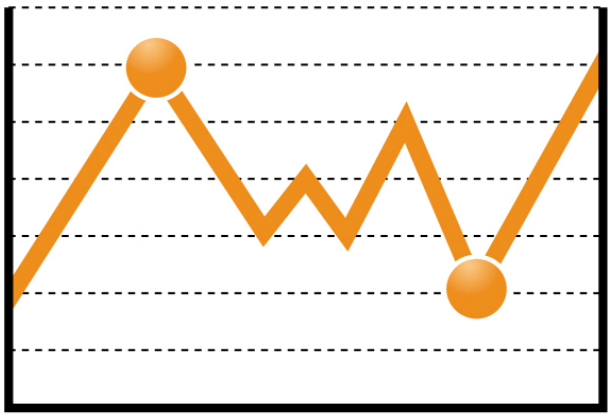
Datenschutzbarometer 2012

Papiertiger Datenschutz?



Datenschutz Barometer

Impressum

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

Rechtliche Hinweise

Inhaltsverzeichnis

1 EINLEITUNG 1

2 HINTERGRUND 2
2.1 Webshops 2
2.2 Webstatistiken 3
2.3 Internet-Werbung 4
2.4 Kontaktformulare 6
2.5 Social Plugins 7

3 GEGENSTAND UND METHODE DES DATENSCHUTZBAROMETERS 2012 9
3.1 Einbindung eines Webshops 10
3.2 Einbindung von Werbenetzwerken 10
3.3 Webstatistiken, Nutzer-Hinweis und Möglichkeiten zum Widerspruch 10
3.4 Einbindung von Kontaktformularen 11
3.5 Einbindung von Social Plugins 11

4 ERGEBNISSE 12
4.1 Risiko durch veraltete Software 12
4.2 Internetwerbung – Warum informieren? 13
4.3 Webstatistik – Der mühevolle Weg zum Licht 14
4.4 Kontaktformulare – Wer will schon Transparenz? 18
4.5 Social Plugins – Ungebremster Datenschutzverstoß 19

5 DAS XAMIT DATENSCHUTZBAROMETER 2012 21

6 AUSSTATTUNG UND ERFOLGE DER DEUTSCHEN DATENSCHUTZAUFSICHT 24
6.1 Personelle Ausstattung im Jahr 2012 24
6.2 Tätigkeiten und Erfolge 27
6.2.1 Datenschutzberatung und Eingaben im Jahr 2011 27
6.2.2 Kontrollen im Jahr 2011 29
6.2.3 Sanktionen im Jahr 2011 30
6.2.4 Erfolge im Jahr 2011 32

7 BETROFFENENAUSKUNFT: 29% BEANTWORTEN BRIEFE VOLLSTÄNDIG 34

8 FAZIT 37

9 ANHANG 39
9.1 Webseiten-Betreiber 39
9.2 Webseiten-Besucher 40

10 WEITERE STUDIEN VON XAMIT ZUM THEMA DATENSCHUTZ 42

11 BEITRÄGE VON XAMIT IN BÜCHERN UND FACHMEDIEN 44

1 Einleitung

Herzlich Willkommen zur fünften Ausgabe des XAMIT Datenschutzbarometers. Wir wollen dieses kleine Jubiläum für einen Rückblick nutzen. Beeinflusst durch Entwicklungen im Datenschutz, durch öffentliche und Fachdiskussionen haben wir das Datenschutzbarometer Jahr für Jahr ausgebaut und mit wechselnden Schwerpunkten versehen:

- 2008 startete das XAMIT Datenschutzbarometer mit der Messung des Datenschutzes im Internet. Seitdem begleitet es die Diskussion um Webstatistiken, insbesondere auch um Google Analytics.
- 2009 kam der Stellenspiegel deutscher Datenschutzaufsichtsbehörden hinzu. Zum ersten Mal wurde das Missverhältnis zwischen personeller Ausstattung und Auftrag öffentlich thematisiert.
- 2010 wurde der Facebook Like-Button eingeführt und hatte auch im Datenschutzbarometer sein Debut. Eine bis heute andauernde Auseinandersetzung zwischen Aufsichtsbehörden und Facebook nahm ihren Anfang. Der Like-Button stieg rasch zum populärsten und kontroversesten Social Plugin auf.
- 2011, dem Zäsurjahr der deutschen Datenschutzaufsicht, veröffentliche XAMIT zum ersten Mal statistische Angaben über die Tätigkeit der Aufsichtsbehörden. Diese Angaben waren teilweise unveröffentlicht oder über zahlreiche Tätigkeitsberichte verstreut.

Die vorliegende Ausgabe schließt methodisch und inhaltlich an unsere bisherigen Datenschutzbarometer an. Im diesjährigen Schwerpunkt untersuchen wir, wie mit dem Auskunftsrecht nach § 34 BDSG von Unternehmen umgegangen wird.

Das Barometer hat sich als Informationsquelle über das empirische Datenschutzniveau und die Datenschutzaufsicht in Deutschland etabliert. So berichteten bspw. SWR.de, heise online, Zeit online, acquisa und das Deutschlandradio über das Datenschutzbarometer.

Zwei Fragen werden uns immer wieder gestellt:

- Warum deckt das Datenschutzbarometer so wenige Datenschutzthemen ab? Viele Datenschutzthemen, wie z.B. Videoüberwachung, illegales Mitschneiden von Callcenter-Anrufen, lassen sich kaum oder nur mit großem Aufwand empirisch messen. Ohne empirisches Vermessen würde die Häufigkeit des Datenschutzverstoßes Spekulation bleiben. Mit dem Datenschutzbarometer möchte XAMIT jedoch die Debatte durch seine empirischen Untersuchungen versachlichen.
- Wer bezahlt das Datenschutzbarometer? XAMIT. Es gibt keinen Auftraggeber oder Sponsor für das Datenschutzbarometer. Ohne die Bereitschaft der Datenschutzaufsichtsbehörden, unsere umfangreichen Fragen zu beantworten, wäre das Barometer in der heutigen Form undenkbar. An dieser Stelle unseren herzlichen Dank dafür.

2 Hintergrund

Im Folgenden zeigen wir in knapper Form auf, an welchen Stellen und auf welche Weise persönliche Nutzerdaten durch Internet-Angebote erhoben werden. Sobald Daten erhoben werden, sind diese auch potentiell gefährdet. In Folge dessen droht ihr Missbrauch.

2.1 Webshops

Mit dem Begriff „Webshop“ werden Webseiten bezeichnet, die Waren oder Dienstleistungen zum sofortigen Online-Kauf anbieten. Dabei bestehen verschiedene Möglichkeiten, einen Webshop technisch zu realisieren. Auf die Feinheiten jeder Variante einzugehen sprengt den Rahmen der Studie. Deshalb skizzieren wir nachfolgend nur grob die generelle Funktionsweise.

Die einfachste Variante eines Webshops generiert eine E-Mail an den Betreiber, in der die bestellten Waren und der Besteller aufgeführt sind. Der Betreiber sorgt dann für die Auslieferung der Waren. Ein solcher Webshop nimmt keine Online-Abbuchungen vor und speichert keine Kundendaten, so dass Kundenkonten, mit denen der Bestellstatus eingesehen wird, fehlen. Kundendaten können folglich auch nicht aus dem Webshop gestohlen werden; wohl aber vom E-Mail-Server des Betreibers. Sicherheitslücken gefährden die Kundendaten deshalb nur im Moment des Bestellvorgangs. Ein nachträglicher Diebstahl aus dem Webshop scheitert an der fehlenden Datenhaltung.

Wesentlich anfälliger für Missbrauch und Diebstahl sind Webshops, die alle Kundendaten und Bestellungen direkt in Datenbanken beim Shop speichern. Solche Webshops bieten ihren Kunden Kundenkonten an, mit denen sie den Bestellstatus abfragen und ihre Kundendaten (Adresse, Zahlungsinformationen) verwalten können. Kreditkartenzahlungen sind ebenfalls möglich. Technisch nutzt diese Webshopklasse oft PHP, um die Shopsoftware auszuführen sowie eine dedizierte Datenbank, um die Artikel und Kundendaten zu speichern. Zur sicheren Aufbewahrung der Kundendaten ist es erforderlich, dass der Datenbankzugriff auf die Shopsoftware beschränkt bleibt. Die Shopsoftware ihrerseits darf die jeweiligen Kundendaten nur berechtigten Personen zugänglich machen. Andernfalls können sämtliche Kundendaten nachträglich aus der Datenbank ausgelesen und schlimmstenfalls gestohlen werden.

Die zuletzt skizzierte komplexe Variante zeigt auf, dass ein Webshop aus verschiedenen Computerprogrammen besteht. Dabei kommt mit PHP ein Programm zum Einsatz, das Skripte (kleine Programme) ausführt. Eine Shopsoftware wird demnach nicht direkt auf dem Server ausgeführt, sondern ist meistens in PHP geschrieben. Der PHP-Server führt die Shopsoftware in ähnlicher Weise aus wie ein Computer einen Browser ausführt.

Ein Webshop kann nur dann sicher sein, wenn PHP und die Shopsoftware keine Sicherheitslücken aufweisen. Grundvoraussetzung hierfür ist, dass am betreffenden PHP-Server, der Shopsoftware sowie der Datenbank entsprechende Sicherheitseinstellungen vorgenommen wurden. Diese Voraussetzung unterstellen wir in der weiteren Betrachtung als gegeben.

Sicherheitslücken kommen zudem durch Implementierungsfehler („Bugs“) oder Designfehler zustande. Keine nicht-triviale Software ist frei von Fehlern. Z. B. wurden in PHP Version 4.x.x für den Bereich MySQL-Datenbank 712 Fehler erfasst. Für die aktuelle Version 5.4 sind es bereits 14 Fehler.[1] Um die Sicherheit von Webshops zu gewährleisten, ist es sehr empfehlenswert, stets die aktuellen Programmversionen einzusetzen. Alternativ nutzen einige Hoster auch speziell abgesicher-

[1] Die Entwickler von PHP betreiben unter http://www.php.net/ eine Fehlerdatenbank. Stand der Abfrage: 2012-10-04.

te PHP-Versionen. Damit lässt sich durchaus ein angemessenes Sicherheitsniveau auch bei älterem PHP erreichen.

2.2 Webstatistiken

Wer eine Webpräsenz betreibt, investiert (viel) Zeit und Geld. Unternehmen und auch Privatpersonen möchten deshalb verständlicherweise wissen, ob dieses Geld wirklich produktiv und effizient investiert ist. Eine Erfolgskontrolle von Webseiten ist für einen wirtschaftlichen Betrieb folglich unverzichtbar. Mit Hilfe von Webstatistiken – auch Web Tracking, Web Analytics oder Webcontrolling genannt – messen Unternehmen das Verhalten ihrer Website-Besucher.

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?

Da aussagekräftige Auswertungen einer Website Fachwissen voraussetzen, nutzen Betreiber hierfür in aller Regel externe Dienstleister – im Folgenden Statistikersteller genannt. Ein Statistikersteller erhebt die entsprechenden Daten meistens selbst und generiert hieraus regelmäßige statistische Auswertungen für den Betreiber, welche nach Aufbereitung dann keinerlei Personenbezug mehr enthalten.

Bei einer eigenständigen Datenerhebung durch den Statistikersteller bindet der Betreiber in alle Webseiten Webpixel oder einen speziellen Skript-Code ein, der die Daten für den Statistikersteller sammelt und direkt an diesen sendet. Meistens werden zusätzlich Cookies eingesetzt. Welche Daten gesammelt werden, entscheidet und kontrolliert der Statistikersteller. Deshalb hat der Betreiber keine Kontrolle über Datenerhebung, Speicherung, Auswertung und weitere Nutzung der Daten.

Ein Beispiel: Max Mustermann surft verschiedene Webpräsenzen an. Der Betreiber kennt das Bewegungsprofil von Max Mustermann für seine eigene Webpräsenz. Weil ein Statistikersteller jedoch verschiedene Webpräsenzen betreut, besitzt er einen wesentlich umfassenderen Überblick über die Aktivitäten von Max. Je mehr Webpräsenzen also denselben Statistikersteller nutzen, desto umfangreicher, detaillierter und somit wertvoller wird dessen Datenbestand und Wissen über Max Mustermann.

Derartige personen- oder unternehmensbezogene Bewegungs- und Verhaltensprofile gehen über eine reine Website-Statistik weit hinaus und sind ungleich wertvoller, da sie weiter reichende Aussagen erlauben. Informiert sich ein Besucher bspw. auf den Webseiten einer Krankenkasse über eine bestimmte Krankheit, liegt die Vermutung nahe, dass er selbst (oder nahe Angehörige) an der recherchierten Erkrankung leidet. Sucht indes ein Unternehmen auf (universitären) Webseiten nach bestimmten Forschungsergebnissen und Veröffentlichungen, liegt die Vermutung nahe, dass es an einem ähnlichen Thema arbeitet.

Dem Interesse an Datentransparenz auf Seiten der Betreiber steht das Interesse nach Anonymität der Nutzer entgegen. Besucher und Unternehmen wollen Webseiten in der Regel unbeobachtet nutzen.

Eine ausführliche Analyse von Webstatistiken finden Sie in unseren Studien „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“ und „Webstatistiken im Test – Welcher

Dienst ist in Deutschland legal?“, 8. Update vom 04. Oktober 2011.[2] Auch wenn beide Studien schon etwas älter sind, sind sie inhaltlich noch aktuell.

Auf der rechtlichen Seite gibt es durch die EU-Richtlinie 2009/136/EG („Cookie Richtlinie“) vom 25. November 2009, die die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ändert, eine substantielle Neuerung. Art. 5 Abs. 3 2002/58/EG knüpft das Setzen eines Cookies zu Statistikzwecken an eine explizite Einwilligung des Besuchers.[3] Eine EU-Richtlinie muss durch die Nationalstaaten in Gesetze umgesetzt werden. Deutschland hat bisher die Richtlinie nicht umgesetzt. Es bleibt folglich unklar, wie die Einwilligung eingeholt werden kann oder muss (z.B. durch Checkbox oder Browsereinstellung). Formal gilt die alte Rechtslage weiter. Gerichte sind aber gehalten die bestehenden Gesetze gemäß der neuen Richtlinie auszulegen. Der Bundesbeauftragte für den Datenschutz will die Richtlinie in der Aufsichtspraxis anwenden.[4]

Ein Verzicht auf Cookies bedeutet nicht das Ende von Nutzungsprofilen und Webstatistiken. Die Erstellung der Profile wird lediglich aufwendiger, da statt eines Datums „Cookie-Inhalt“ mehrere Informationen wie z.B. Browser, Betriebssystem und installierte Schriften kombiniert werden müssten. Diese Informationen werden häufig bereits heute durch Webstatistiken abgefragt. Je mehr Informationen kombiniert werden, desto besser lassen sich Besucher eindeutig identifizieren.[5] Eine Demonstration zeigt das Forschungsprojekt „Panopticlick“ der Electronic Frontier Foundation.[6]

2.3 Internet-Werbung

Webseiten-Betreiber binden häufig Werbung in das eigene Angebot ein, um zusätzliche Einnahmen zu generieren. Typische Darstellungsformen dieser Werbung sind beispielsweise Banner oder Textanzeigen, die wiederum von Werbenetzwerken gestaltet und geliefert werden. Um zu verhindern, dass ein Besucher mehrfach die gleiche Werbung sieht und um nachzuvollziehen, welcher Besucher welche Werbung gesehen hat, setzen Werbenetzwerke Cookies ein oder nutzen ähnliche Techniken wie Webstatistikersteller (Kapitel 2.2).

Ein Beispiel: Sobald Max Mustermann eine Webseite besucht, die Werbung enthält, erfährt nicht nur der Webseitenbetreiber, sondern auch das Werbenetzwerk von seinem Besuch. Dabei sieht Max Mustermann der Werbung nicht unbedingt an, von welchem Unternehmen diese stammt und wer in Folge dessen von seinem Besuch erfährt. Deshalb ist er auf die Datenschutzerklärung des Webseitenbetreibers angewiesen.

Folgendes Beispiel illustriert, welche Unternehmen Webseitenbesuche registrieren, wenn Max Mustermann die 10 populärsten deutschen Webseiten aufruft. Dazu rufen wir hintereinander folgende Webseiten auf:

- Ebay.de
- wer-kennt-wen.de
- mobile.de
- wetteronline.de
- kicker.de
- Chefkoch.de

[2] Kostenfreier Download: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php
[3] EU Richtlinie 2009/136/EG vom 25. November 2009. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:De:PDF. Letzter Zugriff: 2012-010-04.
[4] Heise Online (2012): Schaar: Cookie-Regeln der EU gelten unmittelbar. 08.05.2012. URL: http://www.heise.de/newsticker/meldung/Schaar-Cookie-Regeln-der-EU-gelten-unmittelbar-1570745.html. Letzter Zugriff: 2012-010-04.
[5] Vgl. auch Schleipfer, Stefan (2010): Ist die IP-Nummer zu löschen – Eine Erörterung im Kontext von Nutzungsprofilen. In: Recht der Datenverarbeitung (RDV), 26. Jg, Heft. 4. S. 168-175.
[6] URL: http://panopticlick.eff.org/. Letzter Zugriff: 2012-10-05.

- Transfermarkt.de
- xing.de
- meinestadt.de
- stern.de

Diese wurden am 05.10.2012 von der IVW als die 10 populärsten Seiten nach inländischen Besuchen ausgewiesen. Berücksichtigt haben wir nur Einzelangebote.[7]

Das Firefox Addon „Collusion“[8] zeigt für die aufgerufenen 10 Webseiten an, welcher Werbedienstleister Werbung auf diesen Webseiten schaltet. Rote Punkte in Abbildung 1 zeigen Werbenetzwerke. Am Beispiel Google Display Network wird deutlich, dass Werbeunternehmen Besucher über Websites hinweg beobachten können.

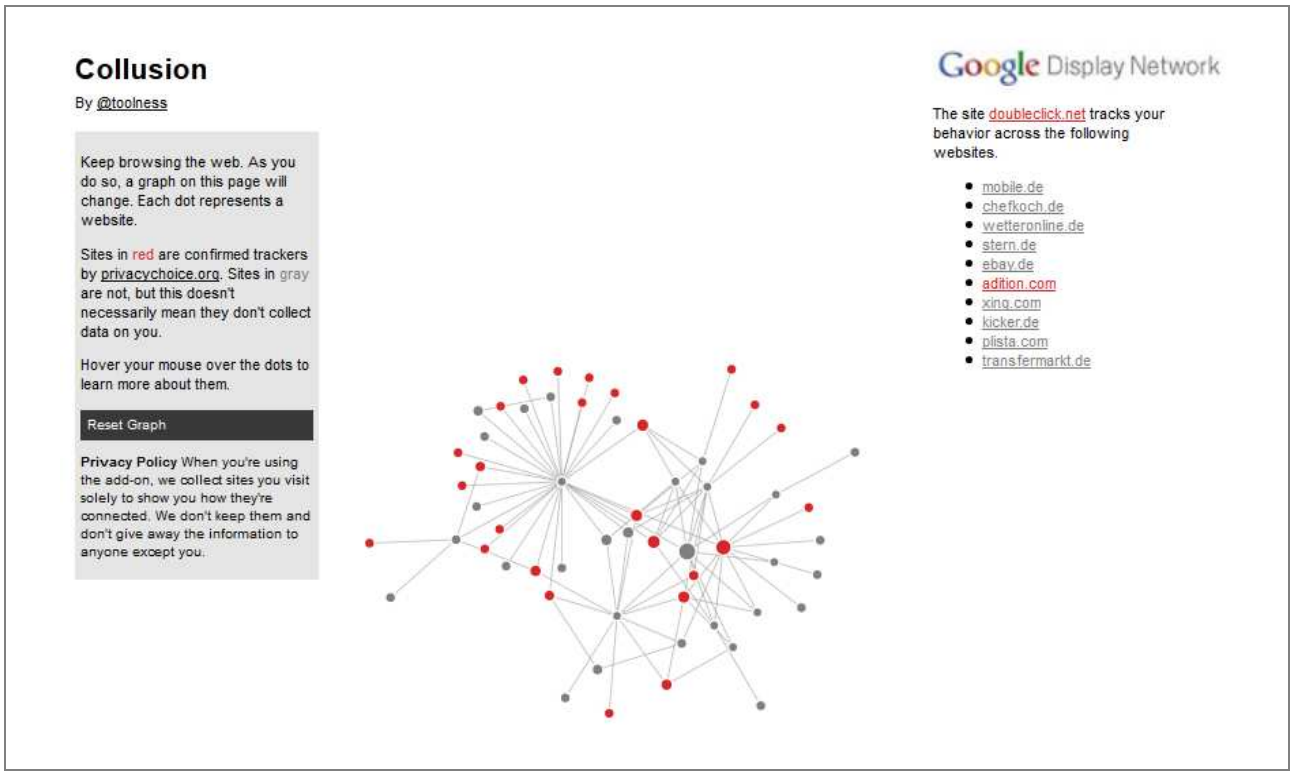


Abbildung 1: Beispiel für Profilbildung

Jede angezeigte Werbung bedeutet eine Übermittlung von Daten, insbesondere der IP-Nummer, des Besuchers an den Werbeanbieter. Auf welcher Rechtsgrundlage geschieht die Übermittlung? Die Frage nach der Rechtsgrundlage ist insofern von Relevanz, da z.B. Google Adsense – das Werbenetzwerk von Google – die IP-Nummer für einen nicht genannten Zeitraum speichert.[9]

Da es sich bei Webseiten um Telemedien handelt, findet das Telemediengesetz (TMG) Anwendung. Aus der Perspektive des Webseitenbetreibers sind zwei Vertragsformen denkbar, die im Folgenden skizziert werden:

[7] URL: http://ausweisung.ivw-online.de/i.php?s=1&mz=201208&sall=1&sort=dvisitsiabs&angebote=1&netz=1&vgm=1&svisits=1&svisitsiabs=1&svisitsipro=1&svisitsaabs=1&svisitsapro=1. Letzter Zugriff: 2012-10-05.

[8] URL: https://addons.mozilla.org/de/firefox/addon/collusion/ Letzter Zugriff: 2012-10-05.

[9] Google (2012): Werbung und Datenschutz – häufig gestellte Fragen. URL: http://www.google.com/policies/privacy/ads/. Letzter Zugriff: 2012-10-04.

- Vermietung von Bildschirmfläche: Der Betreiber vermietet eine bestimmte Fläche an ein Werbeunternehmen, dass dort in Eigenregie Werbung schaltet. Beim Abruf der Webseite werden die Inhalte beider Unternehmen zusammen ausgeliefert. Es spricht viel dafür, sowohl den Betreiber als auch das Werbenetzwerk jeweils als verantwortliche Stelle zu betrachten. Die Vorschriften des TMG, z.B. Impressumspflicht, fänden auch auf das Werbenetzwerk Anwendung. Werbung wäre Impressumspflichtig.

- Beauftragung zur Schaltung von Werbung: Der Betreiber beauftragt das Werbenetzwerk, Werbung zu schalten. Als Rechtsgrundlage käme – neben der nicht praxistauglichen Einwilligung – § 15 Abs. 1 TMG in Betracht, der die Erhebung und Verarbeitung personenbezogener Daten zur Diensterbringung erlaubt. Gehört Werbung zur Diensterbringung? Hier bestehen erhebliche Zweifel, denn eine Webseite, die durch einen Werbeblocker betrachtet wird, funktioniert auch weiterhin.[10] Wenn § 15 Abs. 1 TMG als Rechtsgrundlage ausscheidet, ist keine legitimierende Rechtsgrundlage erkennbar. § 15 Abs. 3 TMG regelt die Profilbildung und nicht die Übermittlung zur Anzeigenschaltung.

Anhand verschiedener Werbenetzwerke untersuchen wir nachfolgend, ob Webpräsenzen, die Werbung anzeigen, auch eine Datenschutzerklärung besitzen.

2.4 Kontaktformulare

Wer via Online-Kontaktformular Waren oder Dienstleistungen bestellt oder auch nur Informationen oder einen Newsletter anfordert, gibt seine persönlichen Daten preis. Neben der Erfüllung einer konkreten Bestellung oder der Beantwortung einer Anfrage erlaubt die moderne Informationstechnik darüber hinaus, die gewonnenen Informationen für unterschiedliche Zwecke weiterzunutzen. Ohne dass es der Webseiten-Besucher (Kunde) ahnt, können

- Konsumentenprofile erstellt und ausgewertet,
- Werbung zielgerichtet versendet,
- oder auch monetäre Zusatzerlöse durch den Verkauf seiner personenbezogenen Daten generiert werden.

Unternehmen signalisieren durch eine Datenschutzerklärung, wozu sie persönliche Angaben nutzen. Diese Transparenz schafft eine wichtige Grundlage für Vertrauen, denn 69% der Bundesbürger sind besorgt darüber, dass Unternehmen ihre Daten für zusätzliche Zwecke (z. B. Direktmarketing) als nur für den ursprünglichen Erhebungszweck nutzen.[11] Datenschutzerklärungen liegen deshalb im Eigeninteresse von Unternehmen. Diese sind nach Ansicht von 61% der Bundesbürger jedoch unklar formuliert.[12]

Zusätzlich regeln gesetzliche Vorschriften den Umgang mit personenbezogenen Daten. Während für den Webauftritt das Telemediengesetz (TMG) gilt, fallen die in einem Kontaktformular von privatwirtschaftlichen Unternehmen, Vereinen und anderen nicht-öffentlichen Betreibern übermittelten Daten unter das Bundesdatenschutzgesetz (BDSG).[13] Bei öffentlichen Stellen der Länder gelten die entsprechenden Landesdatenschutzgesetze.

[10] Ausführlicher haben wir die Frage der Diensterbrinung am Beispiel des Facebook Like Buttons im Datenschutzbarometer 2010 diskutiert. URL: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php

[11] Europäische Kommission (2011): Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. Letzter Zugriff: 2012-12-03.

[12] Heise Online (2011): Studie: Nutzer fordern mehr Transparenz beim Datenschutz im Netz. 01.06.2011. URL: http://heise.de/-1253855. Letzter Zugriff: 2012-12-03.

[13] Hoeren, Thomas (2008): Skript zum Internetrecht. Stand März 2008. URL: http://vg00.met.vgwort.de/na/8181c8ca7c1ad67f6567?l=http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2008.pdf. S. 399. Letzter Zugriff: 2012-12-03.

Ein Beispiel: Max Mustermann füllt ein Kontaktformular aus und klickt auf „absenden“. Darf der Empfänger seine Anfrage beantworten?

§ 4 Abs. 1 BDSG erlaubt eine Verarbeitung personenbezogener Daten nur dann, wenn eine Einwilligung vorliegt oder eine gesetzliche Vorschrift oder eine andere Rechtsvorschrift dies erlaubt. Aus Mangel an speziellen Rechtsvorschriften für Kontaktformulare bedarf es einer Einwilligung von Max Mustermann. Ob seine freiwillige Datenabgabe bereits eine Einwilligung darstellt oder dies in expliziter Form erforderlich ist, ist unter Juristen umstritten.[14]

Unstrittig dagegen ist, dass eine Einwilligung voraussetzt, dass Max Mustermann weiß, worin er einwilligen soll (siehe § 4a Abs. 1 S. 2, § 4 Abs. 3 BDSG). Denn wer würde etwas kaufen, ohne sich vorher mit dem Verkäufer über den Gegenstand und die Modalitäten zu verständigen? Erläutert die Webpräsenz,

- für welche Zwecke die Daten genutzt werden (z. B. Bearbeitung der Anfrage, Zusendung von Werbung) und
- an wen die Daten übermittelt werden,

dann weiß Max Mustermann, worauf er sich einlässt und kann einwilligen. Eine solche Erläuterung nennen wir in dieser Studie „Datenschutzerklärung“. Welche Form eine solche Einwilligung haben sollte, wurde im Rahmen der zurückliegenden XAMIT Studie „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz“[15] ausführlich erläutert und ist im Anhang der vorliegenden Untersuchung zusammengefasst.

Unter den Begriff „Kontaktformular“ fassen wir im Zuge unserer Untersuchung alle Eingabemöglichkeiten für personenbezogene Daten zusammen, also auch Newsletter-Anmeldungen oder Anmeldungen zu persönlichen bzw. Passwort-geschützten Webseitenbereichen.

2.5 Social Plugins

Die Frage, warum Kunden ein Produkt oder eine Dienstleistung kaufen beziehungsweise nicht kaufen, treibt wohl die meisten Unternehmen um. Daher gilt Empfehlungsmarketing schon lange als ein wichtiger Schlüssel zum Werbeerfolg eines Unternehmens. Seit 2010 bietet Facebook mit dem sogenannten „Like-Button“ Empfehlungsmarketing für Webseiten und Produkte an. Google hat mit seinem „+1“ Button kurze Zeit später nachgezogen.

Seit unserer ersten datenschutzrechtlichen Analyse des Facebook Like-Buttons im Datenschutzbarometer 2010[16] – aktualisiert im Datenschutzbarometer 2011 – und der datenschutzrechtlichen Bewertung[17, 18] von Facebook-Diensten durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat sich nicht viel getan.

Die vom ULD angestrebte gerichtliche Klärung, ob der Like-Button gegen deutsches Recht verstößt, hat bisher nicht stattgefunden.[19]

[14] Ebd. S. 409
[15] Kostenfreier Download: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php
[16] Kostenloser Download: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php
[17] ULD (2011): Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook. Version 1.0. URL: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf. Letzter Zugriff: 2012-12-03.
[18] Karg, Moritz; Thomsen, Seven (2012): Tracking und Analyse durch Facebook. In: Datenschutz und Datensicherheit (DuD), Nr. 10, Jg. 2012, S. 729-736.
[19] Weichert, Tilo (2012): Datenschutzverstoß als Geschäftsmodell – der Fall Facebook. In: Datenschutz und Datensicherheit (DuD), Nr. 10, Jg. 2012, S. 716-721.

Solange Datenschutzaufsichtsbehörden eine Nutzung des Like-Buttons als Datenschutzverstoß werten, besteht für Webseitenbetreiber akuter Handlungsbedarf. Sie müssen den Like-Button entfernen, um ein Bußgeld von maximal 50.000 Euro zu vermeiden, oder es auf eine gerichtliche Auseinandersetzung ankommen lassen.

Der Heise Verlag hat eine Lösung vorgestellt, die den Like-Button erst nach expliziter Einwilligung des Besuchers anzeigt. Vorher werden laut Heise keine Daten an Facebook übermittelt.[20] Das ULD sieht diese Lösung u. a. wegen mangelnder Transparenz darüber, was Facebook mit den Daten macht und wegen formaler Überlegungen als unzureichend an.[21]

Wer als Webseitenbetreiber außerdem die Hinweispflicht auf die Datenübermittlung an Facebook in der Datenschutzerklärung nach § 13 TMG ignoriert, riskiert ein zusätzliches Bußgeld von bis zu 50.000 Euro.

Internet-Surfern, die sich gegen die Datensammlung des Like-Buttons oder anderer Soical Plugins schützen möchten, empfehlen wir die Nutzung des Addons „Ghostery“[22] zusammen mit dem Browser „Firefox“ (siehe Tipps im Anhang 9.2).

[20] Heise Online (2011): 2 Klicks für mehr Datenschutz. URL: http://heise.de/-1333879. Letzter Zugriff: 2012-12-03.
[21] Heise Online (2011): Facebook vs. Datenschützer: Streit um Like-Button geht weiter. URL: http://heise.de/-1338660. Letzter Zugriff: 2012-12-03.
[22] Bezugsquelle: http://www.ghostery.com

3 Gegenstand und Methode des Datenschutzbarometers 2012

Eine maschinelle Quellcode-Analyse im August 2012 von 33.634 deutschen Webpräsenzen bildet die Grundlage des XAMIT Datenschutzbarometers 2012. Neben 1.915 Gemeinden und politischen Organisationen sowie 3.805 Vereinen berücksichtigt die vorliegende Studie Unternehmen aus unterschiedlichen Branchen:

- Verarbeitendes Gewerbe
- Handel, Instandhaltung und Reparatur von Kfz und Gebrauchsgütern
- Gastgewerbe und Hotels
- Grundstücks- und Wohnungswesen
- Gesundheitswesen
- Rechtsanwälte & Steuerberater
- Werbung
- Informationstechnik
- Unternehmensberatung
- Handwerk
- Medien
- Energie- und Wasserwirtschaft

Jede Branche ist mit 812 bis 6.376 Webpräsenzen vertreten. Analysiert werden jeweils maximal 1.000 Webseiten pro Webpräsenz.

Insgesamt werteten wir über 3 Mio. Webseiten aus. Hierbei wurde untersucht,

- ob und welche Shop-Software verwendet wird (Kapitel 3.1),
- ob Werbenetzwerke verwendet werden (Kapitel 3.2),
- ob und welche Webstatistiken genutzt werden (Kapitel 3.3),
- ob Kontaktformulare vorhanden sind (Kapitel 3.4) und
- ob Social Plugins genutzt werden (Kapitel 3.5).

In diesem Zusammenhang wurde auch das Vorhandensein von Datenschutzerklärungen geprüft. Datenschutzerklärungen enthalten charakteristische Worte („Datenschutz“, „Zweck“ usw.), um aussagekräftig zu sein. Nach diesen Worten wurde gesucht, um zu bestimmen, welche Webseiten über eine Datenschutzerklärung verfügen und welche nicht. Die Reihenfolge der Worte ist dabei irrelevant. Welche Regelungen in einer Datenschutzerklärung getroffen werden, bleibt aus methodischen Gründen unberücksichtigt.

Durch die maschinellen Analysen sind Fehlzuordnungen nicht auszuschließen. Stichprobenhafte Kontrollen zeigten allerdings keine Fehler. Daher können die Ergebnisse als valide betrachtet werden.

3.1 Einbindung eines Webshops

Wie viele Webshops verwenden aktuelle PHP-Versionen und welche Shopsoftware wird eingesetzt? Um diese Fragen zu beantworten, untersucht XAMIT für jeden erkannten Webshop,

- ob eine identifizierbare Shopsoftware verwendet wird sowie
- ob und in welcher Version PHP eingesetzt wird.

Dazu untersuchten wir maschinell den Quellcode jeder Webseite daraufhin, ob charakteristische Zeichen für bekannte Standardshopsoftware vorhanden sind. Webshops, die keine bekannte Standardshopsoftware einsetzen, sondern eine Eigenentwicklung, konnten wir aufgrund fehlender Charakteristika nicht identifizieren.

Es gibt kein eindeutiges Merkmal, einen Webshop zweifelsfrei von einem reinen Informationsangebot zu unterscheiden. Eine Warenkorbfunktion kann mit „Warenkorb“ betitelt sein, sie muss es aber nicht. Das Wort „Warenkorb“ kommt zudem auch außerhalb von Webshops vor. Erst die Verwendung einer Shopsoftware lässt eindeutig auf einen Webshop schließen.

Die PHP-Version ermittelten wir aus dem Header der Webseite. Allerdings lassen sich Webserver so konfigurieren, dass die PHP-Version im Header gar nicht oder falsch angezeigt wird. Das Verheimlichen der Version erschwert etwa einen möglichen Angriff. Aus diesem Grund konnten wir nicht alle PHP-Installationen aufspüren. Auch lässt sich ein gehärtetes, d. h. „sicheres“ PHP[23] nicht aufspüren. Ungeachtet dessen kann die verwandte Methodik einen ersten Überblick über die Sicherheit von Webshops verschaffen.

3.2 Einbindung von Werbenetzwerken

Für die Einbindung von Werbenetzwerken nutzen Websites charakteristische Zeichenfolgen, die für das jeweilige Netzwerk typisch sind in Form der entsprechenden Java Scripts. Diese Zeichenfolge ist auf allen Webseiten, die das jeweilige Werbenetzwerk einsetzen, identisch. Sobald wir die Zeichenfolge im Quelltext finden, gehen wir von einer Nutzung des zugehörigen Werbenetzwerks aus.

3.3 Webstatistiken, Nutzer-Hinweis und Möglichkeiten zum Widerspruch

Auch 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.

Zusätzlich erheben wir, wie viele Webpräsenzen die gesetzlich geforderte Widerspruchsmöglichkeit gegen die Profilbildung umsetzen.

Google verlangt in § 8.1 seiner Nutzungsbedingungen[24], die Nutzung von Google Analytics an „prominenter“ Stelle zu dokumentieren. Google schreibt den Wortlaut dieser Information oder einen inhaltlich gleichwertigen Text vor und behält sich in § 8.2 ein Kontrollrecht vor. Ob die von Google

[23] Siehe auch http://www.hardened-php.net/suhosin/index.html
[24] Google Analytics Bedingungen. URL: http://www.google.com/analytics/de-DE/tos.html. Letzter Zugriff: 2012-10-05.

vertraglich vorgeschriebenen Formulierungen auf einer Webpräsenz, die Google Analytics nutzt, vorkommen, wurde analog untersucht.

3.4 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 keine systematischen oder lediglich minimale Fehlzuordnungen. Deshalb können wir auch diese Ergebnisse als ausreichend valide betrachten.

3.5 Einbindung von Social Plugins

Für jede Webseite wurde untersucht, ob der Like-Button von Facebook oder der „+1“ Button von Google eingebunden ist. Wir prüften dabei, ob die jeweils zur Verfügung gestellten charakteristischen iframes oder Skript-Codes auf der Seite auffindbar sind. Wurde er gefunden, nehmen wir an, dass der jeweilige Button auf der Seite verwendet wird. Bei manuellen Stichproben wurden keine Fehlzuordnungen festgestellt.

4 Ergebnisse

In diesem Kapitel stellen wir die Befunde hinsichtlich

- sicherer Software (Kapitel 4.1),
- Werbeeinblendungen (Kapitel 4.2),
- Webstatistiken (Kapitel 4.3)
- Kontaktformularen (Kapitel 4.4)
- und der Social Plugins (Kapitel 4.5)

vor. Die Ergebnisse aggregieren wir in Kapitel 5 zum kompakten XAMIT Datenschutzbarometer 2012.

4.1 Risiko durch veraltete Software

Die Beobachtung der früheren Datenschutzbarometer, dass neue PHP-Versionen sich nur sehr langsam verbreiten, bestätigt sich auch 2012. Obwohl die Fehlerbehebung von PHP 4 Ende 2008[25] eingestellt wurde, nutzen diese immer noch 21% der Webpräsenzen, deren PHP-Version ermittelbar war. 2011 betrug der Anteil 26%.

Auch 2012 besitzt das ebenfalls nicht mehr gepflegte PHP 5.2 mit 57% den größten Anteil. Das neue PHP 5.4 besitzt 2012 einen Anteil von unter 1% der Webpräsenzen, deren PHP-Version ermittelbar war (Abbildung 2).

Die jeweils zum Zeitpunkt der Erhebung aktuelle PHP-Version 5.3.15 wurde von 6% der PHP 5.3 nutzenden Webpräsenzen verwendet. Bei PHP 5.4 sieht die Situation mit 66% besser aus, da bei einer Neuinstallation meistens auch die aktuelle Version aufgespielt wird. Bezogen auf alle Webseiten mit PHP nutzen 99% eine veraltete Version. 2011 betrug der Anteil veralteter Installationen 92%. Durch die Einführung von PHP 5.4 sind die PHP-Versionen zahlreicher Webpräsenzen veraltet.

[25] Siehe Ankündigung zu Version 4.4.9. URL: http://php.net/releases/4_4_9.php. Letzter Zugriff: 2012-12-03.

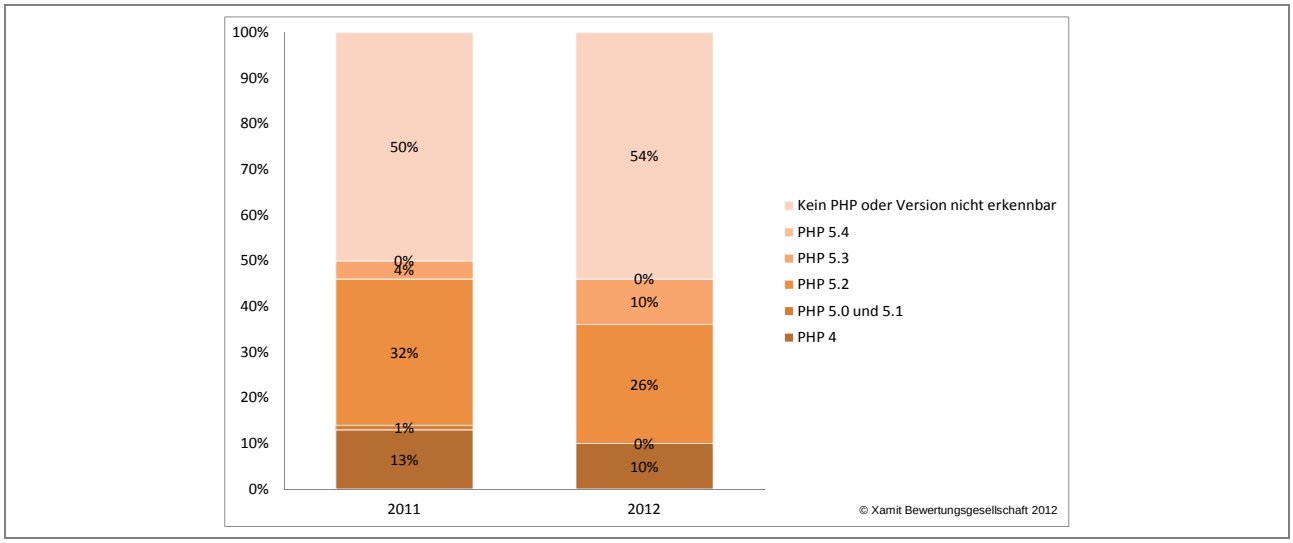


Abbildung 2: Nutzung von PHP nach Versionen

In 988 Fällen konnten wir eine bekannte Shopsoftware erkennen. xtCommerce ist mit einem Anteil von 54% (2011: 69%) unbestrittener Marktführer gefolgt von Oxid Shop mit 25% (2011: 20%) und dem OpenSource-Vertreter osCommerce mit 10% (2011: 7%). Die restlichen 11% verteilen sich auf sechs Programme. Aufgrund der geringen Fallzahlen verzichten wir auf eine Aufteilung nach Branchen.

Angesichts der geringen Anzahl an erkannter Shopsoftware liegt der Verdacht nahe, dass viele Webshops entweder eine kaum verbreitete Standardsoftware oder eine Eigenentwicklung nutzen. Je verbreiteter eine Standardsoftware ist, desto eher werden Sicherheitslücken gefunden und bekannt gegeben. Der Hersteller hat meistens ein vitales Interesse daran, die Lücken schnell zu schließen, da ein hoher Marktanteil zu entsprechend vielen gefährdeten Webshops führt.

Bei Individualsoftware müsste der Shopbetreiber indes aktiv nach Sicherheitslücken suchen (lassen). Dies ist ein kostspieliges Unterfangen, welches nur äußerst selten eingesetzt wird. Wenn Kriminelle (zufällig) auf Sicherheitslücken stoßen, können sie diese unbemerkt ausnutzen. Individualsoftware bedeutet deshalb nicht per se eine höhere Sicherheit.

32% (2011: 23%) der Webshops mit Standardshopsoftware und erkannter PHP-Installation setzen die aktuelle PHP-Version ein. Der Anstieg aktueller PHP-Versionen ist erfreulich, weil veraltete Versionen Sicherheitslücken enthalten können, die Kundendaten gefährden.

Bezogen auf die geringe Anzahl an untersuchten Webshops sind unsere Ergebnisse nicht repräsentativ. Gleichwohl werfen sie ein Schlaglicht auf einen beunruhigenden Sachverhalt: Gefährdete Kundendaten durch veraltete PHP-Versionen.

4.2 Internetwerbung – Warum informieren?

2012 werden neben Google Adsense auch 15 weitere Webenetzwerke berücksichtigt, so dass die Ergebnisse nur eingeschränkt mit den Resultaten von 2011 vergleichbar sind.

Wer Anzeigen eines Werbenetzwerks auf seiner Webpräsenz einbindet, der macht Werbung für fremde Unternehmen und Produkte. Viele der untersuchten Webpräsenzen zählen allerdings nicht zu den typischen Nutzern eines Werbenetzwerks, so dass deren relativ geringer Anteil von 5%

unter den untersuchten Webpräsenzen nicht überrascht. Marktführer ist Google Adsense (Textanzeigen) mit 56,2% gefolgt von Addthis mit 31,7% uns Google Doubleclick (Werbebanner) mit 6,1% der Fundstellen von Werbenetzwerken.

2012 haben 35% der Webpräsenzen mit Werbung eine Datenschutzerklärung. Auf der anderen Seite lassen 65% ihre Besucher im Dunkeln darüber, dass ein Werbenetzwerk einen Cookie setzt und dass Daten, wie die IP-Nummer, zu dem Werbenetzwerk übertragen werden.

Es bestehen deutliche Unterschiede zwischen den Branchen. Unternehmen aus dem Bereich „Medien“ informieren zu 72%, während nur 13% der Handwerker eine Datenschutzerklärung veröffentlichen. Aufgrund der geringen Fallzahlen verzichten wir auf eine weitere Aufteilung nach Branchen.

Die verbreitete Heimlichkeit und Neigung zum Bruch der Nutzungsbedingungen korrespondiert mit unseren Ergebnissen zur Webstatistik (Kapitel 4.3).

4.3 Webstatistik – Der mühevolle Weg zum Licht

Das Beispiel Google Analytics zeigt eindrücklich, wie langwierig und mühevoll der Weg von einer guten Idee zu einer datenschutzkonformen Verwendung ist:

- 2007 – 7% Nutzung:[26] XAMIT untersuchte zum ersten Mal Google Analytics und löste ein breites Medienecho und eine Diskussion in der Fachwelt aus.[27]
- 2009 – 13% Nutzung: Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stufte die Verwendung von Google Analytics durch Webseitenbetreiber als datenschutzwidrig ein.[28]
- 2011 – 22% Nutzung: Der für Google in Deutschland zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Casper, überzeugt das Unternehmen, eine nach deutschem Recht legal einsetzbare Version von Google Analytics bereit zu stellen.[29]
- 2012 – 19% Nutzung: Das Bayerische Landesamtes für Datenschutzaufsicht[30] und der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen kontrollieren Webpräsenzen aus ihrem Bundesland auf die Nutzung von Google Analytics (nicht datenschutzkonforme Version). Von 3.500 softwaremäßig kontrollierten Unternehmensauftritten in NRW sind 1.400 in weiterer Bearbeitung.

Im sechsten Jahr sinkt zum ersten Mal die Verwendung der nicht datenschutzkonformen Version von Google Analytics (Abbildung 3). Ob es an der beginnenden Sanktionierung durch zwei Aufsichtsbehörden oder an der einfachen Verfügbarkeit einer datenschutzkonformen Version liegt, lässt sich nicht sagen. Die Gewinner sind auf jeden Fall die Internetbesucher.

[26] 7% der von uns untersuchten Webpräsenzen nutzen Google Analytics. Für die Quellen vergl. unsere Studien aus dem betreffenden Jahr.
[27] Vgl. Pordesch, Ulrich, Steidle, Roland (2008): Im Netz von Google. Web Tracking und Datenschutz. In: Datenschutz und Datensicherheit (DuD), Nr. 5, Jg. 2008, S. 324-329.
[28] 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: 2012-12-03.
[29] Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit (2011): Beanstandungsfreier Betrieb von Google Analytics ab sofort möglich. URL: http://www.datenschutz-hamburg.de/news/detail/article/beanstandungsfreier-betrieb-von-google-analytics-ab-sofort-moeglich.html?tx_ttnews%5BbackPid%5D=1&cHash=1f795fd22e8f472680d834ed9699fc70. Letzter Zugriff: 2012-12-03.
[30] Bayerischen Landesamtes für Datenschutzaufsicht (2012): BayLDA überprüft bei 13.404 Homepages den datenschutzkonformen Einsatz eines Auswertungsprogramms zur Nutzung der Homepage. Pressemitteilung vom 07.05.2012. URL: http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2012/pm005.html. Letzter Zugriff: 2012-10-16.

Ein Wermutstropfen bleibt jedoch: 2011 setzten in Bayern 22% und in NRW 23% der Webpräsenzen eine nicht datenschutzkonforme Webstatistik ein. 2012 steigt der Anteil auf 23% bzw. 26%. Vor beiden Behörden liegt noch viel Arbeit.

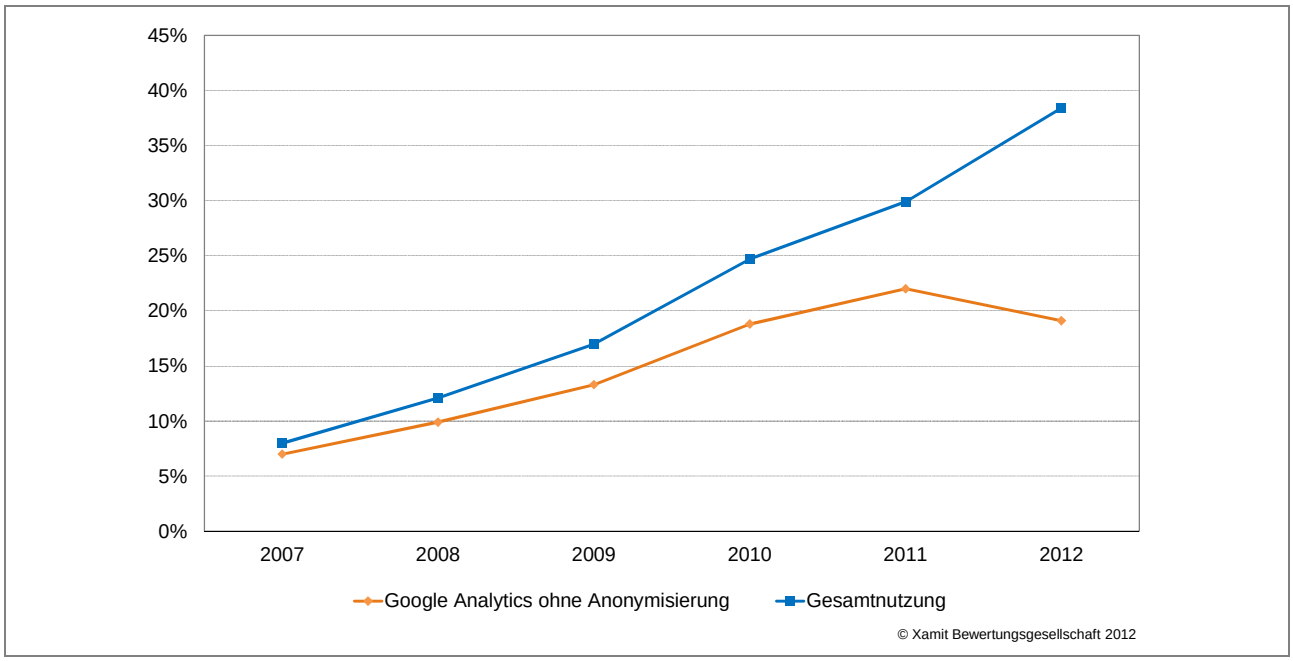


Abbildung 3: Verwendung von Google Analytics ohne Anonymisierung im Vergleich zur Gesamtnutzung von Webstatistiken

2012 nutzen 5,5% (2011: 0,5%) der Webpräsenzen die datenschutzkonforme Version von Google Analytics. Dies ist eine Verzehnfachung zum Vorjahr. Damit erreicht sie einen Marktanteil von 17%. 14,0% (2011: 8%) verwenden heute andere Anbieter. Der Marktanteil von Google beider Versionen sinkt von 75% 2011 auf 74% in 2012.

Wir fanden auf insgesamt 38,4% der untersuchten Webpräsenzen einen Webstatistik-Dienst (2011: 29,9%). Davon verwenden 65,0% (2011: 74,4%) Dienste, die die Kriterien des Düsseldorfer Kreises[31] verfehlen. Der Hauptanteil geht auf das Konto von Google Analytics ohne Anonymisierung. 21,0% (2011: 10,2%) der Dienste erfüllen die Vorgaben des Düsseldorfer Kreises. Die restlichen 14,0% (2011: 15,4%) verteilen sich auf Webstatistik-Dienste, deren Gesetzeskonformität wir aufgrund ihrer geringen Marktabdeckung oder weil sie in Eigenregie eingesetzt werden, nicht geprüft haben.[32] Abbildung 4 zeigt die Nutzung nach Branchen.

[31] Düsseldorfer Kreis (2009): Beschluss. Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten. URL: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.html?nn=409242. Letzter Zugriff: 2012-12-03.

[32] Vgl. XAMIT (2011): Webstatistiken im Test – Welcher Dienst ist in Deutschland legal? 8. Update vom 04.10.2011, S. 10f. URL: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php.

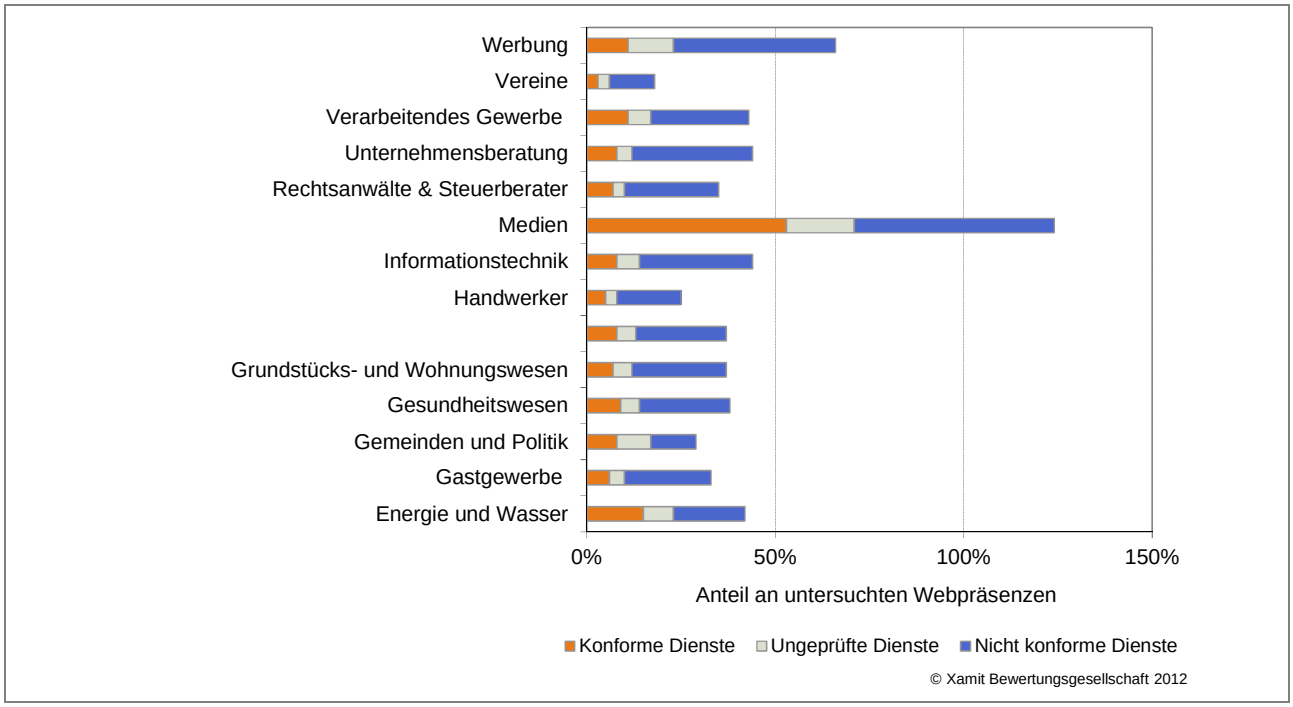


Abbildung 4: Nutzung von Webstatistiken nach Branchen

Die am stärksten nutzenden Branchen haben sich von 2011 zu 2012 nicht verändert. Die meisten nicht konformen Dienste setzen die Branchen Medien (53%), Werbung (43%) und Unternehmensberatungen (32%) ein. Die meisten konformen Dienste nutzen ebenfalls die Medien (53%) gefolgt von Energie und Wasser (15%) sowie dem verarbeitenden Gewerbe und der Werbung mit jeweils 11%.

Der Düsseldorfer Kreis verlangt, dass dem Nutzer „eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen“[33] ist. Auch dieses Jahr messen wir, ob diejenigen Webseitenbetreiber, die eine nach den Kriterien des Düsseldorfer Kreises datenschutzkonforme Webstatistik einsetzen, auch die vorhandene Widerspruchsmöglichkeit nutzen. Dieses Jahr ist auch Google Analytics in der Untersuchung vertreten. Wir fanden auf 7,6% (2011: 2%) der von uns untersuchten Webseiten datenschutzkonforme Webstatistik-Tools, die eine von uns erfassbare Widerspruchsmöglichkeit anbieten. Ein Grund für die Zunahme ist, dass wir 2012 Google Analytics mit erfasst haben. Von diesen Webpräsenzen wiederum geben nur 38,7% (2011: 22,9%) ihren Besuchern die Möglichkeit, der Datensammlung zu widersprechen. Das heißt, dass zwar eine Webstatistik auf datenschutzkonformem Wege erstellt werden könnte, es aber in rund drei von fünf Fällen nicht getan wird. Die Verantwortung liegt hier eindeutig bei den Betreibern der Webpräsenzen. Abbildung 5 zeigt, wie die Widerspruchsmöglichkeit von den einzelnen Branchen umgesetzt wird.

[33] Düsseldorfer Kreis (2009): Beschluss. Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten. URL: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.html?nn=409242. Letzter Zugriff: 2012-12-03.

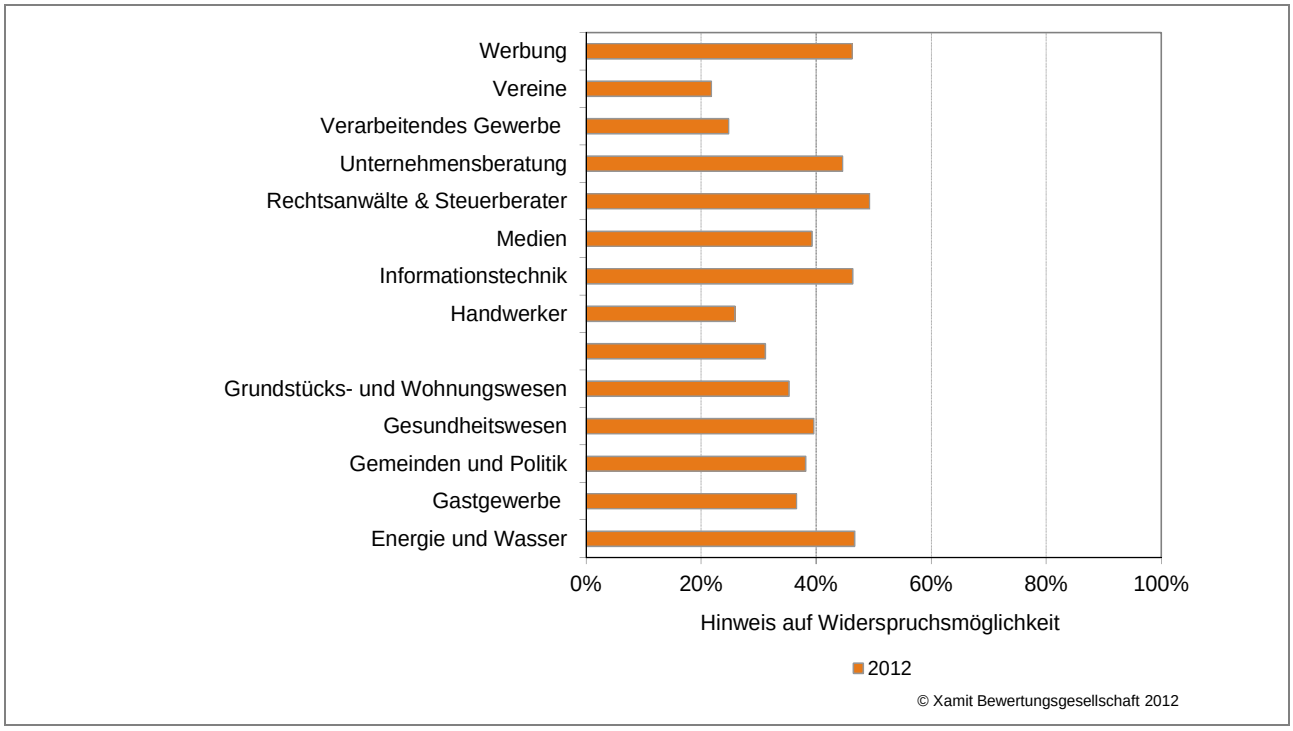


Abbildung 5: Hinweis auf die Widerspruchsmöglichkeit nach Branchen

Nicht nur der Düsseldorfer Kreis fordert einen deutlichen Hinweis auf die Nutzung von Webstatistik-Dienstleistern. Bspw. verlangt Google selber in § 8.1 seiner Nutzungsbedingungen, dass Betreiber die Bewegungsprofile von Besuchern nicht mit personenbezogenen Daten verknüpfen und die Nutzung von Google Analytics an „prominenter“[34] Stelle dokumentieren sollen. Google schreibt den Wortlaut dieser Information oder einen inhaltlich gleichwertigen Text vor und behält sich auch ein Kontrollrecht vor. In der Praxis ignorierten im Jahr 2011 49% der von uns untersuchten Betreiber diese Kennzeichnungspflicht – sei es durch eine eigene Datenschutzerklärung oder den Google Passus. Heute sind es immer noch 42%. Darin enthalten sind nicht nur die Nutzer von Google Analytics, sondern auch alle anderen Nutzer von konformen und nicht konformen Webstatistiken. Das zeigt deutlich, dass viele Betreiber entweder nicht wissen (wollen), was sie tun, oder bewusst die Interessen ihrer Besucher ignorieren, da sie keine Sanktionen fürchten müssen. Die heimliche Nutzung von Webstatistiken nach Branchen zeigt Abbildung 6.

[34] Google Analytics Bedingungen. URL: https://www.google.com/intl/de/analytics/tos.html. Letzter Zugriff: 2012-12-03.

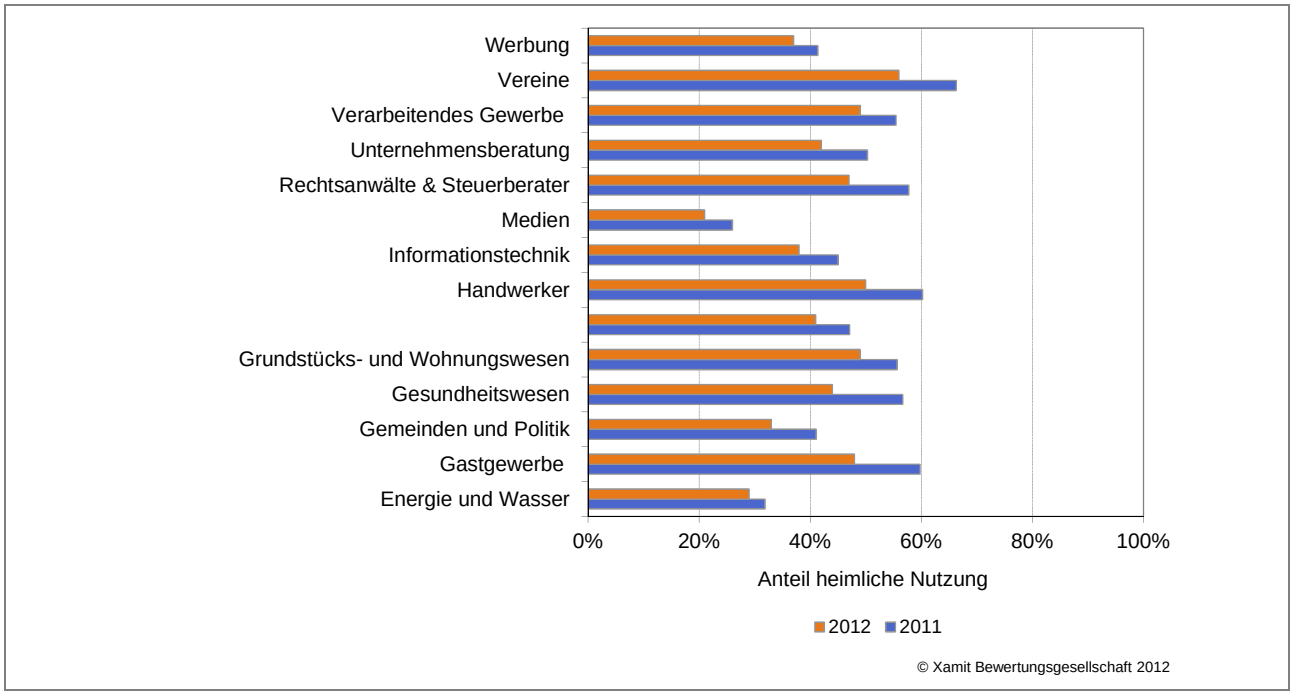


Abbildung 6: Heimliche Nutzung von Webstatistiken nach Branchen

4.4 Kontaktformulare – Wer will schon Transparenz?

Im Jahr 2011 setzten 52% der damals untersuchten Webseiten Kontaktformulare ein. Heute sind es mit 53% nur wenig mehr. Abbildung 7 zeigt die Nutzung nach Branchen. Spitzenreiter sind die Medien in beiden Jahren mit 75% der Webseiten.

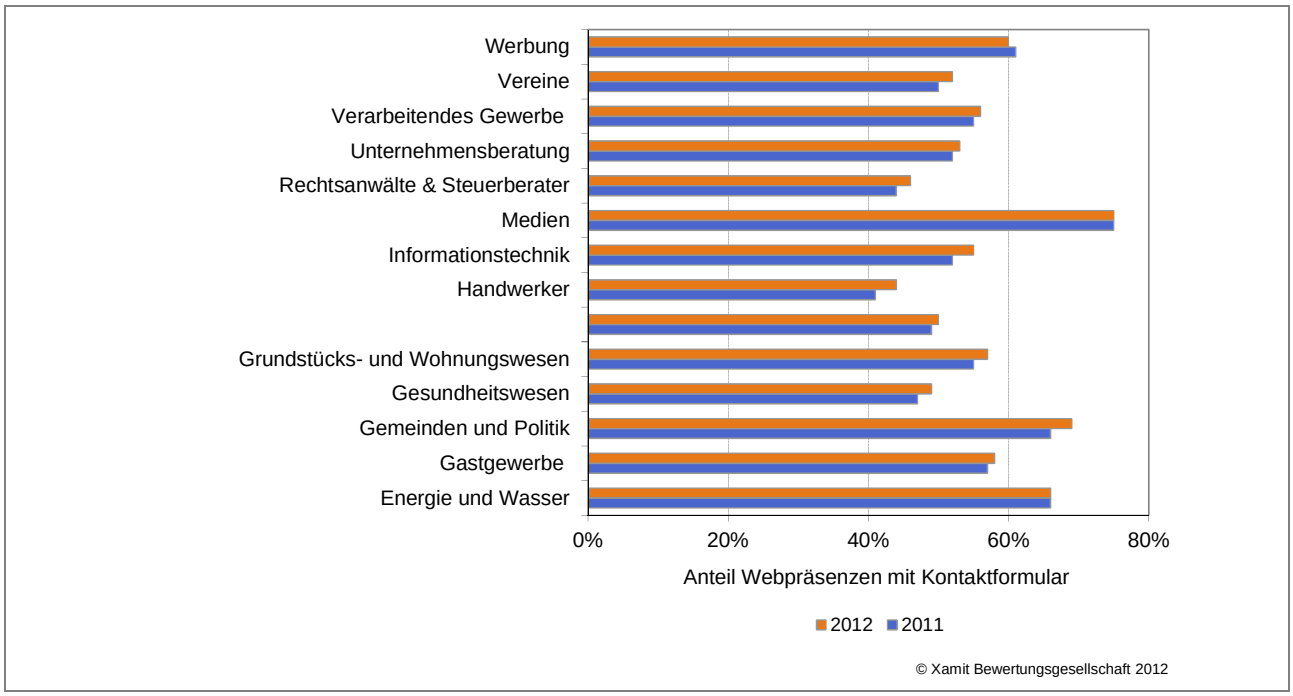


Abbildung 7: Einsatz von Kontaktformularen nach Branchen

Uns interessierte, wie die Betreiber mit den anfallenden personenbezogenen Daten umgehen. Von den Webpräsenzen mit Kontaktformular informieren 38% (2011: 35%) über ihren Umgang mit den erhobenen Daten. 62% (2011: 65%) nutzen ein Kontaktformular ohne Datenschutzerklärung. In Summe werben jedoch immer mehr Betreiber um Vertrauen in ihren Umgang mit den eingegebenen persönlichen Daten. Abbildung 8 zeigt die Verteilung nach Branchen.

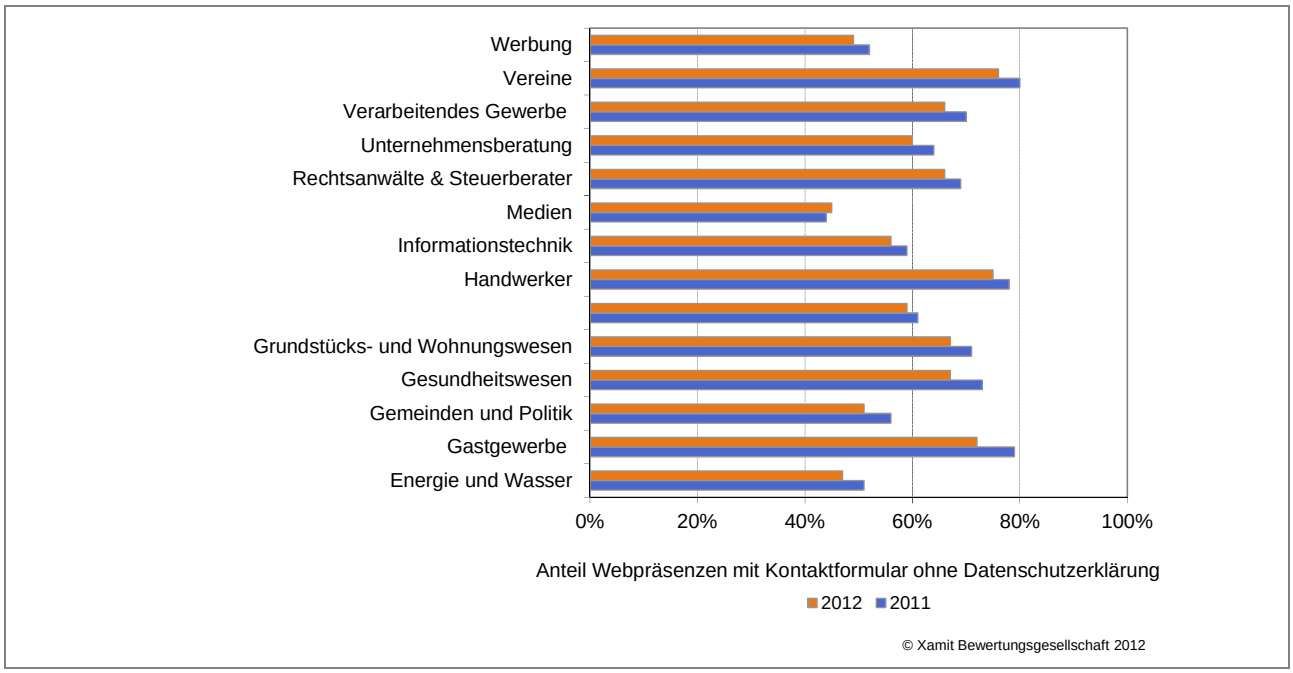


Abbildung 8: Anteil von Kontaktformularen ohne Datenschutzerklärung nach Branchen

4.5 Social Plugins – Ungebremster Datenschutzverstoß

Facebook gab mit seinem Like-Button 2010 den Startschuss für eine rasante Verbreitung von Social Plugins. 2010 setzten erst 0,6% der untersuchten Webpräsenzen den Facebook-Like-Button ein. Zusammen mit dem Social Plugin von Google „+1“ erreichte der Facebook Like-Button 2011 bereits 6,6%. 2012 beträgt der Nutzungsanteil 7,9%.

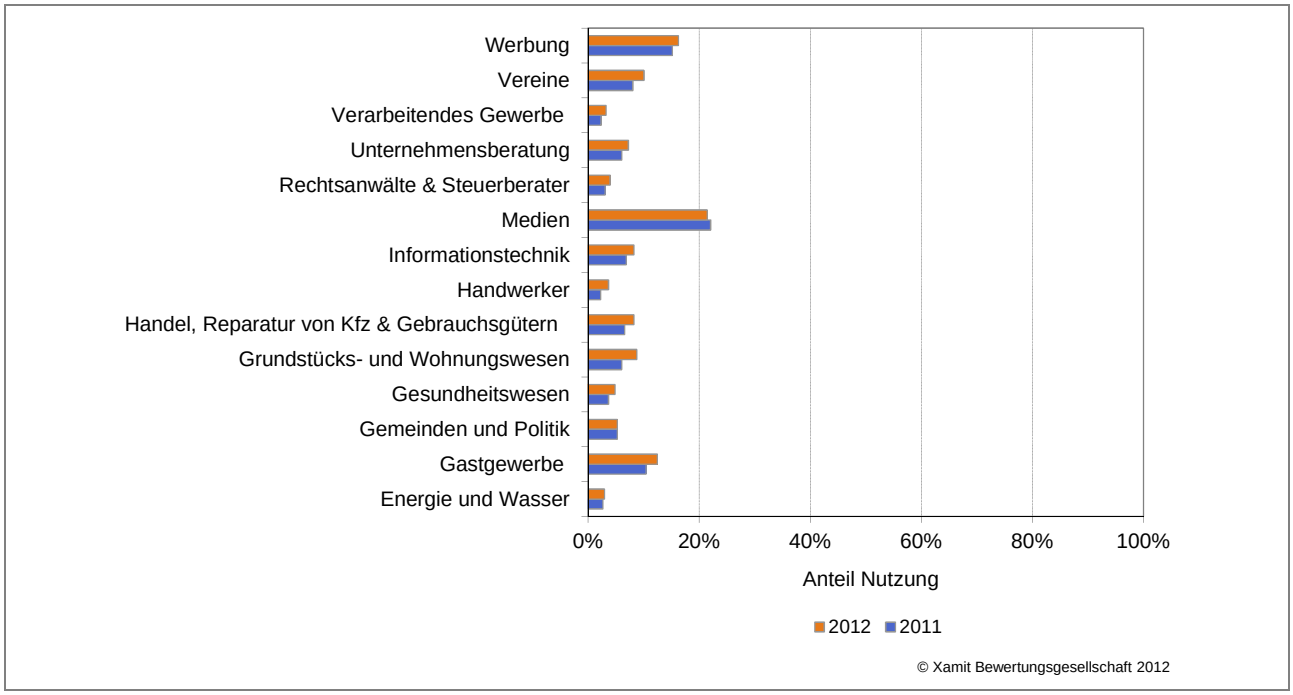


Abbildung 9: Nutzung Facebook-Like-Button nach Branchen

Abbildung 9 zeigt die Nutzung der Social Plugins in den einzelnen Branchen. Überdurchschnittlich viele Social Plugins waren auf Seiten von Medien mit 21,5% (2011: 22,1%) zu finden, gefolgt von Werbung mit 16,3% (2011: 15,2%) sowie dem Gastgewerbe mit 12,5% (2011: 10,5%). Insbesondere Medienseiten sind ihrer Funktion gemäß besonders publikumsstarke Seiten und haben besonders umfangreiche Webauftritte. Daher betrifft ein Datenschutzverstoß auf diesen Seiten naturgemäß sehr viele Surfer.

5 Das XAMIT Datenschutzbarometer 2012

In Kapitel 4 untersuchten wir fünf einzelne Aspekte, die den Umgang mit persönlichen Daten im Internet illustrieren. Alle Aspekte haben wir anhand der gleichen Webpräsenzen untersucht, d. h. die Befunde sind untereinander vergleichbar. Mehr noch, eine Webpräsenz kann sowohl eine Webstatistik nutzen als auch ein Kontaktformular ohne Datenschutzerklärung. Aus diesem Grund kombinieren wir unsere Befunde zu einem Index: dem XAMIT Datenschutzbarometer. Das Datenschutzbarometer zeigt an, wie es um den Schutz persönlicher Daten im Internet bestellt ist. Ähnlich einer Kriminalitätsstatistik zählt das Datenschutzbarometer nun alle Webpräsenzen, die

- heimlich Webstatistiken durch Statistikanbieter erstellen lassen,
- einen nicht mit den Kriterien des Düsseldorfer Kreises konformen Webstatistik-Dienst nutzen,
- einen konformen Webstatistik-Dienst nutzen, jedoch die Widerspruchsmöglichkeit nicht anbieten,
- Kontaktformulare ohne Datenschutzerklärung verwenden,
- Google Adsense ohne Datenschutzerklärung einbinden,
- unsichere PHP-Versionen bei Online-Shops einsetzen und
- den Facebook Like-Button verwenden.

Um das Datenschutzbarometer vergleichbar mit zukünftigen Untersuchungen zu halten, setzen wir die Anzahl an Beanstandungen in Relation zur Anzahl der untersuchten Webpräsenzen.

Die Folgen eines Datenschutzvergehens hängen davon ab, welches Angebot eine Webpräsenz hat oder welchem Zweck sie dient. Eine heimliche Webstatistik eines Sockenhändlers sagt weniger Persönliches aus als die Webstatistik eines Facharztes. Wir fassen deshalb die betrachteten Branchen in folgende Klassen zusammen:

- Sensible Daten: Alle Branchen, die mit sensiblen Daten umgehen, wie das Gesundheitswesen, Rechtsanwälte und Steuerberater.

- Alltag: Hierunter fassen wir alle Branchen zusammen mit denen ein Konsument im Alltag zu tun hat, wie z. B. Handel, Gastgewerbe, Grundstücks- und Wohnungswesen sowie Handwerker, Energiewirtschaft und Medien.

- eGovernment: Alle staatlichen Stellen, wie z. B. Gemeinden, aber auch Parteien fallen in diese Klasse.

- Datenschutzmultiplikatoren: Unternehmen, deren Aufgabenfeld eine größere Datenschutzkompetenz erwarten lässt oder die ihre Kunden im Umgang mit personenbezogenen Daten beraten sollten, fassen wir in dieser Klasse zusammen. Dazu gehören Informationstechnik und Werbung.

- Gewerbe: Unternehmen des produzierenden Gewerbes.

- Dienstleistung: Alle Dienstleistungsunternehmen, die in keine der anderen Klassen fallen, wie z. B. Unternehmensberatungen.

- Vereine: Vereine bilden eine eigene Klasse.

Insgesamt haben wir 91 Verstöße oder Gründe zur Beanstandung auf jeweils 100 untersuchten Webpräsenzen gefunden. 2011 waren es 82. Das ist eine Steigerung um 11%. Abbildung 10 vergleicht die Verstöße 2011 mit 2012. Die Zunahme bei „Werbung ohne Datenschutzerklärung“ resultiert sicherlich auch daher, dass wir dieses Jahr deutlich mehr Werbenetzwerke erfasst haben.

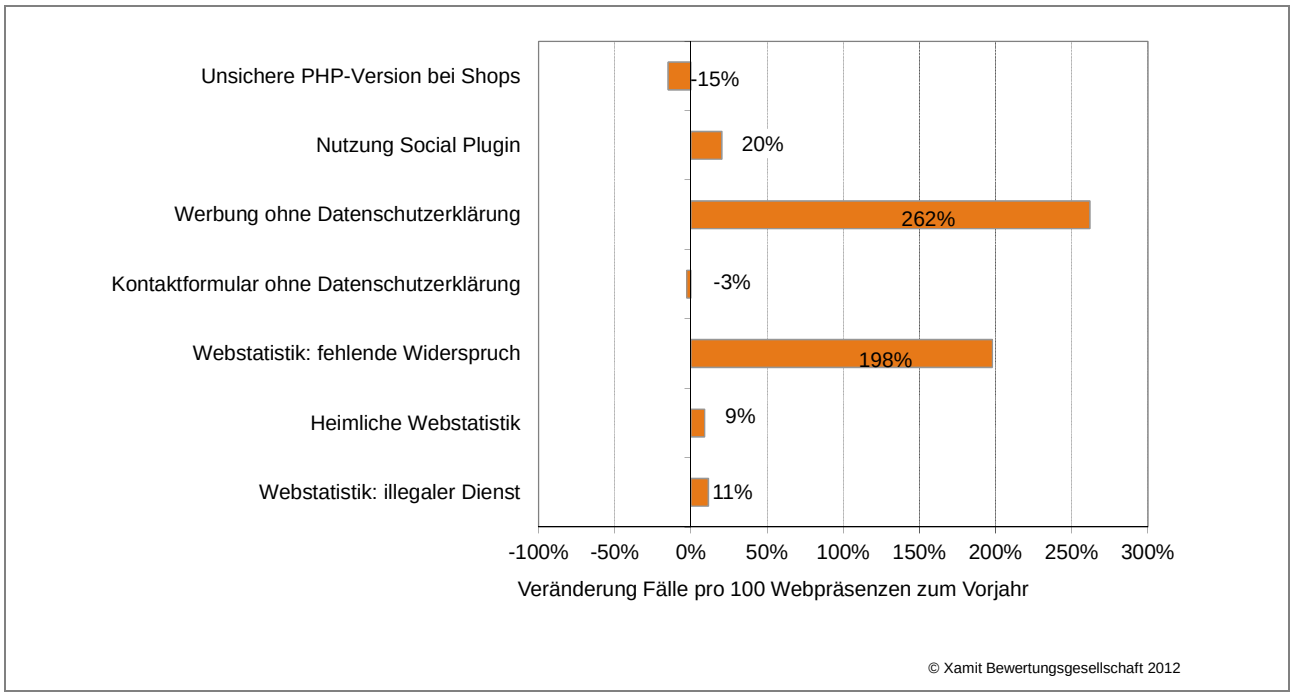


Abbildung 10: Entwicklung der Verstöße und Beanstandungen im Vergleich zum Vorjahr

Spitzenreiter sind seit 2008 die Datenschutzmultiplikatoren. In diesem Jahr mit 114 Verstößen (2011: 104 Verstöße) pro 100 Webpräsenzen (Abbildung 11), d. h. statistisch weist jede Webpräsenz eines Datenschutzmultiplikators mehr als einen Verstoß auf. Danach folgen Dienstleister und Gewerbe. Da viele Unternehmen und Organisationen bei ihren Online-Aktivitäten auf die Kompetenz von Werbe- und IT-Fachleuten setzen, wirkt die Datenschutzsensibilität dieser Datenschutzmultiplikatoren in viele andere Unternehmen hinein. Vermutlich sollte man sich beim Einsatz innovativer Tools nachdrücklicher fragen, ob rechtlich genutzt werden darf, was technisch möglich ist.

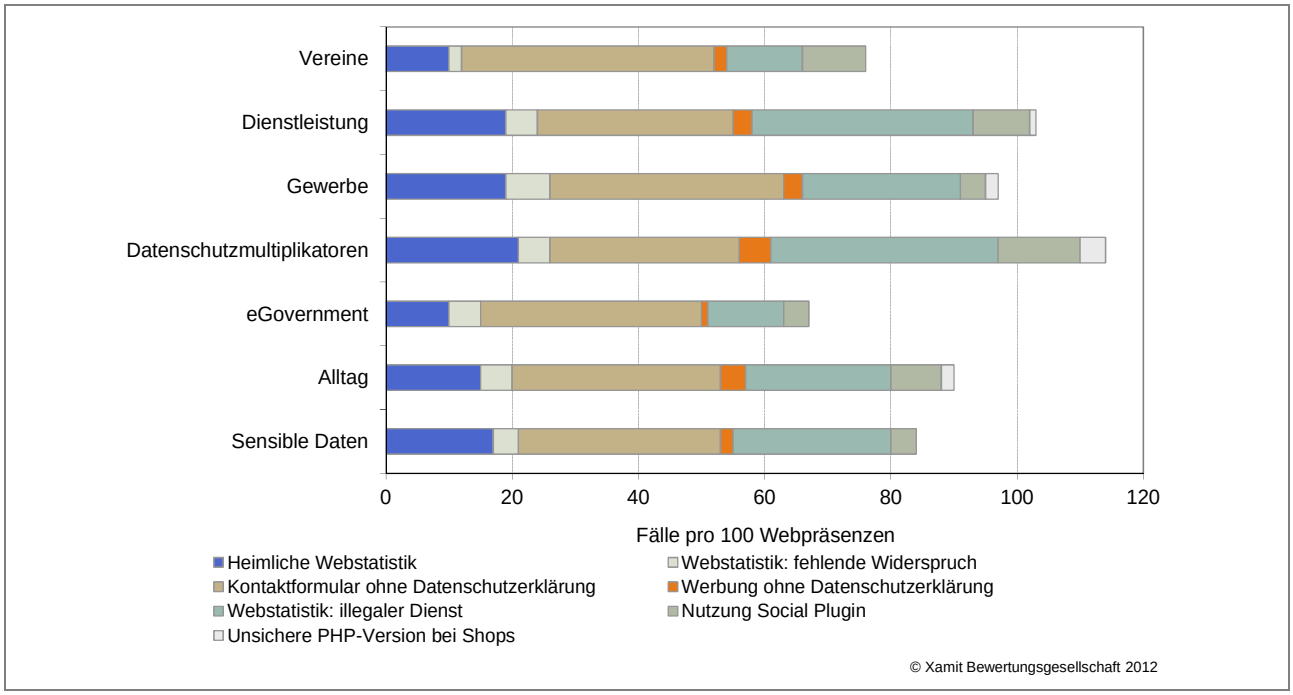


Abbildung 11: Verstöße und Beanstandungen nach Klassen

Eine regionale Verteilung nach Bundesländern zeigt Abbildung 12. Hamburg bleibt mit 110 Verstößen per 100 Webseiten wie im Vorjahr Spitzenreiter. Berlin folgt dicht auf mit 108 Verstößen. Sachsen belegt wie im Vorjahr den 3. Platz mit 97 Verstößen pro 100 Webpräsenzen. In diese Darstellung sind diejenigen Webpräsenzen eingeflossen, deren Betreiber wir einem Bundesland zuordnen konnten. 2.599 Webpräsenzen konnten wir keinem Bundesland zuordnen, weshalb sie in den Zahlen nicht berücksichtigt sind.

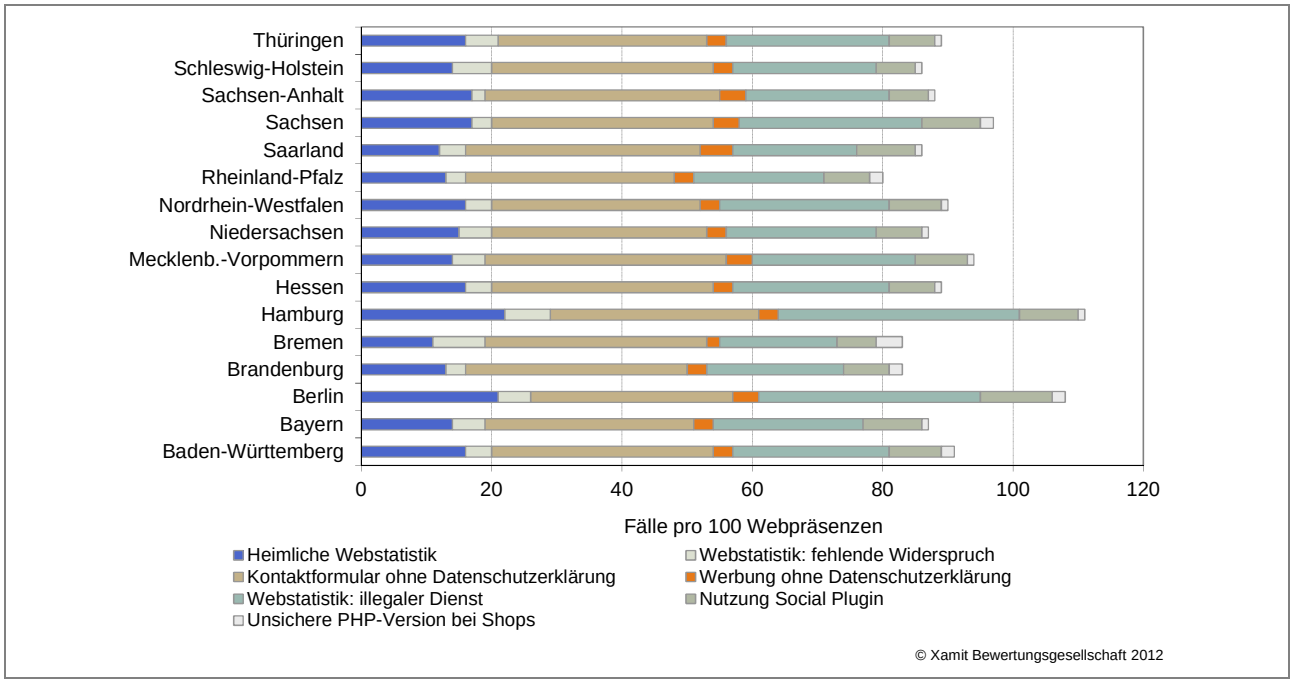


Abbildung 12: Verstöße und Beanstandungen nach Bundesländern

6 Ausstattung und Erfolge der deutschen Datenschutzaufsicht

Wie schon in den Vorjahren haben wir auch dieses Jahr die Aufsichtsbehörden für den öffentlichen (z. B. Behörden) und nicht-öffentlichen Bereich (z. B. Unternehmen, Vereine, Parteien) befragt. An dieser Stelle recht herzlichen Dank für die umfangreichen Antworten. Diese stellen wir in den folgenden Kapiteln vor. Für die Auswertung und Interpretation der Antworten sind allein die Autoren des XAMIT Datenschutzbarometers verantwortlich.

Das Urteil des Europäischen Gerichtshofs vom 9. März 2010 zur mangelnden Unabhängigkeit der Datenschutzaufsichtsbehörden hat die Struktur der Datenschutzaufsicht in Deutschland einschneidend verändert. Bisher gab es zwei Modelle:

- Alles aus einer Hand: Der Landesdatenschutzbeauftragte war zuständig sowohl für den öffentlichen wie auch für den nicht-öffentlichen Bereich.
- Geteilte Aufsicht: Der Landesdatenschutzbeauftragte kümmerte sich um den öffentlichen Bereich und eine weitere Landesbehörde oder ein Referat in einem Ministerium betreute den nicht-öffentlichen Bereich.

Vor allem in 2011 setzten die Bundesländer das Urteil um. 15 Bundesländer entschieden sich für das Modell „Alles aus einer Hand“. Bayern hält an der „geteilten Aufsicht“ fest. Der Bund beruft sich darauf, dass formaljuristisch nur die Bundesländer von dem Urteil betroffen seien und entlässt deshalb den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nicht in die Unabhängigkeit.

6.1 Personelle Ausstattung im Jahr 2012

Seit 2009 befragen wir jährlich alle den Ländern unterstehenden Aufsichtsbehörden und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach ihrer Stellenanzahl.[35] 82% der Behörden haben geantwortet. Für folgende Bundesländer liegen vollständige Angaben vor:

- Bayern
- Berlin
- Brandenburg
- Hamburg
- Hessen
- Mecklenburg-Vorpommern
- Nordrhein-Westfalen
- Rheinland-Pfalz
- Sachsen
- Sachsen-Anhalt
- Schleswig-Holstein

Alle Zahlen geben Vollzeitstellen wieder. Einige Behörden melden Planstellen während andere die besetzten Stellen melden. Wenn Antworten zwischen besetzten Stellen und Planstellen differenzieren, nehmen wir die Planstellen, da sie die maximal mögliche Ausstattung widerspiegeln. Allerdings liegt die Anzahl der besetzten Stellen teilweise deutlich darunter. Ein wichtiger Grund sind haushaltsrechtliche Erwägungen. Mitarbeiter auf Teilzeitstellen haben einen Rechtsanspruch auf eine Vollzeitstelle. Um den Haushalt nicht zu überschreiten, werden Planstellen als Puffer unbe-

[35] Wir verwenden den Begriff „Aufsichtsbehörde“ aus Gründen der Lesbarkeit in Abweichung zum BDSG sowohl für den öffentlichen wie auch für den nicht-öffentlichen Bereich. In beiden Fällen wird faktisch eine kontrollierende Aufsicht geführt.

setzt gelassen. Die hier berichteten Stellen überzeichnen deshalb die tatsächlich vorhandenen Mitarbeiterzahlen.

Einige befragte Behörden nehmen neben ihrer Aufsichtstätigkeit auch weitere Aufgaben wahr, z. B. Aufgaben basierend auf Informationsfreiheitsgesetzen. Aus diesem Grund sind die Stellenangaben nur schwer vergleichbar, denn die hier vorgestellten Zahlen können neben der Datenschutzaufsicht auch Stellen für weitere Aufgaben enthalten. Wir hatten zwar die Behörden explizit nach der Stellenanzahl für die Datenschutzaufsicht gefragt; gleichwohl kann nicht ausgeschlossen werden, dass die Antworten auch Stellen für zusätzliche Aufgabengebiete umfassen. Die Angaben zeigen trotz dieser Einschränkung qualitativ auf, wie es um die Ausstattung der Datenschutzaufsicht bestellt ist.

Das Kernpersonal nahm in Bayern, Berlin, Hamburg, Rheinland-Pfalz und Hessen im Vergleich zum Vorjahr zu. In den Bundesländern, in denen der Landesdatenschutzbeauftragte die Zuständigkeit für den nicht-öffentlichen Bereich im Jahr 2011 übertragen bekommen hat, sind teilweise die Stellenbesetzungen für diesen Bereich noch nicht abgeschlossen (z.B. in Sachsen-Anhalt und Hessen).

In den vergangen Ausgaben des XAMIT Datenschutzbarometers hatten wir bei der Stellenanzahl zwischen den Stellen, die für den öffentlichen Bereich zuständig sind, und den Stellen für den nicht-öffentlichen Bereich unterschieden. Die Konzentration der Zuständigkeit beim Landesdatenschutzbeauftragten nutzten einige Behörden, um die Zuordnung der Stellen nach Bereichen zu Gunsten einer themenspezifische Ausrichtung aufzugeben. Mit dieser Ausgabe des XAMIT Datenschutzbarometers unterscheiden wir bei den Stellen nicht länger zwischen dem öffentlichen und dem nicht-öffentlichen Bereich.

Anmerkungen zur Berechnung

a: Der Bayerische Landesbeauftragte für den Datenschutz hat in seiner Antwort dieses Jahr die Stellenanzahl für 2011 korrigiert.

b, c: Bei den Stellen, die uns zwar im Jahr 2010 oder 2011 geantwortet haben, aber nicht in diesem Jahr, nehmen wir die Zahlen von 2010 bzw. 2011 als Berechnungsgrundlage. Nach unserer Erfahrung sind dadurch keine nennenswerten Fehlzuordnungen zu erwarten. Diese Zahlen sind mit „b“ für 2011 und „c“ für 2010 gekennzeichnet.

d: Da sich die Behörde durch die Zusammenlegung noch im Aufbau befindet sind bisher 30 Stellen besetzt.

e: In den Stellen des Landesbeauftragten für den Datenschutz Baden-Württemberg sind über beide Bereiche summiert zwei abgeordnete Mitarbeiter eingerechnet. Die Angaben in der Tabelle beziehen sich auf besetzte Stellen und nicht auf Planstellen („e“). Der Landesbeauftragte verfügt ohne Abordnungen über 25,5 Planstellen, die wegen des Aufstockungsanspruchs von teilzeitarbeitenden Beamten nicht vollständig besetzt werden können.

g: Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz hat uns die Anzahl der Planstellen für seine Mitarbeiter gemeldet. Wir haben die Anzahl um eins, d.h. um die Stelle des Landesbeauftragten selber erhöht.

h: Die gemeldeten 5 Stellen für die interne Verwaltung haben wir in die Stellenanzahl integriert.

i: Die gemeldeten 4 Hilfskräfte (Archivmitarbeiter usw.) haben wir dem Kernpersonal zugerechnet, da es keine Referendare sind.

Bundesland	2012	2011
Baden-Württemberg	26,20 [e, b]	26,20 [e]
Bayern	45,00	42,00 [a]
Berlin	39,00 [i]	34,00
Brandenburg	22,00	22,00 [b]
Bremen	k. A.	k. A.
Hamburg	18,60 [h]	15,80
Hessen	43,00 [d]	35,20
Mecklenburg-Vorpommern	14,00	14,00
Niedersachsen	17,50 [c]	17,50 [c]
Nordrhein-Westfalen	53,00	53,00
Rheinland-Pfalz	18,50 [g]	17,50 [g]
Saarland	k. A.	k. A.
Sachsen	22,00	22,00
Sachsen-Anhalt	16,00	16,00
Schleswig-Holstein	22,25	22,25
Thüringen	15,00 [b]	15,00
Gesamt gemeldet	**313,60**	**316,70**

Tabelle 1: Personalausstattung Kernpersonal der Datenschutzaufsicht 2012

Die Dienststelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verfügt über 72,5 Stellen für den öffentlichen und 7,5 Stellen für den nicht-öffentlichen Bereich. Diese werden von 12 Hilfskräften wie Referendaren unterstützt. 2011 verfügte der BfDI über 91 Stellen Kernpersonal.

Der Kontrollgegenstand einer Aufsichtsbehörde ist z. B. ein Unternehmen oder eine andere Behörde. Eine wesentliche Kennzahl, um die Größe eines Unternehmens oder einer Behörde zu beschreiben, stellt die Anzahl der sozialversicherungspflichtigen Beschäftigten dar. Wir setzen deshalb gemeldeten Stellen zu der Anzahl an sozialversicherungspflichtig Beschäftigten ins Verhältnis.[36]

Abbildung 13 zeigt die Stellenverteilung pro 100.000 sozialversicherungspflichtig Beschäftigter nach Bundesländern. Deutliche Unterschiede in der Ausstattung fallen ins Auge. Das bevölkerungsreichste Bundesland NRW hat z.B. eine im Verhältnis zur Anzahl an sozialversicherungspflichtig Beschäftigten schwach ausgestattete Aufsichtsbehörde. Für die Ausstattung der Behörden sind die jeweiligen Länderregierungen verantwortlich.

[36] Quelle: Bundesagentur für Arbeit (2012): Arbeitsmarkt in Zahlen, Betriebe und sozialversicherungspflichtige Beschäftigung, Nürnberg, 30. Juni 2011.

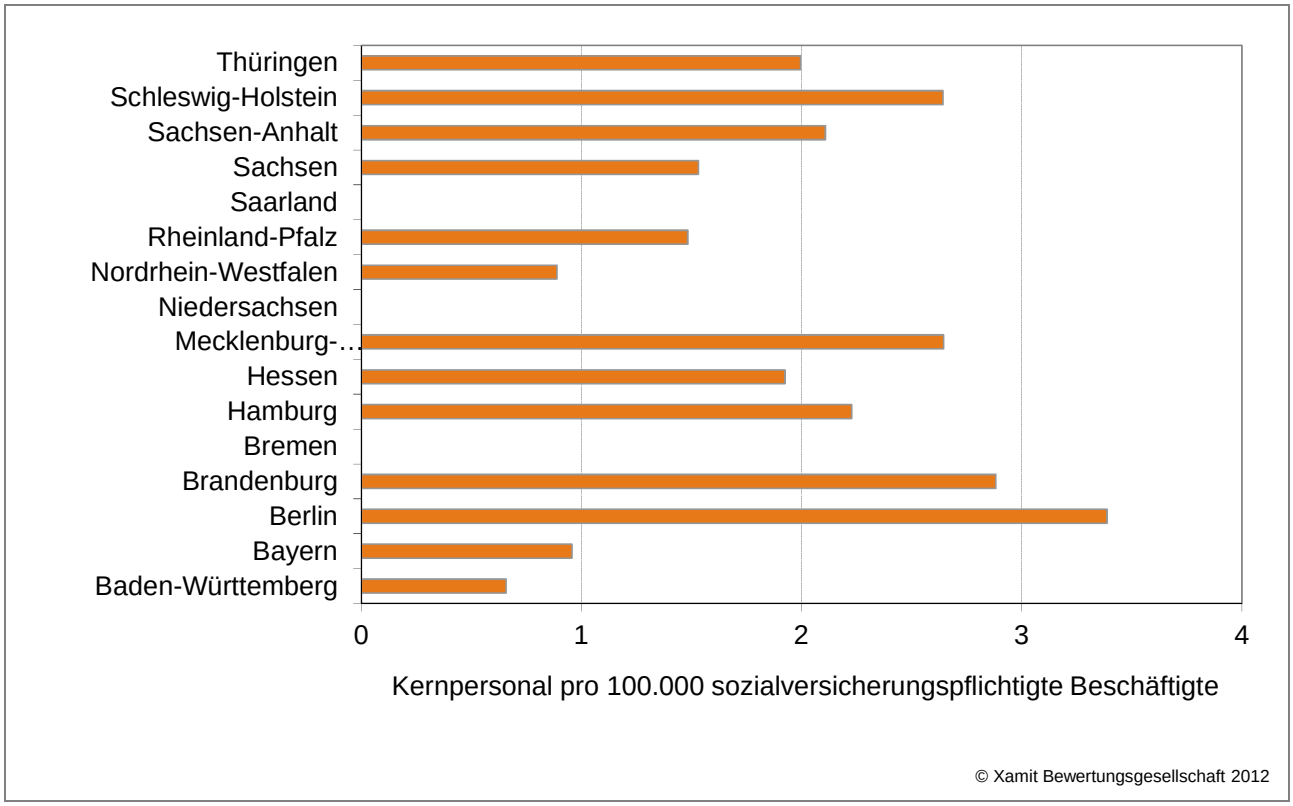


Abbildung 13: Stellenverteilung in Relation zur Anzahl sozialversicherungspflichtiger Beschäftigter.

6.2 Tätigkeiten und Erfolge

Zum Tätigkeitsspektrum einer Datenschutzaufsichtsbehörde zählen in der Praxis:

- Datenschutzberatung und Bearbeitung von Eingaben (Kapitel 6.2.1),
- Kontrolle (Kapitel 6.2.2) und
- Sanktionen (Kapitel 6.2.3).

Eingaben, d. h. Beschwerden, stellen oft den Ausgangspunkt für eine weitergehende Kontrolle dar. Sanktionen können auf Eingaben oder auch als Resultat von Kontrollen erfolgen. Nicht auf jeden Datenschutzverstoß folgt zwangsläufig eine Sanktion. Sanktionen werden nach behördlichem Ermessen im Einzelfall verhängt.

Die größten Erfolge der Aufsichtsbehörden von 2011, die wir in Kapitel 6.2.4 vorstellen, werfen ein Schlaglicht auf weitere Tätigkeiten.

6.2.1 Datenschutzberatung und Eingaben im Jahr 2011

Aufsichtsbehörden sind Anlaufstelle sowohl für Bürger wie auch für Unternehmen und öffentliche Stellen selbst. Neben Fragen adressieren Bürger Beschwerden über den Umgang mit personenbezogenen Daten von öffentlichen und nicht-öffentlichen Stellen. Unternehmen und öffentliche Einrichtungen richten Datenschutzfragen an die Aufsichtsbehörde und bitten um die Prüfung von Datenverarbeitungsverfahren. Diese Tätigkeiten fassen wir unter dem Begriff „Eingaben“ zusammen. Dieser umfasst konkret:

- Beschwerden: Eingaben (per Post, E-Mail, Telefon, Fax usw.), die sich auf ein konkretes Fehlverhalten einer öffentlichen oder nicht-öffentlichen Stelle im Zuständigkeitsbereich (räumlich und sachlich) der Behörde beziehen.

- Fragen und Beratung: Eingaben (per Post, E-Mail, Telefon, Fax usw.) mit Frage- oder Beratungsinhalt, die sich nicht auf ein Fehlverhalten oder die Prüfung eines konkreten Verfahrens (z. B. Genehmigung einer Videoüberwachung) im Zuständigkeitsbereich (räumlich und sachlich) der Behörde beziehen.

- Verfahrensprüfungen: Eingaben (per Post, E-Mail, Telefon, Fax usw.), die sich auf die Prüfung eines konkreten Verfahrens (z. B. Genehmigung einer Videoüberwachung) im Zuständigkeitsbereich (räumlich und sachlich) der Behörde beziehen.

- Sonstige Eingaben: Alle übrigen Eingaben, die weder Beschwerden, Fragen, Beratungen oder Verfahrensprüfungen sind und im Zuständigkeitsbereich (räumlich und sachlich) der Behörde liegen.

- Eingaben außerhalb der Zuständigkeit: Alle Eingaben außerhalb des räumlichen (z. B. falsches Bundesland) oder sachlichen Zuständigkeitsbereichs (z. B. kein Datenschutzbezug).

Von acht Aufsichtsbehörden liegen uns statistische oder geschätzte Angaben für das Jahr 2011 vor.

Aufsichtsbehörden messen ihre internen Vorgänge nach unterschiedlichen Verfahren. Die einen erfassen jeden Kontakt mit der Behörde, andere nur Vorgänge ab einer bestimmten Bearbeitungsdauer und wieder andere orientieren sich daran, ob die Anfrage oder Beschwerde mit einem einmaligen Kontakt abschließend bearbeitet werden konnte. Damit lassen sich die Angaben der Aufsichtsbehörden nicht vergleichen. Aus diesem Grund verzichten wir auf eine Aufschlüsselung nach Behörden oder Bundesländern.

Einige Behörden können die statistischen Angaben zwischen öffentlichen Bereich und nicht-öffentlichen Bereich trennen, andere nicht. In dem Maße, wie die Aufgaben beider Bereiche zusammenwachsen, nimmt die Möglichkeit einer getrennten Erfassung ab. Deshalb betrachten wir beide Bereiche in der Auswertung zusammen.

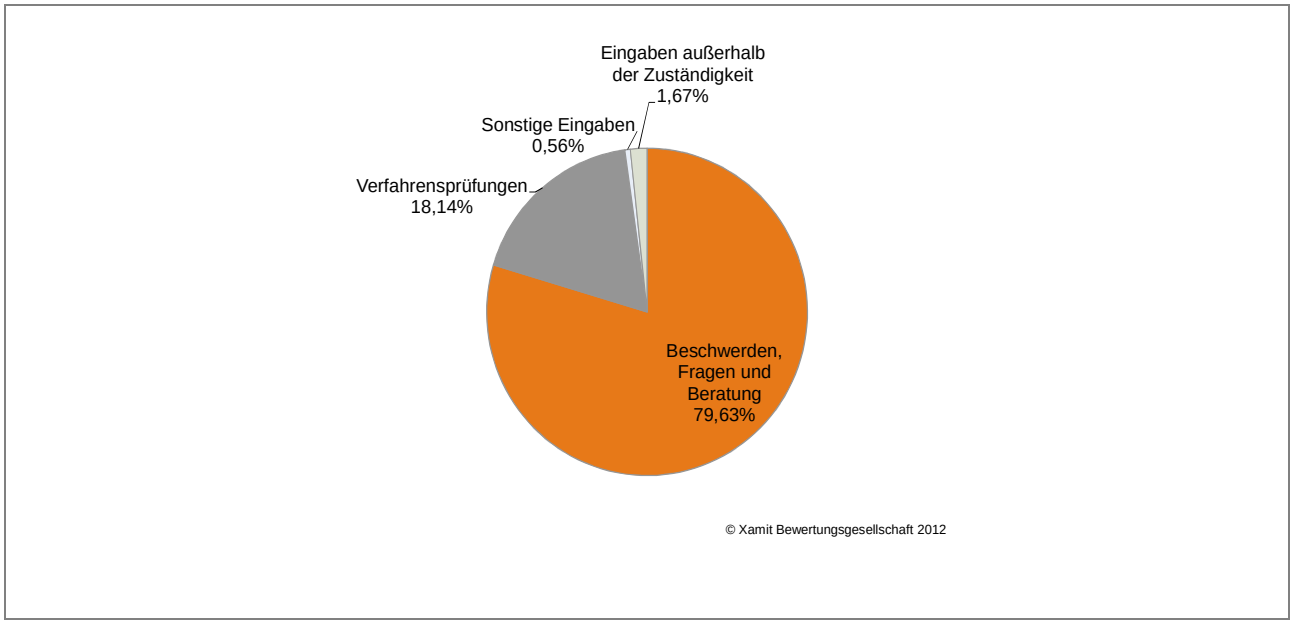


Abbildung 14: Verteilung der Eingaben

Insgesamt wurden uns 34.174 Eingaben gemeldet. 24.187 lassen sich inhaltlich nicht weiter unterteilen. Von den übrigen 9.879 Eingaben bilden Beschwerden, Fragen und Beratung mit 80% den Schwerpunkt. Verfahrensprüfungen folgen mit 18% (Abbildung 14).

Da selbst die Behörden, die uns geantwortet haben, nicht alle Eingaben statistisch erfassen, stellen die hier vorgestellten Zahlen nur die Spitze des Eisberges dar. Weiterhin variiert die Bearbeitungsdauer einer Eingabe von wenigen Minuten bis zu Monaten. Vergleichende Aussagen über den benötigten Personalaufwand sind deshalb schwer möglich, da Äpfel mit Birnen verglichen würden.

Insgesamt wurden 2011 43 Registermeldungen nach § 4d BDSG und 65 Meldungen nach § 42a BDSG (meldepflichtige Sicherheitsvorfälle) berichtet.

6.2.2 Kontrollen im Jahr 2011

Ein Element der Datenschutzaufsicht ist die Kontrolltätigkeit. Kontrollen finden sowohl durch schriftliche Befragungen wie auch durch eine Begehung vor Ort statt. Ziel ist es, die Einhaltung ausgewählter Datenschutzvorschriften zu prüfen.

Fünf Behörden haben unsere Fragen zur Anzahl der Kontrollen im Jahr 2011 beantwortet. Die übrigen Behörden gaben an, keine Statistik zu führen oder dass die Ermittlung mit zu hohem Aufwand verbunden sei. Die Antworten umfassen oft nicht alle Fragen.

Vier Behörden führten jeweils zwischen 15 und 212 Vor-Ort-Kontrollen bei nicht-öffentlichen Stellen durch. In Summe wurden von diesen vier Behörden 453 öffentliche und nicht-öffentliche Stellen vor Ort überprüft. Vor-Ort-Kontrollen sind personalintensiv, weshalb sie zurückhaltend eingesetzt werden.

Zusätzlich zu den Vor-Ort-Kontrollen überprüfte das ULD nach eigener Schätzung 410 öffentliche und 430 nicht-öffentliche Stellen. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kontrollierte 337 öffentliche und 196 nicht öffentliche Stellen. Der Landesbeauftragten

für den Datenschutz Rheinland-Pfalz prüfte 46 öffentliche und nicht-öffentliche Stellen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen befragte zusätzlich zu zahlreichen weiteren Kontrollen postalisch 1.000 Unternehmen, ob sie einen Datenschutzbeauftragten bestellt hätten. 10% der Unternehmen sind ihrer gesetzlichen Pflicht nicht nachgekommen.

Für 2012 plant der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen bei Beschwerden über Videoüberwachungsmaßnahmen in 10% der Fälle vor-Ort-Kontrollen durchzuführen.

6.2.3 Sanktionen im Jahr 2011

Ein Datenschutzverstoß bedeutet, dass die Privatsphäre von Menschen ungerechtfertigt verletzt worden ist. Wer von einem solchen Rechtsverstoß betroffen ist, verlangt – wie die meisten Opfer von Unrecht – eine Bestrafung des Täters. Sanktionen für Gesetzesverstöße sind ein immanenter Teil unserer Rechtsordnung. Sie sind notwendig, um die gesetzlichen Vorschriften durchzusetzen. Wie wirksam Vorschriften sind, deren Übertretung nicht kontrolliert und sanktioniert werden, kann jeder Autofahrer beim Passieren einer Autobahnbaustelle mit Geschwindigkeitsbeschränkung leicht nachvollziehen.

Das Sanktionsinstrumentarium der Aufsichtsbehörden umfasst verschiedene Instrumente, die aber je nach Bundesland oder Bereich nicht alle zum Einsatz kommen:

- Beanstandungen,
- Untersagte Verfahren,
- Abberufung des betrieblichen Datenschutzbeauftragten,
- Antragsrecht für Straftatbestände und
- Bußgelder.

Im öffentlichen Bereich versuchen die Aufsichtsbehörden, Datenschutzverstöße durch Gespräche und Vereinbarungen abzustellen. (Öffentliche) Beanstandungen sind im Allgemeinen ihr letztes Druckmittel. Die übrigen Sanktionen dürfen nur gegenüber nicht-öffentlichen Stellen verhängt werden. Welche Sanktionen eine Aufsichtsbehörde verhängen darf, regelt jedes Bundesland autonom.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist nicht nur für die öffentlichen Stellen des Bundes, sondern auch für die Datenschutzaufsicht über einige Unternehmen zuständig. Gegenüber diesen Unternehmen, z. B. Telekommunikationsunternehmen, besitzt er – ebenso wie bei Behörden – nicht das Recht, Bußgelder zu verhängen.

Weil nicht alle Aufsichtsbehörden die gleichen Sanktionsmöglichkeiten besitzen, kann ein Vergleich der verhängten Sanktionen nur unzulänglich sein. Mit den genannten Einschränkungen wollen wir trotzdem einen Vergleich wagen.

Insgesamt haben sechs Aufsichtsbehörden Angaben zu ausgesprochenen Beanstandungen und untersagten Verfahren gemacht. Viele der übrigen Behörden erfassen nach eigenen Angaben diese Tätigkeiten nicht statistisch. Keine Behörde gab an, ein Verfahren untersagt zu haben. Tabelle 2 zeigt die Beanstandungen.

Bundesland	Beanstandungen öffentl. Bereich	Beanstandungen nicht-öffentl. Bereich
Berlin		1
Bund	3	1
Hessen	1	
Rheinland-Pfalz	1	
Sachsen	11	
Schleswig-Holstein	45 (geschätzt)	150 (geschätzt)

Tabelle 2: Beanstandungen

Eine Aufsichtsbehörde hat die Abberufung eines betrieblichen Datenschutzbeauftragten wegen mangelnder Sachkunde verlangt. Eine Abberufung kommt bei mangelhafter Sachkunde oder fehlender Unabhängigkeit in Betracht. Ein Grund könnte sein, dass Unternehmen bereits auf den Hinweis der Aufsichtsbehörden ihrerseits den betrieblichen Datenschutzbeauftragten von seinen Pflichten entbunden haben, um einer formellen Abberufung zuvorzukommen. Weiterhin wird die Fachkunde und Zuverlässigkeit eines betrieblichen Datenschutzbeauftragten nicht systematisch geprüft, so dass mangelnde Qualifikation oder Interessenskonflikte nicht auffallen. Unternehmen, die einen Datenschutzbeauftragten bestellen müssen, haben meist nur wenige Möglichkeiten, die vom Gesetzgeber erwartete Fachkunde desselben zu prüfen. Als Qualitätsmerkmal für Datenschutzbeauftragte hat deshalb der Berufsverband der Datenschutzbeauftragten (BvD) e.V. ein berufliches Leitbild erstellt, auf das sich seine Mitglieder verpflichten können.[37] Es stellt die Fachkunde und Zuverlässigkeit sicher. Darauf verpflichtete Datenschutzbeauftragte erfüllen damit die Anforderungen des Düsseldorfer Kreises an den betrieblichen Datenschutzbeauftragten.[38]

Sieben Aufsichtsbehörden haben uns die Anzahl und Summe der verhängten Bußgelder mitgeteilt. Es handelt sich teilweise um andere Behörden als im vergangenen XAMIT Datenschutzbarometer. Deshalb ist ein Vergleich mit 2010 nur eingeschränkt möglich.

Im Jahr 2011 wurden insgesamt 66 (2010: 50) Bußgelder von zusammen 219.395 Euro (2010: 554.740 Euro) verhängt. Davon sind 167.640 Euro rechtskräftig. Tabelle 3 zeigt eine Rangliste der verhängten Bußgelder nach Bundesländern in absteigender Reihenfolge. Dabei macht der erste Rang (Schleswig-Holstein) 43% der Gesamtsumme an Bußgeldern in 2011 aus.

Rang	Bundesland
1	Schleswig-Holstein
2	Nordrhein-Westfalen
3	Berlin
4	Sachsen
5	Hamburg
6	Rheinland-Pfalz
7	Sachsen-Anhalt
k. A.	Übrige Bundesländer

Tabelle 3: Rangliste der verhängten Bußgelder (rechtskräftige und nicht rechtskräftige) gegen nicht-öffentliche Stellen nach Bundesländern

[37] URL: https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/leitbild/bvd-leitbild-2011.pdf. Letzter Zugriff: 2012-12-03.
[38] Düsseldorfer Kreis: Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG). 2010. URL: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.html?nn=409242. Letzter Zugriff: 2012-12-03.

Abbildung 15 zeigt die Entwicklung der Bußgelder seit 2004, sofern diese öffentlich bekannt geworden sind. Die Summen sinken seit 2008. Auf der anderen Seite hat die Anzahl der bekannt gewordenen Bußgelder von 2010 zu 2011 zugenommen, obwohl weniger Behörden geantwortet haben. Das könnte bedeuten, dass ein Bußgeld weniger für spektakuläre Fälle eingesetzt wird, sondern als unterstützende Sanktion im Alltag.

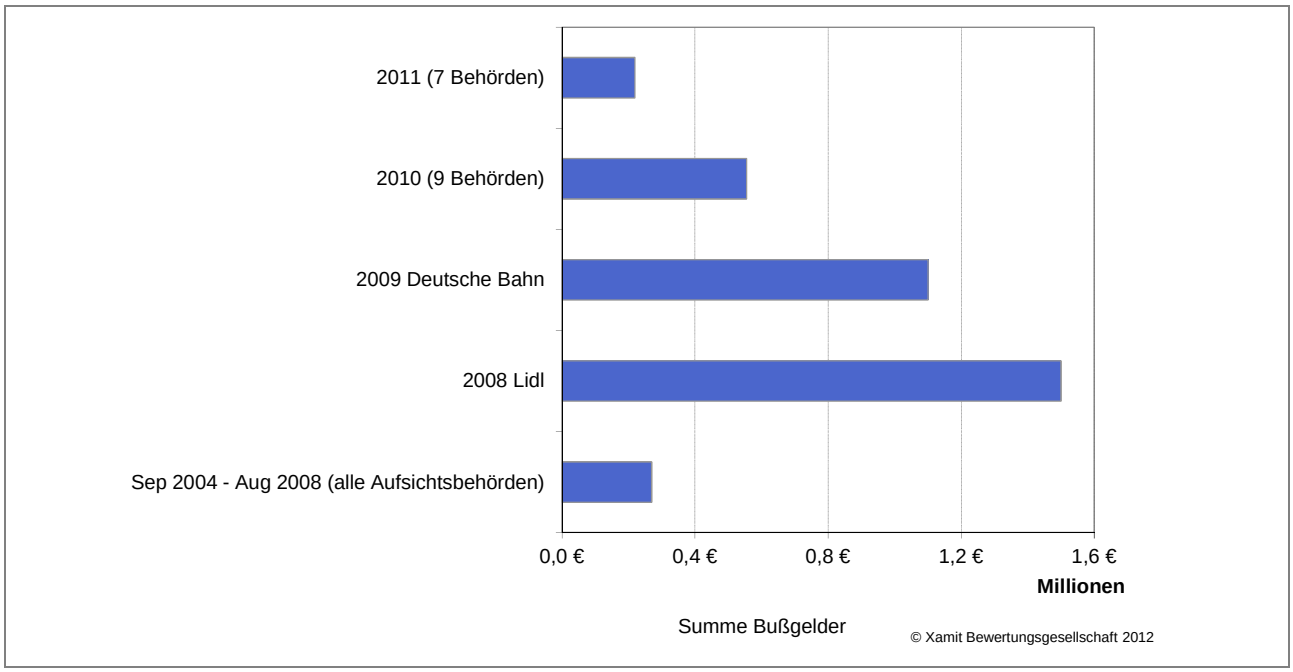


Abbildung 15: Vergleich Bußgelder[39] [40] [41]

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit erließ 2011 zusätzlich 8 Strafanträge.

6.2.4 Erfolge im Jahr 2011

Einige Aufsichtsbehörden haben uns ihre größten Erfolge 2011 mitgeteilt. Diese werfen ein Schlaglicht auf weitere Tätigkeiten, die Aufsichtsbehörden ausüben.

2011 war für die meisten Aufsichtsbehörden eine Zäsur, die durch einen neuen aufsichtsrechtlichen Rahmen und die Zusammenführung von Behörden bzw. die Übernahme eines neuen Tätigkeitsbereichs geprägt war. Vor diesem Hintergrund freut sich der Hessische Datenschutzbeauftragte, Prof. Dr. Michael Ronellenfitsch, über die Zusammenlegung der Datenschutzaufsicht in Hessen.

Ulrich Lepper, der Landesdatenschutzbeauftragte von NRW, sieht, dass Datenschutz aus vielen kleinen Schritte besteht:

[39] Die Angaben für die Bußgelder 2004 bis 2008 sind entnommen aus: SEIFFERT, Evelyn: Datenschutzprüfung durch die Aufsichtsbehörden. Frechen: 2., völlig neu bearb. Aufl. Aufl. Datakontext, 2009. – 9783895775413. S. 21 ff. Berechnung der Summe durch Xamit.

[40] FAZ (2008): Lidl soll 1,5 Millionen Euro Bußgeld zahlen. 11.09.2008. URL: http://www.faz.net/aktuell/wirtschaft/unternehmen/bespitzelung-von-mitarbeitern-lidl-soll-1-5-millionen-euro-bussgeld-zahlen-1694753.html. Letzter Zugriff: 2012-12-03.

[41] eRecht24 (2009): Datenschutz-Affäre: Bußgeld in Millionenhöhe für Deutsche Bahn AG. URL: http://www.e-recht24.de/news/datenschutz/6065-datenschutz-bussgeld-bahn.html. Letzter zugriff: 2012-11-02.

> *„Erfolgreich bin ich, wenn Datenschutzmängel wegen meiner Tätigkeit beseitigt werden. Das war 2011 vielfach der Fall. Erfolgreich bin ich aber auch dann, wenn wegen meiner Tätigkeit schon gar keine potenziellen Datenschutzmängel auftreten. Dieser Erfolg läßt sich zwar selten kausal nachweisen, ich bin aber überzeugt, dass die Sensibilität für Datenschutzfragen bei Unternehmen und Behörden, Politik und Gesellschaft sowie bei vielen Bürgerinnen und Bürgern immer größer wird."*

Herr Wagner, Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, nennt als größten Erfolg das Projekt „Schülerworkshop". Seit 2010 bietet seine Behörde Schulen 4-stündige Schülerworkshops zum Thema „Datenverantwortung und Datenschutz" an. 19 externe Honorarkräfte haben ca. 500 Workshops durchgeführt. Ab dem Schuljahr 2012/2013 wird das Projekt auf Grundschulen ausgeweitet.

Datenschutzrechtliche Einschätzungen von Aufsichtsbehörden treffen bei den betroffenen Unternehmen oder öffentlichen Einrichtungen nicht immer auf Zustimmung. Manchmal entscheidet dann ein Gericht. So auch im Streit über die „Hausarztzentrierte Versorgung". Nach einem Beschluss des Oberverwaltungsgerichts Schleswig-Holstein[42] verstoße der Vertrag zwischen den Leistungserbringern (Hausärzteverband Schleswig-Holstein, Ärztegenossenschaft) und einigen Krankenkassen (AOK NordWest, IKK Landesverband Nord, Landwirtschaftlichen Krankenkasse Schleswig-Holstein und Hamburg) geschlossene Vertrag gegen gesetzliche Vorgaben, nach denen der überwiegende Teil des Datenbestandes beim Auftraggeber verbleiben müsse. Damit bestätigte das Gericht die Richtigkeit einer Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an den Hausärzteverband Schleswig-Holstein.[43]

Wenn ausländische Unternehmen in Europa personenbezogene Daten verarbeiten wollen, treten mitunter Konflikte zwischen der europäischen und deutschen Rechtslage auf der einen Seite und dem Recht im Heimatland auf der anderen Seite auf. Facebook ist ein Beispiel (vgl. Kapitel 2.5). Wenn direkte Sanktionsinstrumente fehlen, hilft manchmal öffentlicher Druck. Diesen erzeugt das ULD durch zahlreiche Aktivitäten, die „dazu führte[n], dass mittlerweile Facebook und die FTC [„Federal Trade Commission", die Redaktion] auf ULD-Schreiben reagieren und die deutschen Datenschützer sichtbarer geworden sind".

[42] Schleswig-Holsteinisches Oberverwaltungsgericht. Beschluss vom 12.01.2011, Az. 4 MB 56/10 und 14 B43/10.
[43] ULD (2011): 33. Tätigkeitsbericht des ULD (2010). Landtagsdrucksache 17/1220. URL: https://www.datenschutzzentrum.de/material/tb/tb33/kap04_5.htm#453. Letzter Zugriff: 2012-12-03.

7 Betroffenenauskunft: 29% beantworten Briefe vollständig

Das informationelle Selbstbestimmungsrecht beschreibt, das im Grundsatz jeder Mensch selber entscheidet, wer was über ihn wissen soll. Zahlreiche Gesetze greifen in dieses Recht ein, so dass keine schrankenlose Verfügungsgewalt besteht. Als Ausgleich erhält der betroffene Mensch ein Auskunftsrecht. Jede nicht-öffentliche Stelle (z.B. Unternehmen, Vereine und Parteien) muss auf Anfrage alle gespeicherten Daten der betroffenen Person gegenüber offenlegen. Nur in Ausnahmen können Angaben zurückgehalten werden (vgl. § 34 BDSG). Das Auskunftsrecht schafft für die betroffenen Personen Transparenz, welche Daten verarbeitet werden, wohin diese übermittelt werden und ob sie richtig sind. Damit kommt ihm eine zentrale Rolle im Datenschutz zu.

Wir wollten wissen, wie erfolgreich sich das Auskunftsrecht im Alltag anwenden lässt. Dazu haben wir 11 Hotels und zwei Rabattsysteme um Auskunft gebeten. Jedes Unternehmen wurde von einer Person – und eins von zweien – per Brief oder E-Mail angeschrieben, d.h. in Summe wurde 14 Anfragen gestellt. Die Person hatte vorher Leistungen des Unternehmens in Anspruch genommen, so dass zu erwarten war, dass personenbezogene Daten vorhanden sind.

Ohne Bezug auf die gesetzliche Grundlage zu nehmen, baten wir um folgende Angaben, die den Vorgaben von § 34 Abs. 1 BDSG folgen:

- Gespeicherte Daten,
- Herkunft der Daten,
- Empfänger der Daten und
- Zwecke der Erhebung, Speicherung und Nutzung.

Weiterhin haben wir nach dem (öffentlichen) Verfahrensverzeichnis gefragt. Das Verfahrensverzeichnis beschreibt

- den Zweck der Datenverarbeitung,
- die Rechtsgrundlage,
- wer die Daten verarbeitet,
- welche Daten verarbeitet werden,
- von wem Daten verarbeitet werden und
- wohin die Daten übermittelt werden.

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), um jedermann in die Lage zu versetzen, sich ein Bild über die verarbeiteten personenbezogenen Daten zu machen.

Wir bewerten, ob die gewünschten Informationen mitgeteilt wurden. Eine rechtliche Bewertung der Antworten, insbesondere die Zulässigkeit der Zwecke, erfolgt nicht.

Ein Hotel kontaktierte den Auskunftsersuchenden, um sich zu vergewissern, dass sie die Daten der richtigen Person beauskunften. Die Privatanschrift war fehlerhaft. Daraufhin erhielt das Unternehmen eine kurze Hilfestellung, welche Angaben eine Antwort enthalten sollte.

Das von zwei Personen angeschriebene Rabattsystem benötigte für eine Antwort 55 Tage. Das zweite Rabattsystem reagiert gar nicht. Von den Hotels antworteten 91%. Leider aber nicht immer mit der erbetenen Auskunft. Abbildung 16 zeigt für beide Branchen zusammen die Qualität der Antworten. Nur 29% der angeschriebenen Unternehmen haben konkret die gespeicherten Daten

genannt und ein Verfahrensverzeichnis beigelegt oder auf die Onlineversion verwiesen. 36% antworteten ohne die gespeicherten Daten konkret zu nennen.

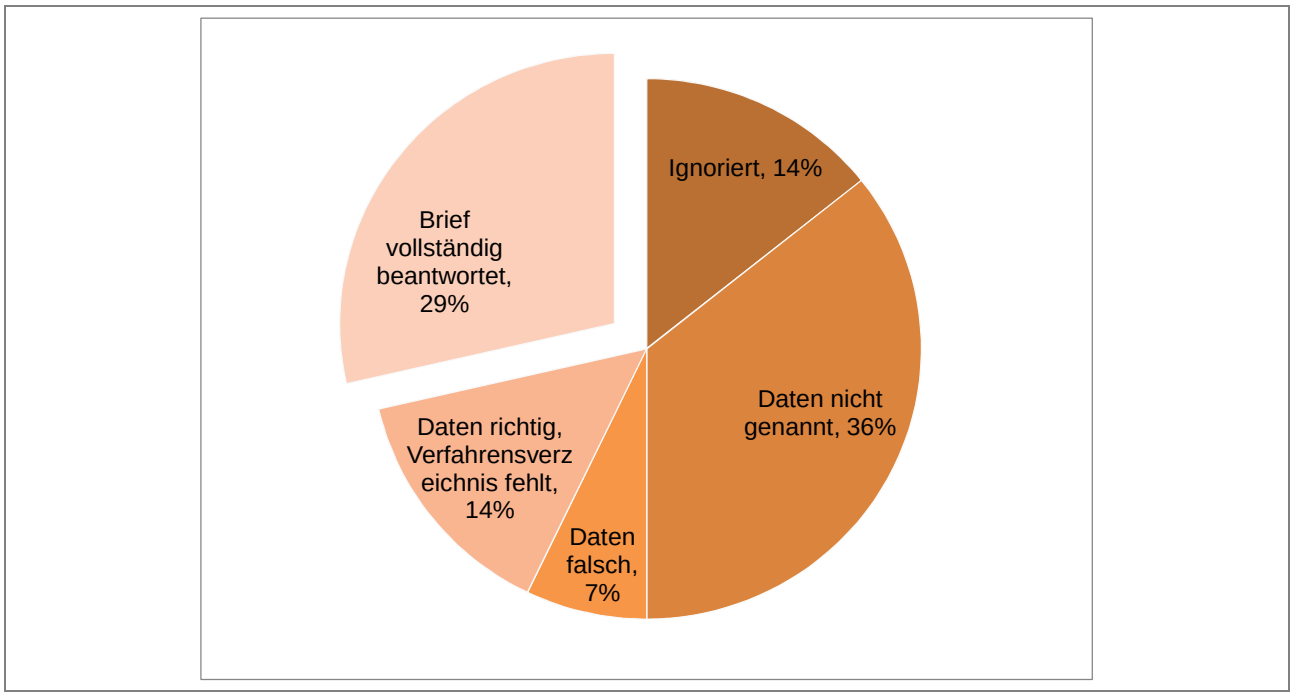


Abbildung 16: Reaktionen auf Auskunftsbegehren

Diese nicht repräsentative Erhebung beleuchtet, wie wichtig es ist, Datenschutz in Unternehmensabläufe zu integrieren. Datenschutzkonformität erschöpft sich nicht in der Bestellung eines Datenschutzbeauftragten. Die Bestellung ist vielmehr der Anfang. Die eigentliche Datenschutzkonformität lässt sich ausschließlich erreichen, indem Datenschutzvorgaben in jeden Ablauf im Unternehmen integriert werden. Für die Betroffenenauskunft heißt das bspw.:

- Mustertexte für die Antwort erstellen, die Zwecke, Datenherkunft, Datenempfänger und für die Kür die Löschfristen enthalten.
- Ein Verzeichnis über die Speicherorte von personenbezogenen Daten erstellen, damit alle Daten beauskunftet werden können.
- Den mit der Beantwortung beauftragten Mitarbeiter Lesezugriffe auf die Datenbanken geben, aus denen die Daten beauskunftet werden sollen.
- Den Ablauf einer Auskunft in Arbeitsanweisungen festlegen.
- Die Mitarbeiter schulen.

Der Lohn der Mühe ist nicht nur ein rechtskonformes Handeln, sondern ein positiver Eindruck beim Kunden. Was erzeugt mehr Vertrauen: eine umfassende Auskunft oder ein Abspeisen mit Floskeln wie „wir nehmen Datenschutz ernst“?

Das Hotel „Alexander Plaza Berlin Mitte“ fiel uns besonders positiv auf, da die Zwecke, Datenübermittlung und Löschfristen ausführlich erläutert wurden.

Ein Rabattsystem stach durch seinen herablassenden Ton hervor: „Wir können nachvollziehen und befürworten, dass Sie sich als moderner Verbraucher über das Thema Datenschutz Gedanken machen.“ Ein Verfahrensverzeichnis erhielten wir nicht.

Wie wichtig Schulung ist, demonstrierte ein Hotel. Eine sichtlich um das Kundenwohl bemühte Mitarbeiterin versuchte telefonisch die Datenlage zu erklären. Ihr Unwissen, wie sie mit der Anfrage umgehen soll, führte sie hörbar in die Verzweiflung. Dabei vergaß sie, sich zu vergewissern, ob sie mit der um Auskunft ersuchenden Person sprach. Geduldig hörte der Anrufbeantworter eines Familienanschlusses zu.

8 Fazit

Fünf Jahre Datenschutzbarometer sind auch fünf Jahre zunehmende Datenschutzverstöße im Internet (Abbildung 17). Nach unserer Beobachtung gehen Unternehmen, Behörden und Vereine im Internet nicht sorgloser mit denen ihnen anvertrauten Daten um als außerhalb des Internets.

Täter sind aber nicht nur Unternehmen mit Geschäftsmodellen, die auf Datenschutzverstößen nach deutschem Recht aufbauen,[44] sondern ein breites Spektrum an Unternehmen, Behörden, Stadtverwaltungen usw.

Datenschutzverstöße gedeihen, weil

- sie meistens im Verborgenen passieren,
- für die Betroffenen keine unmittelbar spürbare negative Konsequenz („Schmerz“) hervorrufen,
- der Aufwand für den Betroffenen sich zu wehren seine juristischen Kenntnisse oder finanziellen Mittel übersteigt,
- der Verfolgungsdruck unmerklich ist und
- die Sanktionen nicht schmerzen.

Wir sprechen hier nicht von den Verstößen, die einer unsicheren Rechtslage oder der Praxisferne des Bundesdatenschutzgesetzes geschuldet sind, sondern von den bewusst oder fahrlässig begangenen Verstößen, wie eine Nutzung von Google Analytics ohne Anonymisierung oder die Missachtung eines Auskunftsbegehrens.

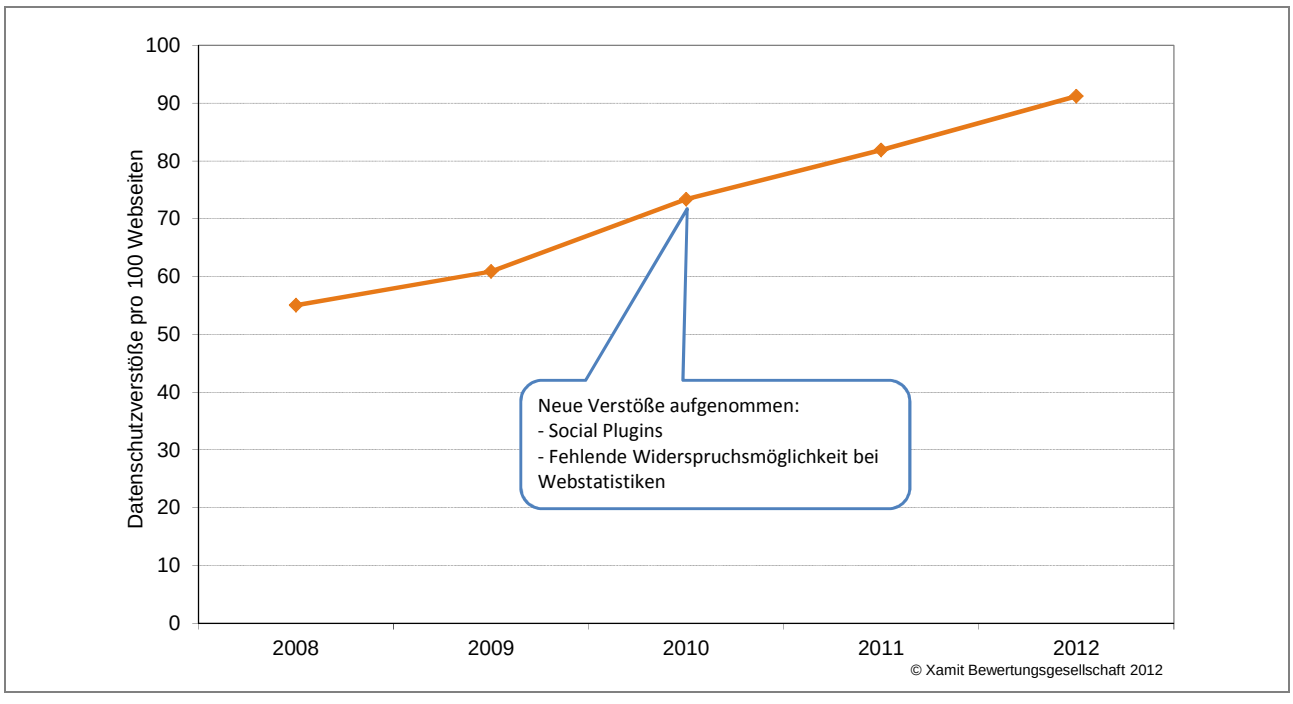


Abbildung 17: Entwicklung der Datenschutzverstöße seit 2008

[44] Weichert, Thilo (2012): Datenschutzverstoß als Geschäftsmodell – der Fall Facebook. In: Datenschutz und Datensicherheit. Nr. 10, 2012. S. 716-721.

Das A und O für einen durchsetzungsstarken Datenschutz ist einerseits die innerbetriebliche Selbstkontrolle durch fachkompetentes Datenschutzpersonal. Diese hat jedoch nur begrenzte Reichweite, solange die Datenschutz-Aufsichtsbehörden wegen mangelnder Ressourcen nicht unterstützend eingreifen können. Daher bleibt – wie auch schon in den letzten Jahren – die Forderung nach besserer Ausstattung der Behörden durch die Landesregierungen, damit der Datenschutz in Deutschland kein Papiertiger ist.

9 Anhang

Im Rahmen dieses Kapitels werden die aus den Ergebnissen resultierenden Handlungsempfehlungen für Webseiten-Betreiber (Kapitel 9.1) und Webseiten-Besucher (Kapitel 9.2) zusammengefasst.

9.1 Webseiten-Betreiber

Unternehmen, die ein kundenfreundliches und Vertrauen bildendes Image bevorzugen, sollten genau prüfen, welche Signale Ihre Webpräsenz an Besucher aussendet. Sobald

- ein Kontaktformular verwendet,
- Werbung Dritter angezeigt oder
- eine Webstatistik angefertigt wird,

darf eine Datenschutzerklärung nicht fehlen. Eine Datenschutzerklärung sollte

- verständlich formuliert sein,
- den Zweck für die Datennutzung angeben,
- die Zusendung von Werbung regeln,
- die Übermittlung an Dritte erläutern,
- direkt im Umfeld des Kontaktformulars, der Newsletteranmeldung etc. platziert sein oder durch einen gut sichtbaren und erkennbaren Link erreichbar sein und
- im vorbildlichen Fall auf das Auskunftsrecht oder das Widerspruchsrecht mit Wirkung für die Zukunft hinweisen.

Wer einen externen Dienstleister für die Webstatistik beauftragt, sollte einen Vertrag abschließen, der die Datenschutzrechte sichert und festlegt, ob und in welchem Umfang der Dienstleister die erhobenen Daten für eigene Zwecke nutzen darf. Ein solcher Vertrag ermöglicht eine Datenverarbeitung im Auftrag gemäß § 11 BDSG, für die das Datenschutzrecht Privilegien vorsieht. Eine Zustimmung zu der Dienstleister-AGB ohne weiteren Vertrag reicht im Regelfall nicht aus.

Wer personenbezogene Daten in einer Datenbank sammelt (z. B. in einem Webshop), geht eine besondere Verpflichtung ein. Diese Daten müssen sicher aufbewahrt und vor den neugierigen Augen Unbefugter geschützt werden. Wer veraltete Software (PHP, Shop-Software) nutzt, lässt Sicherheitslücken offen, die zu einem Datendiebstahl einladen. Suchmaschinen helfen, potentielle Opfer schnell zu finden. Der nachfolgende Angriff läuft dann teilweise vollautomatisch ab. Die Haltung „Mein Shop ist klein. Wer will bei mir einbrechen?“ gefährdet die Existenz des Unternehmens.

Weiterführende Informationen zu Webstatistiken und Kontaktformularen finden Sie in unseren Studien[45]:

[45] Kostenfreier Download: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php

- „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“,
- „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen – Kontaktformulare und Datenschutz“ und
- „Webstatistiken im Test – Welcher Dienst ist in Deutschland legal?“, 8. Update vom 4. Oktober 2011.

9.2 Webseiten-Besucher

Ein Website-Besucher hat zwar keinen direkten Einfluss auf die Art und Weise der Datenverarbeitung durch den Betreiber, doch kann er durch sein (Surf-)Verhalten vorbildliche Webpräsenzen unterstützen und somit auch seine eigenen Daten schützen. In Ermangelung wirksamer Standards und Kontrollen hilft nur Selbstschutz:

- Datenschutzerklärungen lesen,
- Betreiber ohne eine nach persönlicher Einschätzung akzeptable Datenschutzerklärung meiden,
- Dateneingaben auf das erkennbare Minimum reduzieren und Pflichtfelder im Zweifel mit sinnlosen Eingaben zufriedenstellen,
- Schwarze Schafe bei der zuständigen Aufsichtsbehörde[46] oder den Verbraucherzentralen[47] anzeigen.

Jeder Mensch und jedes Unternehmen hat Geheimnisse. Alle Informationen, die nicht für die Öffentlichkeit bestimmt sind, brauchen Schutz. Wer will seine Krankengeschichte im Internet lesen? Welches Unternehmen will seine Forschungspläne mit der Konkurrenz teilen? Bereits mit einfachen und kostenlosen Mitteln können Privatpersonen und Unternehmen ihre Surfspuren verringern:

- Browser so einstellen, dass Cookies höchstens für die aktuelle Sitzung angenommen werden.[48]
- Bei sensiblen Themen einen Anonymisierungsdienst verwenden.[49]
- Bei Nutzung von Mozilla Firefox die Skripte selektiv mit der Firefox-Erweiterung „noscript“ [50] steuern, so dass Cookies von Google und Co. gar nicht erst gesetzt werden können und der Like-Button von Facebook ebenfalls gar nicht erst angezeigt wird. Ein vergleichbares Werkzeug ist uns für den Internet Explorer nicht bekannt.

[46] Jedes Bundesland hat eine eigene Aufsichtsbehörde für den Datenschutz. Eine entsprechende Liste stellt der „Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ zur Verfügung. URL: http://www.bfdi.bund.de/cln_136/DE/AnschriftenUndLinks/AnschriftenUndLinks_node.html. Letzter Zugriff: 2012-12-03.

[47] URL: http://www.verbraucherzentrale.de. Letzter Zugriff: 2012-12-03.

[48] Anleitungen für unterschiedliche Browser finden Sie im Internet. Bspw. hier: http://www.informationelle-selbstbestimmung-im-internet.de/node4.html. Letzter Zugriff: 2012-12-03.

[49] Kostenlos und relativ einfach zu installieren ist Jondonym (https://www.jondos.org). Von dem Dienst Tor raten wir ab, da er gerne genutzt wird, um Passwörter auszuspähen.

[50] Zu viele Webpräsenzen benötigen Skripte, um zu funktionieren. Deshalb stößt ein generelles Abschalten schnell an praktikable Grenzen. Bezugsquelle: http://www.erweiterungen.de/detail/NoScript. Letzter Zugriff: 2012-12-03.

- Das Add on „Ghostery“[51] blockiert den Tracking-Code von Webstatistikdiensten und Elemente, wie den Facebook Like-Button. Es arbeitet automatisch und ist deshalb komfortabler, als noscript zu bedienen.

- Keine Toolbar von Google, Yahoo, Alexis u. a. im Browser einsetzen, da diese Toolbars das Surfverhalten protokollieren.

[51] Bezugsquelle: http://www.ghostery.com. Letzter Zugriff: 2012-12-03.

10 Weitere Studien von XAMIT zum Thema Datenschutz

Alle Studien und ausgewählte Fachbeiträge finden Sie als kostenlosen Download auf unserer Webpräsenz.[52]

Datenschutzbarometer 2011: Milliardengewinne durch Datenschutzverstöße

XAMIT führte im Rahmen des Datenschutz-Barometers 2011 eine umfassende Überprüfung von mehr als 37.000 Webpräsenzen von in Deutschland ansässigen Unternehmen, politischen Organisationen, Gemeinden und Vereinen durch. Insgesamt wurden über 3,2 Millionen Webseiten auf die Einhaltung geltender Datenschutzbestimmungen hin untersucht. Im Durchschnitt wurden 82 Verstöße pro 100 Webseiten gefunden, das ist eine Steigerung von 12% gegenüber 2010. Außerdem wurden die deutschen Aufsichtsbehörden zu ihrer Stellenanzahl, ihren Erfolgen und weiteren Tätigkeiten befragt.

Webstatistiken im Test – Welcher Dienst ist in Deutschland legal? – 8. Update vom 4. Oktober 2011

XAMIT hat die in Deutschland populärsten Webstatistik-Dienstleister untersucht, ob sie eine datenschutzkonforme Webstatistik anbieten. Insgesamt decken die elf untersuchten Statistikdienstleister mehr als 91% des Marktes ab.

Datenschutzbarometer 2009 – (kein) Datenschutz in Deutschland

Für das Datenschutzbarometer 2009 wurden alle 23 den Ländern unterstehenden Aufsichtsbehörden angeschrieben und ihre Stellenanzahl in Vollzeitäquivalenten erfragt. Das Ergebnis: Ein Unternehmen muss - statistisch betrachtet - alle 39.400 Jahre mit einer Datenschutzüberprüfung rechnen. Außerdem wurden 24.376 deutsche Webpräsenzen auf die Einhaltung geltender Datenschutzbestimmungen untersucht. 61 von 100 Webseiten verstoßen gegen geltendes Datenschutzrecht oder bieten Grund zur Beanstandung.

Parteien und Datenschutz - Datenschutzpraxis deutscher Parteien und parteinaher Organisationen

Keine der im Bundestag vertretenen Parteien handelt beim Thema Datenschutz uneingeschränkt gesetzeskonform. Untersucht wurden u. a. der Umgang mit Online-Spenden oder das Vorhandensein eines datenschutzrechtlich vorgeschriebenen Verfahrensverzeichnisses. In Summe werden etwa ein Drittel der denkbaren Verstöße auch begangen. Das heißt, entsprechende gesetzliche Vorschriften werden von den Parteien und deren verwandten Organisationen vielfach ignoriert.

Datenschutzbarometer 2009

Für das Datenschutzbarometer 2009 wurden alle 23 den Ländern unterstehenden Aufsichtsbehörden angeschrieben und ihre Stellenanzahl in Vollzeitäquivalenten erfragt. Das Ergebnis: Ein Unternehmen muss - statistisch betrachtet - alle 39.400 Jahre mit einer Datenschutzüberprüfung rechnen. Außerdem wurden 24.376 deutsche Webpräsenzen auf die Einhaltung geltender Datenschutzbestimmungen untersucht. 61 von 100 Webseiten verstoßen gegen geltendes Datenschutzrecht oder bieten Grund zur Beanstandung.

[52] http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php

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?

11 Beiträge von XAMIT in Büchern und Fachmedien

Datenschutzverstöße und Vollzugsdefizite. Datenschutz und Datensicherheit 03/2012

Datenschutzbarometer 2011: Ungebrochener Trend zu mehr Datenschutzverstößen. BvD-News 1/2012

Vom Datum zum Dossier. Heise Zeitschriften Verlag, 2011. EAN: 9783936931709.

Datenschutzverstöße im Internet. Datenschutz und Datensicherheit 10/2011.

Vorsicht Falle: Einbindung von Empfehlungen auf die eigene Webseite. BvD-News 2/2011.

Messung des Datenschutz-Vollzugsdefizits. Datenschutz und Datensicherheit 10/2010.

Nur ein Vollzugsdefizit? – Parteien vernachlässigen den Datenschutz. FIfF-Kommunikation 4/2009.

Datenschutz im Internet: Ergebnisse des XAMIT Datenschutzbarometers 2008. Datenschutz und Datensicherheit 10/2009.

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 2008

Datenschutz bei Webstatistiken. Datenschutz und Datensicherheit 4/2008.

XAMIT – der Spezialist für Datenschutz und IT-Sicherheit

Die Anforderungen an Unternehmen im Bereich IT-Sicherheit und Datenschutz steigen ständig. Mangelnde Compliance ist ein Risiko, das sich kein Unternehmen leisten kann.

XAMIT minimiert Ihre Risiken. So werden Unternehmenswerte geschützt und die Kosten bleiben im Rahmen.

Leistungen

- Stellung von Datenschutzbeauftragten (TÜV-geprüft)
- Begleitung bei Genehmigungsverfahren und meldepflichtigen Vorfällen
- Beratung bei Datenschutzprüfungen durch Aufsichtsbehörden
- Datenschutz in internationalen Konzernen
- Internet-Datenschutz

- Begleitung und Durchführung von Audits und IT-Prüfungen
- Ermittlung von Compliance-Verstößen und Sicherheitslücken, Klassifikation der Risiken
- IT-Controlling
- Interimsmanagement
- Beratung und Schulung

Ihre Vorteile mit XAMIT

- gebündelte Themen- und Branchen-Erfahrung, insbesondere Telekommunikation, Banken, Handel und Werbung
- Experten-Team aus Informatikern, Betriebswirten, Juristen und Pädagogen
- anerkanntes und geprüftes Fachwissen
- neutral und unabhängig von Herstellern
- die Kosten im Blick für unternehmerisch sinnvolle Lösungen

Schützen Sie Ihren Erfolg. Sprechen Sie uns an.

XAMIT Bewertungsgesellschaft mbH
Datenschutz ▪ Audits ▪ IT-Projekte

Monschauer Str. 12
40549 Düsseldorf

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

www.xamit.de
info@xamit.de