnis enthält sensible Informationen wie z.B. IT-Sicherheitsmaßnahmen und braucht außer an die Aufsichtsbehörde an niemanden herausgegeben zu werden.

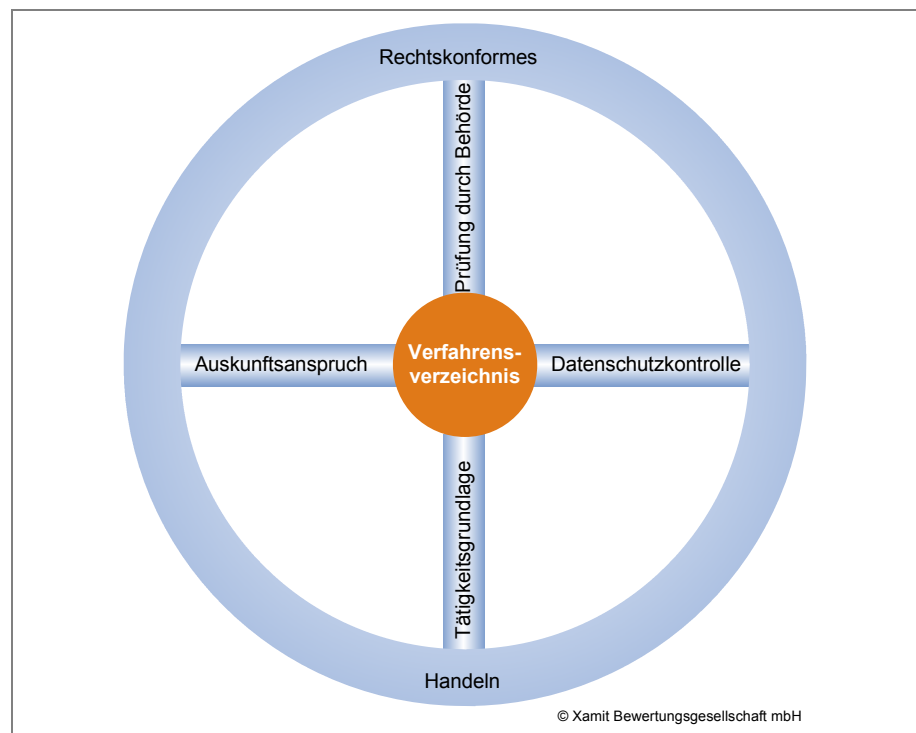


Abbildung 9: Verfahrensverzeichnis als Grundlage rechtskonformen Handelns

Kein Verfahrensverzeichnis,
keine Selbstkontrolle

Ohne ein Verfahrensverzeichnis fehlt einem Unternehmen oder einer Partei der Überblick, welche personenbezogenen Daten verarbeitet werden (Abbildung 9). In der Folge wird die Selbstkontrolle unmöglich, Auskunftersuchen können nur schwer beantwortet werden. Datenschutzverstöße sind vorprogrammiert.

Für alle, die sich ein öffentliches Verfahrensverzeichnis zulegen wollen, stellt die Gesellschaft für Datenschutz und Datensicherung e.V (GDD) ein Muster zur Verfügung.¹⁵

¹⁵ <https://www.gdd.de/nachrichten/news/das-verfahrensverzeichnis-fur-jedermann>. Unser Dank gilt der saarländischen FDP für den Hinweis.

5.2 Verfahrensverzeichnis? Haben wir nicht!

Eine Testperson hat per E-Mail an die im Impressum auf der Webseite angegebene Adresse bei jeder Partei, Stiftung oder parteinahen Vereinigung um die Zusendung des öffentlichen Verfahrensverzeichnisses gebeten. Die Zusendung konnte elektronisch oder postalisch erfolgen. Der Untersuchungszeitraum im Juli und August 2009 betrug knapp vier Wochen.

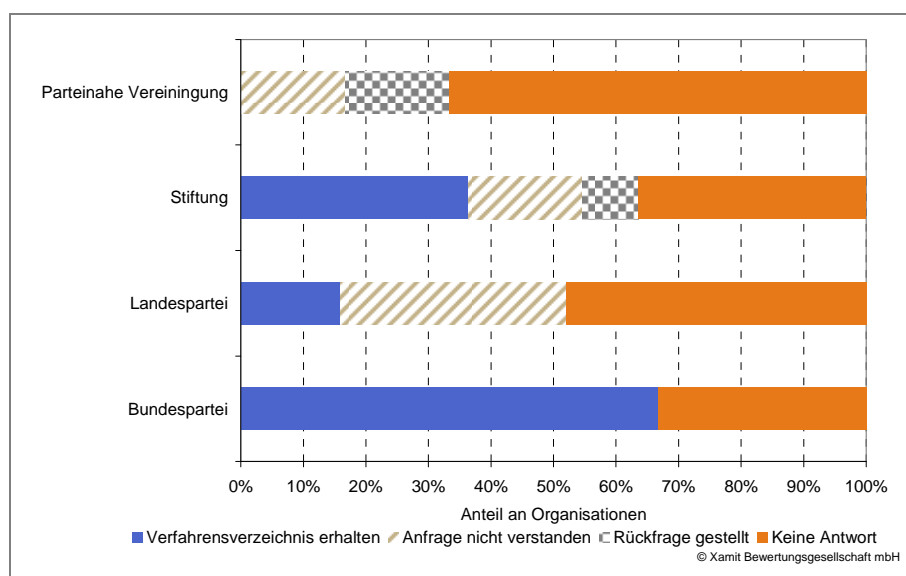


Abbildung 10: Reaktion auf Anfrage nach Verfahrensverzeichnis nach Organisationen

Zwei Bundesparteien reagierten auf unsere Anfrage nach einem Verfahrensverzeichnis überhaupt nicht (Abbildung 10). 36% der Stiftungen reagierten ebenfalls nicht.

Zwei Bundesparteien reagierten nicht auf die Anfrage

9% der Stiftungen stellten eine Rückfrage, 18% verstanden die Anfrage nicht. Landesparteien konnten noch seltener etwas mit unserer Anfrage anfangen. Lediglich 16% schickten ein Verfahrensverzeichnis zu. Parteinahe Vereinigungen sandten kein einziges Verfahrensverzeichnis zu oder boten eine andere Möglichkeit zur Kenntnisnahme an. Insgesamt stellten nur 25% der angeschriebenen Institutionen ein Verfahrensverzeichnis zur Verfügung.

Nur ein Viertel der Befragten schickte das Verfahrensverzeichnis

Das Angebot zur Einsichtnahme seitens der CDU werten wir ebenfalls als vorliegendes Verfahrensverzeichnis. Dabei haben wir zugunsten dieser Partei unterstellt, dass die Beschränkung auf eine Einsichtnahme in Berlin nur für unsere Untersuchung galt und nicht gängige Praxis ist. Das Verfahrensverzeichnis einer bayerischen Partei weckt erhebliche Zweifel an seiner Vollständigkeit, da die üblichen Verfahren einer Partei wie Interessentenwerbung oder öffentliche Veranstaltungen fehlen.

Insgesamt 25% der angeschriebenen Organisationen haben unsere Frage nicht verstanden oder ausweichend reagiert. An dieser Stelle

herzlichen Dank auch für die vielen erheiternden Begründungen, warum gerade die eigene Organisation nicht unter das Bundesdatenschutzgesetz fällt!

4% hatten Rückfragen und wollten eine Begründung für unser Interesse, obwohl für die Zusendung des öffentlichen Verfahrensverzeichnisses keine weiteren Angaben wie z.B. ein Rechtsgrund notwendig sind. Von diesen Organisationen haben wir bis heute kein Verfahrensverzeichnis erhalten.

Fast die Hälfte der Institutionen antwortete nicht

46% antworteten gar nicht erst. Zwei Parteien und ihnen nahe stehenden Institutionen haben kein Verfahrensverzeichnis zugesandt (Abbildung 11).

Zusammengefasst wurde dem Recht auf Einsicht in das öffentliche Verfahrensverzeichnis von 75% der Parteien und parteinahen Organisationen nicht Genüge getan.

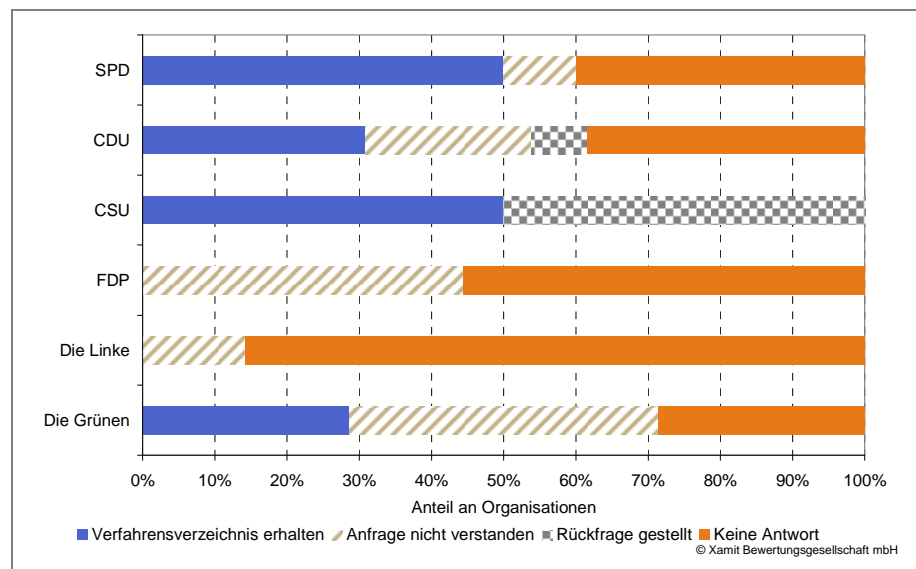


Abbildung 11: Reaktion auf Anfrage nach Verfahrensverzeichnis nach Parteien

Die Grünen aus NRW schickten eine nahezu beleidigende Antwort

Der Umgang mit unserer Anfrage wirft ein bezeichnendes Schlaglicht auf den Umgang einzelner Parteien mit Bürgeranfragen. Neben vielen Antworten, aus denen Unverständnis und Unwissen spricht (siehe Kapitel 6), erhielten wir sogar eine nahezu beleidigende Antwort, in der deutlich die Missachtung des Anfragenden zum Ausdruck gebracht wird (Abbildung 12): Die Grünen aus NRW schickten als Antwort einen Link zu dem Dienst „lass mich das für Dich Googlen“ (imgtfy.com). Dieser Dienst imitiert eine Google-Suche (Abbildung 13) und schließt mit der Bemerkung „War das so schwierig?“. Statt ihr eigenes Verfahrensverzeichnis zu versenden, wie es ihre gesetzliche Pflicht ist, machten die Grünen unsere Testperson lächerlich. Die imitierte Suche führte im Übrigen nicht zum Verfahrensverzeichnis der NRW-Grünen.

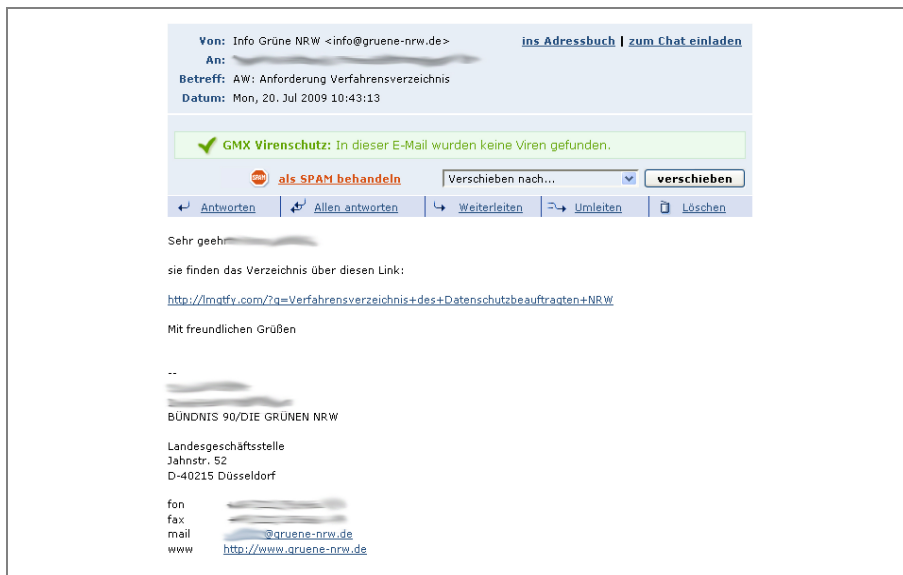


Abbildung 12: Antwort der NRW-Grünen ...



Abbildung 13: ... und das Ergebnis

Update: Frau Sabine Brauer, politische Landesgeschäftsführerin des Landesverbands NRW, entschuldigte sich am 3. September 2009 bei Xamit mit den Worten:

„[...] Es war aber keineswegs als eine absichtliche Herabsetzung gemeint, sondern – wie dargestellt – ein falsches Verhalten aufgrund einer falschen Einschätzung. Insofern handelt es sich um einen Fehler bei uns im Haus, für den wir uns entschuldigen möchten. [...]“

Wir sind beruhigt, dass es sich um einen Fehler handelt und nicht um die offizielle Position der NRW-Grünen.

6 Häufige Irrtümer und Wissenslücken

Unsere Anfrage nach einem Verfahrensverzeichnis hat einige Empfänger in sichtliche Verwirrung gestoßen. An dieser Stelle klären wir anhand der erhaltenen Antworten die häufigsten Irrtümer und Fehlvorstellungen auf:

„... Ihre Anfrage müssten Sie an den Datenschutzbeauftragten des Landes richten. ...“

Das ist nicht richtig. Jede verantwortliche Stelle, d.h. jede Partei, jedes Unternehmen, muss ein Verfahrensverzeichnis pflegen (vgl. § 4g Abs. 2a BDSG). Der Datenschutzbeauftragte des Landes ist zuständige die Aufsichtsbehörde für die öffentlichen Stellen, wie Ministerien. Je nach Bundesland ist der Datenschutzbeauftragte des Landes auch für die nicht-öffentliche Stellen, wie Unternehmen, verantwortlich. Zu seinen Aufgaben gehört die Kontrolle aber nicht die Pflege von Verfahrensverzeichnissen für Parteien und Unternehmen.

Wenn eine Anfrage nach einem Verfahrensverzeichnis an den Datenschutzbeauftragten des Landes ginge, dann wäre das eher in Form einer Beschwerde über das Fehlen eines Verfahrensverzeichnisses. Führt eine Partei oder ein Unternehmen kein Verfahrensverzeichnis, kann die Aufsichtsbehörde ein Bußgeld von bis zu 50.000 € verhängen.

„... Auf welche gesetzliche Grundlage berufen Sie sich und zu welchem Zweck erbitten Sie ein „Verfahrensverzeichnis“? ...“

Da die Anforderung eines Verfahrensverzeichnisses ein Jedermannrecht ist, kann nicht ernsthaft erwartet werden, dass ein Laie die verantwortliche Stelle, hier eine Partei, über die Rechtslage in Deutschland aufklärt. Zum Nachlesen: § 4g Abs. 2. S. 2 BDSG.

„... Ich bitte um Verständnis, dass wir bei der etwaigen Herausgabe derartiger Unterlagen sehr sorgfältig verfahren. ...“

Leider keine Chance. Das öffentliche Verfahrensverzeichnis ist auf Anfrage auszuhändigen (§ 4g Abs. 2. S. 2 BDSG). Doch keine Sorge, dort stehen keine sensiblen Informationen, wie z.B. IT-Sicherheitsmaßnahmen. Nur das interne Verfahrensverzeichnis enthält sensible Informationen und braucht nicht herausgegeben zu werden.

„... Leider verfügen wir über kein Verfahrnsverzeichnis. ...“

Dieses Eingeständnis bedeutet einen eindeutigen Verstoß gegen das BDSG. Da das Verfahrnsverzeichnis die Grundlage für datenschutzkonformes Handeln ist, stellt sich hier die Frage, ob eventuell weitere Gesetzesverstöße begangen wurden.

„... Es wäre hilfreich, wenn Sie uns noch mitteilen könnten, in welcher Beziehung Sie zu unserer Institution stehen, z.B. als Geschäftspartner. ...“

Warum? Diese Angaben haben keinen Einfluss auf das öffentliche Verfahrnsverzeichnis. Erst bei einem Auskunftsrecht sind sie hilfreich. Eine Auskunft wurde aber nicht erbeten.

„... Unser Aufnahmeantrag weist eine Datenschutzerklärung aus...“

Hervorragend. Eine Datenschutzerklärung ist jedoch kein Ersatz für das Verfahrnsverzeichnis.

„... Wir sind die XXX (Landespartei) und keine datenverarbeitende Stelle im Sinne des Datenschutzgesetzes. ...“

Das BDSG gilt für alle nicht öffentlichen Stellen unabhängig von ihrer Größe und Aufgabe, d.h. auch für Parteien und die öffentlichen Stellen des Bundes. Für die öffentlichen Stellen der Länder, z.B. Ministerien, gelten die Datenschutzgesetze der Länder. Einzig Familien fallen weder unter das BDSG noch unter die Datenschutzgesetze der Länder. Betrachtet diese Partei sich als Familie?

„... Als Institution haben wir andere Rechte und andere Zuständigkeiten und verfügen nicht über solch ein Verfahrnsverzeichnis. ...“

Stehen Parteien über dem Gesetz?

„... Um Einsicht in die einzelnen Verfahrnsverzeichnisse zu bekommen, sollten Sie sich an die jeweiligen Datenschutzbeauftragten der öffentlichen Stellen wenden. ...“

Mit ihrer Antwort hat sich diese Partei viel Mühe gegeben, da sie extra eine Anfrage bei der zuständigen Aufsichtsbehörde eingeleitet hat. Respekt und Kompliment für diesen Service! Liebe Partei, wir wollten doch ihr Verfahrnsverzeichnis einsehen und nicht das aller öffentlichen Stellen des Landes.

„... Leider verstehe ich nicht, was Sie wollen. ...“

Bedauerlich. Fehlt hier eine Datenschutzausbildung?

„... Nun ist XXX keine Gliederung, in der zehn oder mehr Menschen personenbezogene Daten einsehen oder bearbeiten können, deshalb haben wir leider auch kein Verzeichnis. ...“

Jede verantwortliche Stelle muss ein Verzeichnis führen – unabhängig von der Größe der Organisation

So einfach ist das nicht. Wenn kein Datenschutzbeauftragter bestellt werden muss, übernimmt die Geschäftsführung die entsprechenden Pflichten (§ 4g Abs. 2a BDSG):

„Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.“

Zu den Pflichten zählt auch, ein Verzeichnis, das in § 4e Satz 1 Nr. 1 bis 8 BDSG beschrieben ist, auf Antrag zur Verfügung zu stellen (§ 4g Abs. 2 S. 2 BDSG). Kurz: Die Unternehmensgröße schützt nicht vor datenschutzrechtlichen Verpflichtungen.¹⁶

¹⁶ Hinweis: Der Artikel „Verzeichnis“ auf Wikipedia mit Stand 2009-08-20 gibt den Sachverhalt falsch wieder. URL: <http://de.wikipedia.org/wiki/Verzeichnis>.

Wichtige Begriffe aus dem Datenschutzrecht

Personenbezogene Daten

§ 3 Abs. 1 BDSG: Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Name, Anschrift, Telefonnummer, Geburtsdatum, Auto-Kennzeichen, Kontonummer, Einkommen, Beruf, Hausbesitzer, Bewertungen und Werturteile, ...) In der Regel sind alle Daten personenbezogen, die sich auf einen bestimmten oder bestimmbarer Menschen zurückführen lassen.

Betroffener

§ 3 Abs. 1 BDSG: Eine natürliche Person, deren personenbezogene Daten durch eine „verantwortliche Stelle“ erhoben, verarbeitet oder genutzt werden. Da nur eine natürliche Person Betroffener sein kann (d.h. nur ein „Mensch aus Fleisch und Blut“), zählen juristische Personen (z.B. eine GmbH oder eine AG) nicht zu den Betroffenen. Ihre Daten werden vom Datenschutz nicht geschützt.

Verantwortliche Stelle

§ 3 Abs. 7 des BDSG: Jede natürliche oder juristische Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder die dies durch andere im Auftrag vornehmen lässt. In einem Konzern ist jede rechtlich eigenständige Gesellschaft eine eigene verantwortliche Stelle, auch wenn es sich um Tochterunternehmen handelt.

Öffentliche Stelle

§ 2 Abs. 1-3 BDSG: In erster Linie Behörden oder behördenähnliche Einrichtungen. Das sind Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der Länder und der Gemeinden.

7 Fazit

Parteien beeinflussen durch ihre Bundestags- und Landtagsabgeordneten das Datenschutzniveau in Deutschland maßgeblich:

- durch Gesetze und
- durch die Mittelzuweisung an die Datenschutzaufsichtsbehörden.

Kurz: Parteien bestimmen mit, was erlaubt und was verboten ist und legen gleichzeitig die Kontrolldichte fest. In Wahlkampfaussagen zeichnen sie zudem ein Bild des besorgten Bürgeranwalts.

Der Umgang mit Online-Spenden weckt daran zumindest Zweifel:

- Die CSU hat für Online-Spender ausschließlich die Nutzung von PayPal vorgesehen. Eine Übermittlung und Datenverarbeitung in den USA ist damit inbegriffen.
- Die FDP verzichtet auf erweiterte SSL-Zertifikate, d.h. ein Spender kann nicht sicher sein, dass die angezeigte Webseite authentisch ist.
- Die Linke überträgt sensible Finanzdaten wie Kontonummern bei Plakatspenden unverschlüsselt.
- Die SPD informiert ihre Spender nicht über den Empfänger der übermittelten Finanzdaten.

Darüber hinaus wurden folgende Praktiken festgestellt:

- Betrieb von Webstatistiken ohne Datenschutzerklärung,
- Einsatz von Google Analytics in Widerspruch zum BDSG und TMG,
- Kontaktformulare ohne Datenschutzerklärung und
- Fehlendes Verfahrensverzeichnis.

Wir haben diese wie folgt ausgewertet: Begeht eine Organisation alle vier Verstöße gegen datenschutzrechtliche Bestimmungen – die Spendenpraxis außen vorgelassen –, so werden diese auch vierfach gezählt. Die untersuchten 48 Organisationen konnten deshalb zusammen maximal 192 Verstöße begehen. 0% an Verstößen wäre gleichbedeutend mit gesetzeskonformem Handeln aller Organisationen des jeweiligen Typs. 100% an Verstößen wäre gleichbedeutend mit einer konsequenten Missachtung des Rechts durch alle Organisationen des jeweiligen Typs.

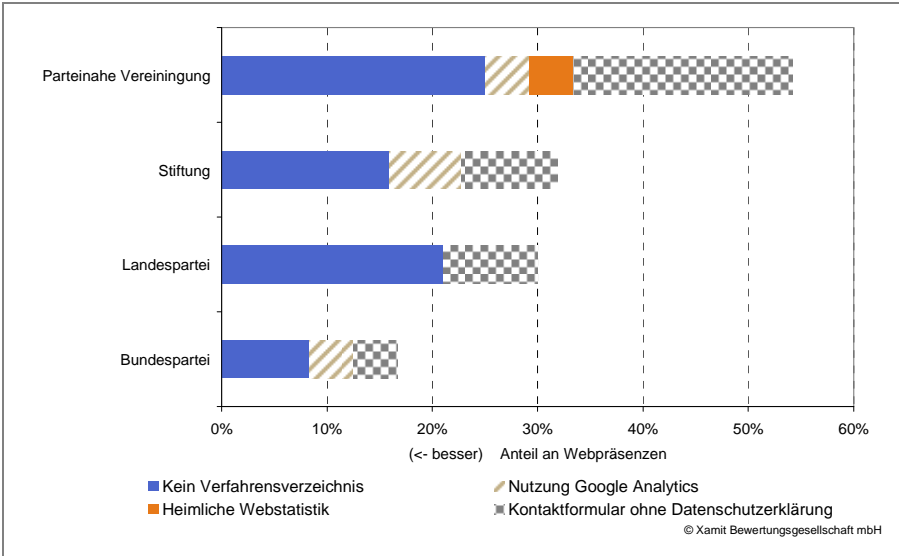


Abbildung 14: Anteil maximal möglicher Verstöße pro Organisation

Alle Organisationen zusammen begingen 32% der möglichen Verstöße. Abbildung 14 zeigt, dass die Verstöße bei Bundesparteien mit 17% im Vergleich gering ausfallen. Landesparteien und Stiftungen begingen 30% bzw. 32% der möglichen Verstöße. Parteinaher Vereinigungen schaffen sogar 54%. Jenseits der (Medien)-Aufmerksamkeit gedeihen Gesetzesverstöße anscheinend deutlich besser.

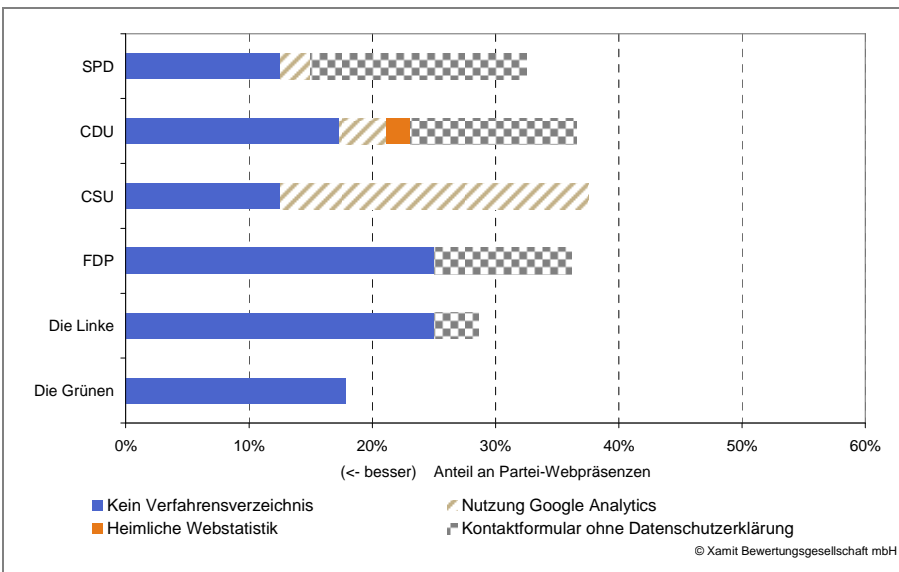


Abbildung 15: Anteil maximal möglicher Verstöße pro Partei

Spitzenreiter unter den Parteien sind die Volksparteien CDU (37%), CSU (38%) sowie die FDP (36%), dicht gefolgt von der SPD (33%) (Abbildung 15). Die Linke kommt auf 29% und die Grünen auf 18% möglicher Gesetzesverstöße.

Insbesondere die Antworten auf die Fragen unserer Testperson brachten eine weitverbreitete Unkenntnis datenschutzrechtlicher Be-

stimmungen bei den Parteien zu Tage. In etlichen Fällen war darüber hinaus eine deutliche Abwehrhaltung gegenüber legalen Auskunftsersuchen zu spüren.

Es liegt nahe, dass diese beiden Faktoren den Nährboden für die zahlreichen und vielfältigen Datenschutzverstöße bildeten.

8 Weitere Studien von Xamit zum Thema Datenschutz

Alle Studien und ausgewählte Fachbeiträge finden Sie als kostenlosen Download auf unserer Webpräsenz.¹⁷

Datenschutzbarometer 2008 – Datenschutz im Internet

Das Datenschutzbarometer 2008 stellt eine in dieser Form erstmalig durchgeführte Überprüfung von insgesamt 26.209 deutschen Internetpräsenzen dar. 45 von 100 Webseiten verstoßen gegen die gesetzlichen Bestimmungen oder weisen sonstige Indikatoren für ein mangelhaftes Schutzniveau auf.

Wie Unternehmen im Internet bei Konsumenten Misstrauen säen

Gut 85 Prozent aller Unternehmen und Behörden in Deutschland, die durch den Einsatz von Dialoginstrumenten personenbezogene Daten ihrer Website-Besucher sammeln, verzichten auf jegliche Information dahingehend, was mit diesen Daten geschieht. So lautet das Ergebnis einer repräsentativen Studie der Xamit Bewertungsgesellschaft mbH, bei der im Februar 2008 mehr als 815.000 Webseiten privater Firmen und öffentlicher Institutionen begutachtet wurden.

Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet

Wer protokolliert das Surfverhalten im World Wide Web? Wer ist Marktführer beim Web Tracking? Werden Besucher über eine Datenerhebung informiert? Wer kann technisch Bewegungsprofile mit Namen verknüpfen?

Beiträge in Fachmedien

Vertrauensvolle Datenverwendung: Basis des Geschäftserfolges. direkt marketing 5/2009

Umgang mit Datenschutzerklärungen im Internet. Datenschutz und Datensicherheit 1/2009

Vertrauensverlust beschert signifikante Umsatzeinbußen. IT-Sicherheit

Datenschutz bei Webstatistiken. Datenschutz und Datensicherheit 4/2008.

¹⁷ <http://www.xamit-leistungen.de/studienundtests/index.php>

Xamit Bewertungsgesellschaft mbH

Der IT-Spezialist für den Mittelstand – unabhängig, neutral, zuverlässig.

Unser Leistungsspektrum:

- **Xamit Firmen Check – Mit Sicherheit zum Erfolg.**
Beim Xamit Firmen Check nehmen wir Ihr Unternehmen fachmännisch unter die Lupe, analysieren die Sicherheit Ihrer IT-Systeme, zeigen Schwachstellen auf und erarbeiten mit Ihnen ein Konzept zur Optimierung Ihrer Sicherheit oder Ihres Datenschutzes.
- **Xamit Projekt Check – Rechnen Sie mit Erfolg.**
Der Xamit Projekt Check ist Ihre Versicherung für effizientes Arbeiten. Wir machen Ihre Software-Projekte transparent. Die Risiken werden kalkulierbar. Ihr Erfolg wird planbar.
- **Xamit Studien und Tests**
Wir bieten aktuelle Studien und Tests sowie weitergehende detaillierte Informationen zu IT-relevanten Themen.

Xamit-Leistungen stehen für begutachtete Kompetenz und Qualität: Das Unternehmen ist geprüftes Mitglied im Beraternetzwerk des IBWF Instituts e.V. und gehört darüber hinaus der Gesellschaft für Datenschutz und Datensicherung (GDD) sowie dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) an.

Ihre Vorteile mit Xamit

- Anerkanntes Fachwissen,
- Neutrale Beratung und
- Unabhängigkeit.

Setzen Sie nicht leichtfertig Ihr Unternehmen aufs Spiel. Sichern Sie Ihren Erfolg.
Rufen Sie uns an.

Xamit Bewertungsgesellschaft mbH

Zülpicher Str. 6
40549 Düsseldorf

Tel.: 0211 / 58 300 330
Fax: 0211 / 58 300 331

E-Mail: info@xamit.de
WWW: www.xamit.de