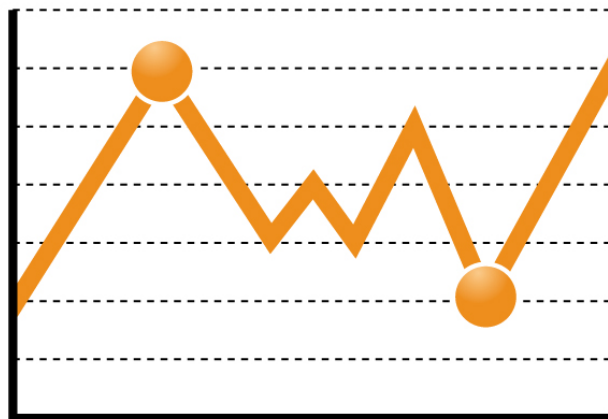




DATENSCHUTZBAROMETER 2011

Datenschutzverstöße, ein Milliardenbusiness



Datenschutz

Barometer

Impressum

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

© XAMIT Bewertungsgesellschaft mbH 2011

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

Rechtliche Hinweise

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

Inhaltsverzeichnis

1	EINLEITUNG	1
2	HINTERGRUND	5
2.1	Webshops	5
2.2	Webstatistiken	6
2.3	Internet-Werbung	7
2.4	Kontaktformulare	8
2.5	Facebook Like-Button	9
3	GEGENSTAND UND METHODE DES DATENSCHUTZBAROMETERS 2011	13
3.1	Einbindung eines Webshops	14
3.2	Einbindung von Google Adsense	14
3.3	Webstatistiken, Nutzer-Hinweis und Möglichkeiten zum Widerspruch	14
3.4	Einbindung von Kontaktformularen	15
3.5	Einbindung des Facebook Like-Buttons	15
4	ERGEBNISSE	17
4.1	Risiko durch veraltete Software	17
4.2	Google Adsense – Daten werden heimlich übertragen	19
4.3	Webstatistik – Licht und Schatten	19
4.4	Kontaktformulare – Datenverarbeitung oft ohne Erklärung	24
4.5	Facebook Like-Button: Gefällt uns gar nicht	25
5	DAS XAMIT DATENSCHUTZBAROMETER 2011	27
6	AUSSTATTUNG UND ERFOLGE DER DEUTSCHEN DATENSCHUTZAUF SICHT	31
6.1	Unabhängig sollt ihr sein	31
6.2	Personelle Ausstattung im Jahr 2011	34
6.3	Tätigkeiten und Erfolge	38
6.3.1	Datenschutzberatung und Eingaben im Jahr 2010	39
6.3.2	Kontrollen im Jahr 2010	41
6.3.3	Sanktionen im Jahr 2010	41
6.3.4	Erfolge im Jahr 2010	45
7	VERZERRTER WETTBEWERB: MILLIARDENGEWINNE DANK DATENSCHUTZVERSTÖßE	49
8	FAZIT	53
9	ANHANG	55
9.1	Webseiten-Betreiber	55
9.2	Webseiten-Besucher	56
10	WEITERE STUDIEN VON XAMIT ZUM THEMA DATENSCHUTZ	58
11	BEITRÄGE VON XAMIT IN BÜCHERN UND FACHMEDIEN	60

1 Einleitung

Im April 2011 waren für 100 Millionen Kunden von Sony die Folgen einer vernachlässigten IT-Sicherheit hautnah zu spüren. Unbekannte hatten sich Zugriff auf die persönlichen Daten von Kunden des Playstation Networks (PSN), des Musikdiensts Qriocity und von Sony Online Entertainment (SOE) verschafft.¹ Nicht nur dieser Vorfall zeigt, dass mangelnde IT-Sicherheit weiterhin die Privatsphäre und das Vermögen von Menschen bedroht:

- 2,7 Mio. US-Dollar durch Kundendatendiebstahl bei Citibank erbeutet²
- Daten von über einer Million Gewinnspielteilnehmern bei Neckermann.de gestohlen³
- Datenklau bei Software-Hersteller Ashampoo⁴
- EU stoppt Emissionsrechtehandel wegen gravierender Sicherheitsprobleme⁵
- Gezielter Angriff auf Kunden von K&M-Elektronik⁶
- Bankdaten tausender Westermann-Kunden gestohlen⁷
- Sensible Mitarbeiterdaten im ungeschützten Zugriff bei der Rheinbahn⁸
- Hacker klauen Kundendaten von Marktkauf⁹
- Gema offenbar gleich mehrfach gehackt¹⁰
- Mitgliederdaten der CDU geklaut¹¹

Auch wenn finanzielle Schäden und verletzte Privatsphären durch mangelhafte IT-Sicherheit mittlerweile häufig publik werden, stellen sie nur einen Teil der alltäglichen Datenschutzverstöße dar. Ein Betroffener ist heute nicht mehr in der Lage zu überblicken, wer seine Daten wie verwendet. Damit sind sie kaum in der Lage, eine ungesetzliche Verarbeitung zu erkennen. So sind auch Fälle von illegaler Datenerhebung und -nutzung von Organisationen, denen Menschen vertrauten, wie z. B. Arbeitgeber, Banken oder Gesundheits-

¹ Heise Online (2011): Sony-Chef entschuldigt sich – Update. 06.05.2011. URL: <http://heise.de/-1238585>. Letzter Zugriff: 2011-11-24.

² Heise Online (2011): Datendiebe erbeuten 2,7 Millionen US-Dollar von Citibank-Kunden. 26.06.2011. URL: <http://heise.de/-1268108>. Letzter Zugriff: 2011-11-25.

³ Heise Online (2011): Daten von über einer Million Kunden bei Neckermann.de gestohlen. 31.05.2011. URL: <http://heise.de/-1253010>. Letzter Zugriff: 2011-11-24.

⁴ Heise Online (2011): Datenklau bei Ashampoo . 20.04.2011. URL: <http://heise.de/-1230523>. Letzter Zugriff: 2011-11-24.

⁵ Heise Online (2011): EU stoppt Emissionsrechtehandel wegen gravierender Sicherheitsprobleme. 20.01.2011. URL: <http://heise.de/-1172352>. Letzter Zugriff: 2011-11-24.

⁶ Heise Online (2011): Gezielter Angriff auf Kunden von K&M-Elektronik. 22.06.2011. URL: <http://heise.de/-1265222>. Letzter Zugriff: 2011-11-24.

⁷ Heise Online (2011): Bankdaten tausender Westermann-Kunden abgefischt. 08.07.2011. URL: <http://heise.de/-1276189>. Letzter Zugriff: 2011-11-24.

⁸ RP Online (2011): Daten-Panne erschüttert die Rheinbahn. 16.07.2011. URL: <http://nachrichten.rp-online.de/titelseite/daten-panne-erschuettert-die-rheinbahn-1.1333672>. Letzter Zugriff: 2011-11-24.

⁹ Hamburger Morgenpost (2011): Hacker klauen Kundendaten von Marktkauf. 31.07.2011. URL: <http://www.mopo.de/nachrichten/eine-million-datensaetze-geklaut-hacker-klauen-kundendaten-von-marktkauf,5067140,8732632.html>. Letzter Zugriff: 2011-11-24.

¹⁰ Heise Online (2011): Gema offenbar gleich mehrfach gehackt. 24.08.2011. URL: <http://heise.de/-1328737>. Letzter Zugriff: 2011-11-24.

¹¹ Heise Online (2011): Mitgliederdaten der CDU geklaut. 26.08.2011. URL: <http://heise.de/-1331876>. Letzter Zugriff: 2011-11-24.

dienstleister publik geworden. Eine Verarbeitung ist ungesetzlich, wenn eine Rechtsgrundlage oder eine Einwilligung des Betroffenen fehlt, wie z. B. bei der Videoüberwachung von Toiletten. Die Folge ist eine hohe Dunkelziffer von Datenschutzverstößen.

Fragwürdiger Umgang mit personenbezogenen Daten ist eine weitere Ursache für Datenschutzverstöße, durch die für die Betroffenen Nachteile entstehen können. Einige Beispiele aus 2011:

- Patientendaten der Arbeiterwohlfahrt im Altpapier¹²
- ADAC Nordbayern spioniert Mitarbeiter aus¹³
- Wittener Zahnarztpraxis entsorgt Patientenakten auf öffentlichem Parkplatz¹⁴
- Datenskandal beim Demminer DRK¹⁵
- Unzulässige Datenübermittlung durch die Easycash GmbH: 60.000 Euro Bußgeld¹⁶

Diese Aufzählungen sind bei weitem nicht vollständig und stellen nur die Spitze des Eisbergs dar.¹⁷ Mit der vorliegenden Untersuchung versucht XAMIT, eine empirische Antwort auf die Frage nach dem Datenschutzniveau in Deutschland insbesondere für das Internet zu finden und so ein möglichst realistisches Bild zu zeichnen. Dabei knüpfen wir methodisch und inhaltlich an unsere bisherigen Studien zum Thema Datenschutz und Internet an¹⁸:

- „Wissen Sie, was Sie tun? Wissen Sie, wer es noch weiß? – Surfen im Internet“ über heimliche Datenerhebung bei Webstatistiken,
- „Wie Unternehmen im Internet bei Konsumenten Misstrauen säen“ über die Transparenz der Datennutzung bei Kontaktformularen,
- XAMIT Datenschutzbarometer 2008, 2009 und 2010 über das Datenschutzniveau im deutschen Internet,
- „Parteien und Datenschutz – Datenschutzpraxis deutscher Parteien und parteinaher Organisationen“ sowie
- „Webstatistiken im Test - Welcher Dienst ist in Deutschland legal?“, 8. Update vom 4. Oktober 2011.

¹² Wedel-Schulauer Tageblatt (2011): Patientendaten im Altpapier. 08.02.2011. URL: <http://www.wedel-schulauer-tageblatt.de/nachrichten/home/top-thema/article//patientendaten-im-altpapier.html>. Letzter Zugriff: 2011-11-24.

¹³ Süddeutsche (2011): Wanzen beim ADAC. 17.03.2011. URL: <http://www.sueddeutsche.de/bayern/mitarbeiter-ausspioniert-wanzen-beim-adac-1.1073031>. Letzter Zugriff: 2011-11-24.

¹⁴ Der Westen (2011): Praxis-Abfall illegal entsorgt. 04.04.2011. URL: <http://www.derwesten.de/staedte/witten/praxis-abfall-illegal-entsorgt-id4503524.html>. Letzter Zugriff: 2011-11-24.

¹⁵ Nordkurier.de (2011): Datenskandal beim Demminer DRK.

¹⁶ Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (2011): NRW-Datenschutzbeauftragter schließt Verfahren gegen die Easycash GmbH mit einem Bußgeld von 60.000 Euro ab. Pressemitteilung vom 12.09.2011. URL: https://www.lidi.nrw.de/mainmenu_Service/submenu_Pressemitteilungsarchiv/Inhalt/PM_Datenschutz/Inhalt/2011/Easycash/Easycash.php. Letzter Zugriff: 2011-11-24.

¹⁷ Weitere Sicherheitsvorfälle finden Sie auf unserer Webseite: <http://www.xamit-leistungen.de/sicherheitsvorfaelle/index.php>.

¹⁸ Kostenfreier Download: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>

Alle Studien stellen den Umgang mit personenbezogenen Daten im Internet in den Vordergrund und untersuchen unter anderem, wie stark Webseitenbetreiber Ihren Besuchern offenlegen, welche Daten erhoben werden und was mit diesen geschieht.

Unsere seit 2009 durchgeführte jährliche Erhebung der Vollzeitäquivalente in den deutschen Datenschutz-Aufsichtsbehörden wird um eine Erhebung ihrer Tätigkeiten und Erfolge erweitert. Die Arbeit, aber auch die Grenzen der Datenschutzaufsicht werden zum ersten Mal umfassender dargestellt.

Mit dem Datenschutzbarometer 2011 stellt XAMIT einen einzigartigen Überblick über das aktuelle Datenschutzniveau im Internet in Deutschland zur Verfügung. XAMIT wiederholt diese Untersuchung regelmäßig und in identischer Form, um die Entwicklung des Datenschutzniveaus vergleichbar zu dokumentieren.

Stellen, Tätigkeiten und Erfolge der Aufsichtsbehörden werden in Kapitel 6 dargestellt

Das Datenschutzbarometer gibt einen Überblick über das Datenschutzniveau im deutschen Internet

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.

Kundenkonten erhöhen
Gefahr eines
Datendiebstahls

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 5.3 sind es bereits 90 Fehler.¹⁹ Um die Sicherheit von Webshops zu gewährleisten, ist es also zwingend notwendig, stets die aktuellen Programmversionen einzusetzen.

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.

¹⁹ Die Entwickler von PHP betreiben unter <http://www.php.net/> eine Fehlerdatenbank. Stand der Abfrage: 2011-10-21.

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.

Von der Einzelstatistik zum komplexen Bewegungsprofil

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 2011.²⁰

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 Werbeunternehmen 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 Werbeunternehmen 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 Werbeunternehmen 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.

Alle Beteiligten bestens im Bilde – nur der Besucher ahnt nichts

²⁰ Kostenfreier Download: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>

Anhand des Angebotes von Google AdSense untersuchen wir nachfolgend, ob Webpräsenzen, die Google AdSense anzeigen, auch eine Datenschutzerklärung besitzen. Google verpflichtet die Nutzer von Google AdSense in § 2.6 der Allgemeinen Geschäftsbedingungen für Google AdSense™ Online, in einer Datenschutzerklärung auf Google AdSense hinzuweisen.²¹ Insbesondere ist laut Google dabei zu erwähnen, dass dieser Dienst einen Cookie setzt.

Selbstverständlich handelt es sich bei Google nicht um den einzigen Anbieter für Website-Werbung. Gleichwohl zählt Google mit den Diensten AdSense und Doubleclick zu den marktführenden und bekanntesten Anbietern und hat in Folge dessen repräsentativen Charakter. Die im Rahmen der Untersuchung ermittelten Ergebnisse sind also auf weitere Werbeunternehmen übertragbar.

2.4 Kontaktformulare

Datenschutzerklärungen machen Datennutzung für den Besucher transparent

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.²² Datenschutzerklärungen liegen deshalb im Eigeninteresse von Unternehmen. Diese sind nach Ansicht von 61% der Bundesbürger jedoch unklar formuliert.²³

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

²¹ Google (2008): Allgemeine Geschäftsbedingungen (AGB) für AdSense. URL: <https://www.google.com/adsense/localized-terms>. Stand: 2011-10-21.

²² 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: 2011-11-25.

²³ Heise Online (2011): Studie: Nutzer fordern mehr Transparenz beim Datenschutz im Netz. 01.06.2011. URL: <http://heise.de/-1253855>. Letzter Zugriff: 2011-11-25.

(BDSG).²⁴ Bei öffentlichen Stellen der Länder gelten die entsprechenden Landesdatenschutzgesetze.

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.²⁵

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“²⁶ ausführlich erläutert und ist im Anhang der vorliegenden Untersuchung zusammengefasst.

Datenschutzerklärung als Entscheidungsgrundlage für Webseitenbesucher

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 Facebook Like-Button

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. Denn Werbetreibende wissen, dass gerade Empfehlungen von Freunden, Bekannten oder Geschäftspartnern bei Kaufentscheidungen viel Gewicht haben. Mittlerweile werden Empfehlungen vielfach online ausgesprochen auf Meinungsportalen oder direkt in einem Online-Shop.

Empfehlungsmarketing mit dem Facebook Like-Button

²⁴ 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

²⁵ Ebd. S. 409

²⁶ Kostenfreier Download: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>

Die klassische Empfehlung wird jedoch noch immer in einem persönlichen Gespräch gegeben und hat in der Regel ungleich mehr Gewicht. Für Werbetreibende hat diese Art der Empfehlung nur einen entscheidenden Haken: Man weiß nicht, wer eine Empfehlung wann für welches Produkt oder welche Dienstleistung abgibt. Deshalb suchen sie nach Möglichkeiten, Empfehlungen einfach und ohne Gespräch zu ermöglichen. Seit 2010 bietet Facebook mit dem sogenannten „Like-Button“ eine solche Möglichkeit an.

Der Betreiber einer Webseite kann einfach einen von Facebook zur Verfügung gestellten Skript-Code einbinden. Besucht der Internetsurfer Max Mustermann eine so vorbereitete Webseite, dann sieht er einen kleinen Button mit einem nach oben gerichteten Daumen, der die Beschriftung „Like“ oder „Gefällt mir“ trägt. Ist Max ein Facebook-Nutzer, könnte er auf diesen Button klicken, um anderen Facebook-Mitgliedern mitzuteilen, dass ihm diese Webseite oder ein Element darauf, etwa ein spannender Bericht, besonders gut gefällt.

Doch was ist inzwischen unbemerkt von Max passiert? Nachdem er die Webadresse in den Browser eingetippt hat, fordert dieser die entsprechende Webseite an. Je nach gewählter Button-Variante ist in der Webseite ein iframe von Facebook oder ein Skript eingebettet. Beide Varianten nehmen über eine von Facebook bereitgestellte Schnittstelle Kontakt mit dem sozialen Netzwerk auf. Welche Daten Facebook nach eigenen Angaben erhebt, hängt nicht nur vom Mitgliedsstatus ab, sondern auch davon, ob Max schon früher einmal facebook.com aufgerufen hatte.²⁷ Facebook erhebt je nach Status des Webseitenbesuchers folgende Daten bzw. setzt folgende Cookies:

Facebook erhebt Daten auch von Nicht-Mitgliedern

- Nicht-Mitglieder, die noch nie facebook.com aufgerufen haben:
 - IP-Nummer (deutsche IP-Nummern werden vor Speicherung anonymisiert).
- Nicht-Mitglieder, die gleichzeitig facebook.com aufgerufen haben:
 - IP-Nummer (deutsche IP-Nummern werden vor Speicherung anonymisiert) und
 - Cookie, der zwei Jahre gültig bleibt.
- Mitglieder (zur selben Zeit im Browser bei facebook.com angemeldet oder nicht):
 - IP-Nummer,
 - Datum und Uhrzeit des Aufrufs,
 - URL der angesehenen Seite und
 - Browsertyp.

²⁷ Heise Online (2011): Like-Button: Facebook erklärt Details zur Speicherpraxis. URL: <http://heise.de/-1339079>. Letzter Zugriff: 2011-10-21.

Über diese Daten hinaus vermutet der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, dass auch ein Browserfingerabdruck genommen wird, sofern Java Script aktiviert ist.²⁸ Das bedeutet, dass auch Daten über den Rechner selbst durch den Browser übermittelt werden. Das können z. B. die Bildschirmauflösung, installierte Browser Plugins und Schriftarten oder das Betriebssystem des Rechners sein. Da Computer individuell konfiguriert werden, ist ein solcher Browserfingerabdruck (nahezu) einzigartig. Seine Individualität hängt insbesondere von der Menge der für den Fingerabdruck herangezogenen Daten ab.²⁹

Ohne auch nur einmal auf den Like-Button geklickt zu haben, informiert Max auf diese Weise Facebook während des Surfens über alle von ihm besuchten Seiten, die den Like-Button oder andere Dienste von Facebook eingebunden haben. Max bemerkt davon nichts. Klickt Max auf den Button und ist dabei gleichzeitig bei Facebook angemeldet, so erhalten seine Freunde in ihrem Facebook News-Feed eine Mitteilung, welche Webseite er mag inklusive eines Links zu dieser Seite.

Auch ohne Klick darauf informiert der Like-Button Facebook über die vom Websurfer besuchten Seiten

Nach unserer ersten datenschutzrechtlichen Analyse des Like-Buttons im Datenschutzbarometer 2010³⁰ hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) eine datenschutzrechtliche Bewertung von Facebook-Diensten veröffentlicht.

Das ULD kommt zu dem Schluss, dass bei allen untersuchten Diensten inkl. des Like-Buttons zahlreiche gesetzliche Vorgaben – sowohl datenschutzrechtliche wie auch Vorschriften zu AGB – nicht eingehalten werden. Die Analyse des ULD berücksichtigt auch die Datenerhebung von Facebook Mitgliedern und die Anbindung des Like-Buttons an die Reichweitenmessung „Insights“.³¹

ULD: Die Verwendung des Facebook Like-Buttons verstößt u. a. gegen datenschutzrechtliche Vorschriften

Mit „Insights“ bietet Facebook Betreibern, die den Like-Button auf ihren Webseiten einbinden, eine Reichweitenmessung (siehe Kap. 2.2) an. Nach Aussagen des ULD wird dabei das Verbot, die Reichweitenmessung mit personalisierten Besucherdaten zu verknüpfen, (§ 15 Abs. 3 TMG) missachtet, denn einige personenbezogene Angaben aus den Facebook Profilen fließen demnach in die Reichweitenmessung ein.

Solange Datenschutzaufsichtsbehörden eine Nutzung des Like-Buttons als Datenschutzverstoß werten, besteht für Webseitenbetreiber akuter Handlungsbedarf. Sie müssen den Like-Button entfernen,

²⁸ Schneider, R. (2010): Facebook "Like"-Button. In: Virtuelles Datenschutzbüro. URL: <http://www.datenschutz.de/feature/detail/?featid=100>. Letzter Zugriff: 2011-07-15.

²⁹ Eckersley, Peter (2010): Peter How Unique Is Your Web Browser? In: Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science. URL: <https://panopticklick.eff.org/browser-uniqueness.pdf>. Letzter Zugriff: 2011-08-15.

³⁰ Kostenloser Download: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>

³¹ ULD (2011): Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook. Version 1.0. URL: <https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf>. Letzter Zugriff: 2011-08-23.

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.³² Das ULD sieht diese Lösung u. a. wegen mangelnder Transparenz darüber, was Facebook mit den Daten macht und wegen formaler Überlegungen als unzureichend an.³³

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 schützen möchten, empfehlen wir den Einsatz eines Internetbrowsers, der Skripte nur nach Aufforderung ausführt (siehe Tipps im Anhang 9.2).

³² Heise Online (2011): 2 Klicks für mehr Datenschutz. URL: <http://heise.de/-1333879>. Letzter Zugriff: 2011-10-21.

³³ Heise Online (2011): Facebook vs. Datenschützer: Streit um Like-Button geht weiter. URL: <http://heise.de/-1338660>. Letzter Zugriff: 2011-10-21.

3 Gegenstand und Methode des Datenschutzbarometers 2011

Eine maschinelle Quellcode-Analyse im Zeitraum von September bis Oktober 2011 von 37.732 deutschen Webpräsenzen bildet die Grundlage des XAMIT Datenschutzbarometers. Neben 1.804 Gemeinden und politischen Organisationen sowie 3.961 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 335 bis 4.272 Webpräsenzen vertreten. Analysiert werden jeweils maximal 1.000 Webseiten pro Webpräsenz.

Insgesamt werteten wir über 3,2 Mio. Webseiten aus. Hierbei wurde untersucht,

- ob und welche Shop-Software verwendet wird (Kapitel 3.1),
- ob Google AdSense verwendet wird (Kapitel 3.2),
- ob und welche Webstatistiken genutzt werden (Kapitel 3.3),
- ob Kontaktformulare vorhanden sind (Kapitel 3.4) und
- ob der Facebook Like-Button genutzt wird (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.

Maschinelle Quellcode-analyse erkennt Verwendung von PHP und verschiedener Webshop-Software

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 sind, 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“ PHP³⁴ nicht aufspüren. Ungeachtet dessen sollte die verwandte Methodik einen ersten Überblick über die Sicherheit von Webshops verschaffen.

3.2 Einbindung von Google Adsense

Unverkennbar: „Adsense“ von Google

Für die Einbindung von Google Adsense nutzen Websites eine charakteristische Zeichenfolge in Form des entsprechenden Java Scripts von Google. Diese Zeichenfolge ist auf allen Webseiten, die Google Adsense aufweisen, identisch. Sobald wir die Zeichenfolge im Quelltext finden, gehen wir von einer Adsense-Nutzung 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

³⁴ Siehe auch <http://www.hardened-php.net/suhosin/index.html>

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.

Umsetzung der Widerspruchsmöglichkeit

Google verlangt in § 8.1 seiner Nutzungsbedingungen³⁵, 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 vertraglich vorgeschriebenen Formulierungen auf einer Webpräsenz, die Google Analytics nutzt, vorkommen, wurde analog untersucht.

Überprüfung der Einhaltung der Nutzungsbedingungen von Google Analytics

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.

Umfang und Qualität der abgefragten Daten

3.5 Einbindung des Facebook Like-Buttons

Für jede Webseite wurde untersucht, ob der Like-Button von Facebook eingebunden ist. Wir prüften dabei, ob der von Facebook zur Verfügung gestellte charakteristische iframe oder der Skript-Code auf der Seite auffindbar ist. Wurde er gefunden, nehmen wir an, dass der Button auf der Seite verwendet wird. Bei manuellen Stichproben wurden keine Fehlzuordnungen festgestellt.

³⁵ Google Analytics Bedingungen. URL: <http://www.google.com/analytics/de-DE/tos.html>. Letzter Zugriff: 2011-12-05.

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 des Facebook Like-Buttons (Kapitel 4.5)

vor. Die Ergebnisse aggregieren wir in Kapitel 5 zum kompakten XAMIT Datenschutzbarometer 2011.

4.1 Risiko durch veraltete Software

Insgesamt haben wir 4.744 Installationen von PHP der Version 4 und 13.820 Installationen der Version 5 identifiziert (Mehrfachnennung möglich). Davon nutzen 1.469 die Versionen 5.3. Die veralteten Versionen 4, 5.0, 5.1 und 5.2 verfügen damit über einen Anteil von 92% an allen PHP-Installationen. 2010 waren es 98% (Abbildung 1). Nur langsam steigen die Betreiber auf die aktuellen Versionen 5.3 um. Dies ist insofern bedenklich, da z. B. die Betreuung und Fehlerbehebung von Version 4 mit der Version 4.4.9 Ende 2008 eingestellt wurde.³⁶ Von allen erkannten PHP-Installationen haben wir bei nur 1,3% die zum Zeitpunkt der Erhebung aktuelle Version 5.3.8 entdeckt. 2010 nutzen noch weniger die damals aktuelle Version 5.3.2 (0,7%).

92% der Webshops
basieren auf veralteter
PHP-Installation

³⁶ Siehe Ankündigung zu Version 4.4.9. URL: http://php.net/releases/4_4_9.php. Letzter Zugriff: 2010-11-12.

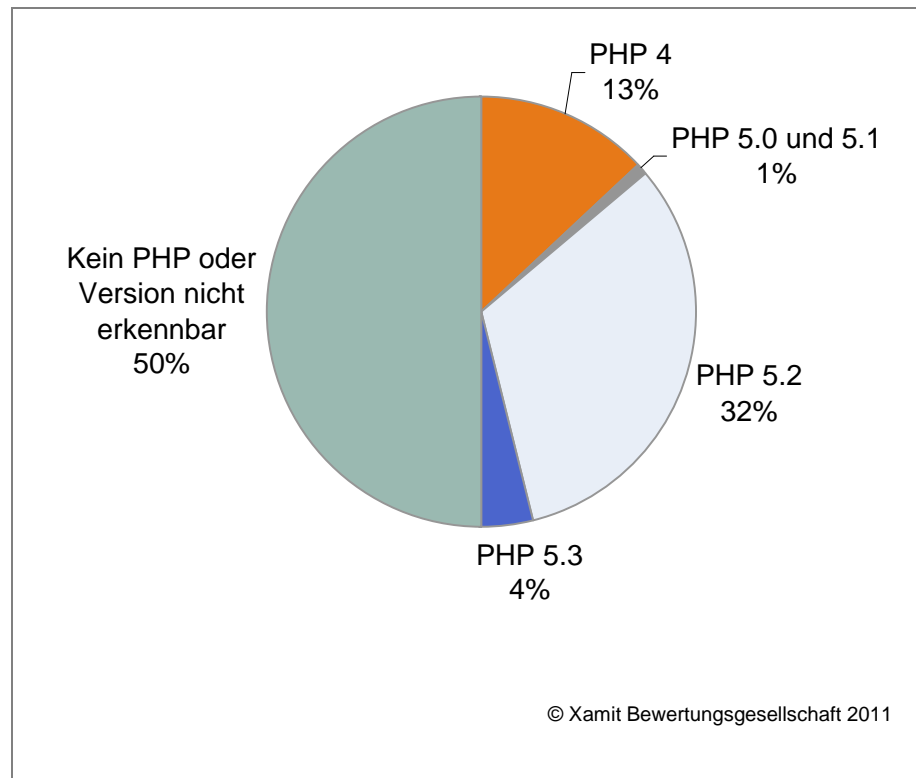


Abbildung 1: Nutzung von PHP nach Versionen

Nach einer Studie des Web Application Security Consortium (WASC) von 2008 sind 7% der Webpräsenzen und Webshops anfällig für das Einschleusen von SQL-Codes. Ein solches Code-Einschleusen erlaubt i. d. R. den Diebstahl von Kundendaten aus einem Webshop. PHP ist dabei ein mögliches Einfallstor. Das WASC ermittelte mit Hilfe automatischer Scanner und manueller Tests die Schwachstellen von mehr als 12.186 Webpräsenzen und Webshops.³⁷

In 1.369 Fällen konnten wir eine bekannte Shopssoftware erkennen. xtCommerce ist mit einem Anteil von 69% unbestrittener Marktführer gefolgt von Oxid Shop (20%) und dem OpenSource-Vertreter osCommerce mit 7%. Die restlichen 4% verteilen auf sich drei Programme. Aufgrund der geringen Fallzahlen verzichteten wir auf eine Aufteilung nach Branchen.

Angesichts der geringen Anzahl an erkannter Shopssoftware 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 Unter-

³⁷ WASC (2008): Web Application Security Statistics 2008, S.7. URL: <http://projects.webappsec.org/f/WASS-SS-2008.pdf>. Letzter Zugriff: 2010-10-12.

fangen, 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.

23% der Webshops mit Standardshopsoftware und erkannter PHP-Installation setzen die aktuelle PHP-Version ein. Dieser geringe Anteil deutet darauf hin, dass viele Webshops ihre PHP-Installation nicht regelmäßig aktualisieren. Sie bleiben für Sicherheitslücken in PHP anfällig und gefährden so Kundendaten.

77% der Webshops auf PHP-Basis gefährden Kundendaten

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 Google Adsense – Daten werden heimlich übertragen

Wer Google Adsense auf seiner Webpräsenz einbindet, der macht Werbung für fremde Unternehmen und Produkte. Viele der untersuchten Webpräsenzen zählen allerdings nicht zu den typischen Adsense-Nutzern, so dass deren relativ geringer Anteil von 1,5% unter den untersuchten Webpräsenzen nicht überrascht.

Informierten 2008 erst 21% der Webpräsenzen mit Adsense ihre Besucher mit einer Datenschutzerklärung, waren es 2009 bereits 32% und 2010 39%. Heute haben 42% der Adsense-Nutzer auf ihrer Webseite eine Datenschutzerklärung. Auf der anderen Seite setzen sich aber immer noch 58% (2010: 61%) über die Nutzungsbedingungen von Google hinweg und lassen ihre Besucher im Dunkeln darüber, dass Google ein Cookie setzt und dass Daten, wie die IP-Nummer, zu Google übertragen werden.

Noch immer nutzen 58% der Webpräsenzen Google Adsense heimlich

Es bestehen deutliche Unterschiede zwischen den Branchen. Unternehmen aus dem Bereich „Medien“ informieren zu 86%, während keine einzige Webseite des verarbeitenden Gewerbes eine Datenschutzerklärung veröffentlicht und so die Nutzungsbedingungen von Google Adsense nicht einhält. 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 – Licht und Schatten

Vor gut vier Jahren haben wir zum ersten Mal die Nutzung von Google Analytics durch deutsche Webseitenbetreiber untersucht. Ein breites Medienecho und eine Diskussion in der Fachwelt über die

rechtliche Zulässigkeit waren die Folge.³⁸ Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stufte die Verwendung von Google Analytics durch Webseitenbetreiber im Januar 2009 als datenschutzwidrig ein.³⁹ Nach einer mehrjährigen Diskussion hat der für Google in Deutschland zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Casper, Google überzeugt, eine nach deutschem Recht legal einsetzbare Version von Google Analytics bereit zu stellen.⁴⁰ Um Google Analytics datenschutzkonform einzusetzen, muss ein Webseitenbetreiber u. a. folgendes tun:⁴¹

Aufgaben des Webseitenbetreibers für den gesetzeskonformen Einsatz von Google Analytics

- Einen Vertrag zur Auftragsdatenverarbeitung mit Google schriftlich abschließen.
- Nutzer in einer Datenschutzerklärung über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics aufklären und auf die Widerspruchsmöglichkeiten hinweisen.
- Die Funktion „_anonymizeIp()“ im Code des Google-Trackingskriptes einbauen, um die IP-Nummern der Besucher zu anonymisieren.
- Die Altdaten löschen, wenn Google Analytics bereits vor dieser Umstellung genutzt wurde.

Wenn die Funktion „_anonymizeIp()“ im Code von Google Analytics gefunden wurde, rechnen wir den Fund der legalen Nutzung zu. Fehlt die Funktion, liegt eine datenschutzwidrige Nutzung vor. Diese stellte eine Ordnungswidrigkeit dar, die mit einem Bußgeld von bis zu 50.000 Euro geahndet werden kann.

Der Einsatz von Google Analytics steigt sowohl in der anonymisierenden als auch in der nicht datenschutzkonformen Version

Zum Zeitpunkt unserer ersten Erhebung im Jahr 2007 nutzten 7% der Webpräsenzen Google Analytics und 1% einen anderen Anbieter. 2009 waren es bereits 13% für Google Analytics und weitere 4% nutzten andere Dienste. 2010 stieg der Anteil für Google Analytics auf 19%. In 2011 sammelt Google Analytics ohne Anonymisierung auf 22% der Webpräsenzen Daten. Das ist eine Steigerung um 16% gegenüber 2010. Auf 0,5% der Webseiten wird die anonymisierte Version von Google Analytics eingesetzt. 8,0% (2010: 4,9%) verwenden heute andere Anbieter. Insgesamt erfreut sich Google Analytics steigender Beliebtheit über alle Branchen hinweg.

74,4% der gefundenen Webstatistik-Dienste sind nicht datenschutzkonform

Wir fanden auf insgesamt 29,9% der untersuchten Webpräsenzen einen Webstatistik-Dienst (2010: 24,7%). Davon verwenden 74,4%

³⁸ 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.

³⁹ Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (2009): Datenschutzrechtliche Bewertung des Einsatzes von Google Analytics. URL: https://www.datenschutzzentrum.de/tracking/20090123_GA_stellungnahme.pdf. Letzter Zugriff: 2009-08-05.

⁴⁰ 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: 2011-10-21.

⁴¹ Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (2011): Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen. URL: http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_Webseitenbetreiber_in_Hamburg.pdf. Letzter Zugriff: 2011-09-29.

(2010: 80%) Dienste, die die Kriterien des Düsseldorfer Kreises verfehlen. Der Hauptanteil geht auf das Konto von Google Analytics ohne Anonymisierung. 10,2% (2010: 9%) der Dienste erfüllen die Vorgaben des Düsseldorfer Kreises. Die restlichen 15,4% (2010: 11%) verteilen sich auf Webstatistik-Dienste, deren Gesetzeskonformität wir aufgrund ihrer geringen Marktabdeckung oder weil sie in Eigenregie eingesetzt werden, nicht geprüft haben.⁴² Abbildung 2 zeigt die Nutzung nach Branchen.

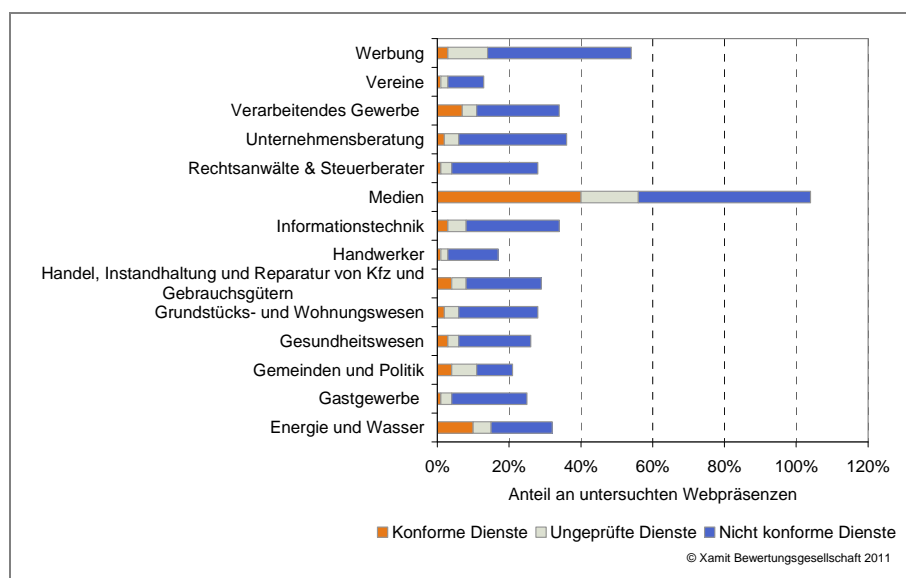


Abbildung 2: Nutzung von Webstatistiken nach Branchen

Die am stärksten nutzenden Branchen haben sich von 2010 zu 2011 nicht verändert. Die meisten nicht konformen Dienste setzen die Branchen Medien (48%), Werbung (40%) und Unternehmensberatungen (30%) ein. Die meisten konformen Dienste nutzen ebenfalls die Medien (40%) gefolgt von Energie und Wasser (10%) sowie dem verarbeitenden Gewerbe (7%).

Der Düsseldorfer Kreis verlangt, dass dem Nutzer „eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen“⁴³ ist. Wie bereits 2010 messen wir auch dieses Jahr, ob diejenigen Webseitenbetreiber, die eine nach den Kriterien des Düsseldorfer Kreises datenschutzkonforme Webstatistik einsetzen, auch die vorhandene Widerspruchsmöglichkeit nutzen. Da Google Analytics keinen Widerspruchs-Cookie setzt, bleibt dieser Dienst außen vor. Wir fanden nur auf 2% (2010: 2%) der von uns untersuchten Webseiten datenschutzkonforme Webstatistik-Tools, die eine von uns erfassbare Widerspruchsmöglichkeit anbieten. Von diesen Webpräsenzen wiederum geben nur 22,9% (2010: 22,4%) ihren Besuchern die Möglichkeit, der Datensammlung zu widersprechen. Das heißt, dass

Widerspruchsmöglichkeit gegen Nutzerprofile wird fast nicht umgesetzt.

⁴² Vgl. XAMIT (2011): Webstatistiken im Test – Welcher Dienst ist in Deutschland legal? 8. Update vom 4.10.2011, S. 10f. URL: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>.

⁴³ Düsseldorfer Kreis (2009): Beschluss zur Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten. URL: <http://www.datenschutz-mv.de/dschutz/beschlue/Analyse.pdf>. Letzter Zugriff: 2010-10-27.

zwar eine Webstatistik auf datenschutzkonformem Wege erstellt werden könnte, es aber in rund vier von fünf Fällen nicht getan wird. Die Verantwortung liegt hier eindeutig bei den Betreibern der Webpräsenzen. Abbildung 3 zeigt, wie die Widerspruchsmöglichkeit von den einzelnen Branchen umgesetzt wird.

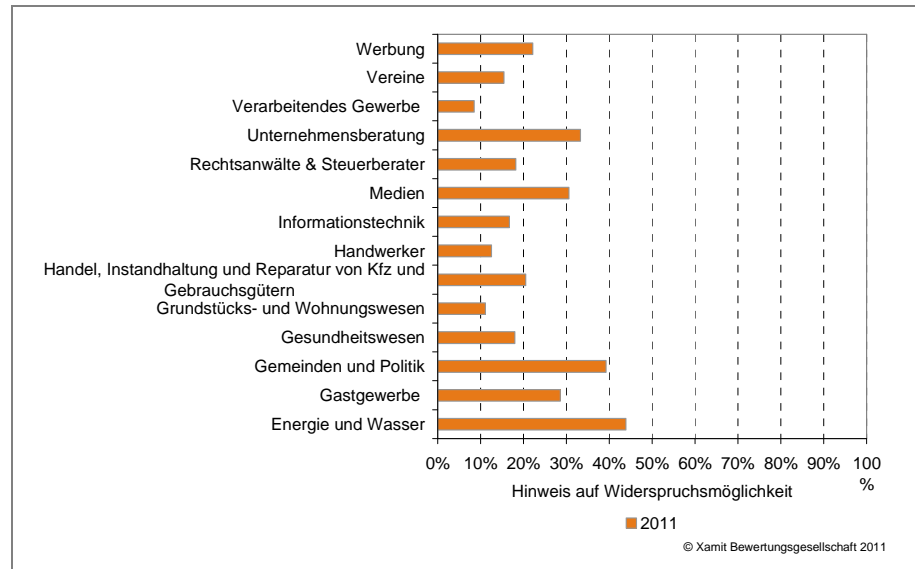


Abbildung 3: Hinweis auf die Widerspruchsmöglichkeit nach Branchen

49% der Webseiten mit Webstatistik nutzen diese heimlich

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“⁴⁴ 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 2010 69% der von uns untersuchten Betreiber diese Kennzeichnungspflicht – sei es durch eine eigene Datenschutzerklärung oder den Google Passus. Heute sind es immer noch 49%. 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 4.

⁴⁴ Google Analytics Bedingungen. URL: <https://www.google.com/intl/de/analytics/tos.html>.
 Letzter Zugriff: 2011-12-04.

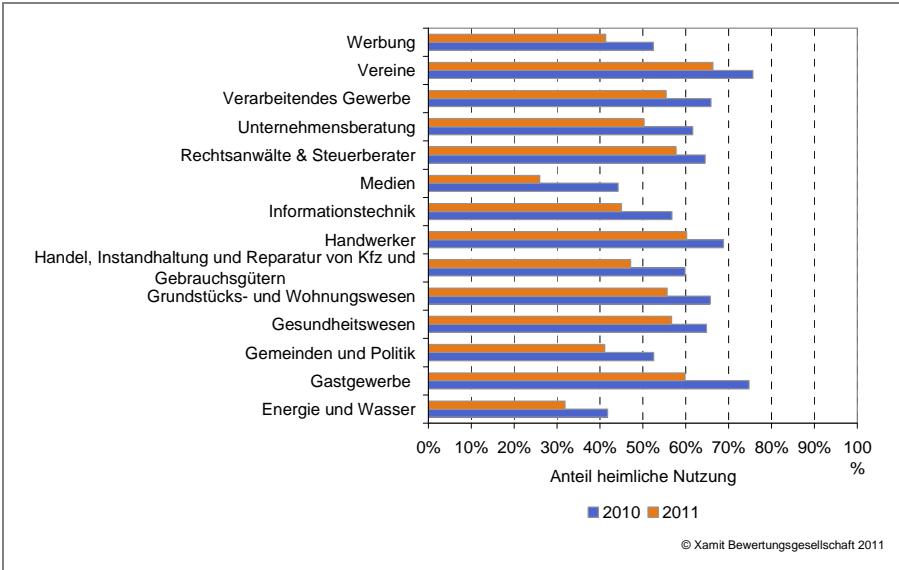


Abbildung 4: Heimliche Nutzung von Webstatistiken nach Branchen

Immer noch setzen Vereine und das Gastgewerbe mit 66% bzw. 60% auf eine meist heimliche Datensammlung. Der Rückgang ist sicherlich eine sehr positive Folge der öffentlichen Datenschutzdebatte. Allerdings dauert diese bereits vier Jahre an. Nach einem so langen Zeitraum stellt sich die Frage, wie lange fortgesetzte Datenschutzverstöße noch geduldet werden sollen? Exemplarisch am Marktführer Google Analytics (ohne Anonymisierung) zeigt Abbildung 5 die seit 2007 jährlich zunehmende Nutzung. Mit jeder Nutzung gehen Datenschutzverstöße durch die Betreiber einher – ohne Konsequenzen.

Vereine und Gastgewerbe sind die größten heimlichen Datensammler

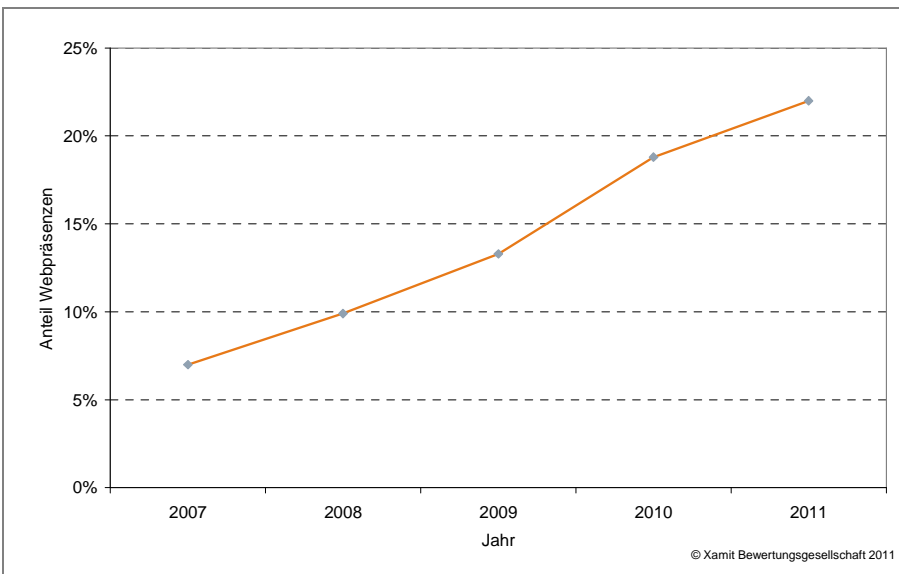


Abbildung 5: Verwendung von Google Analytics ohne Anonymisierung

4.4 Kontaktformulare – Datenverarbeitung oft ohne Erklärung

Im Jahr 2010 setzten 42% der damals untersuchten Webseiten Kontaktformulare ein. Heute sind es 52%. Abbildung 6 zeigt die Nutzung nach Branchen. Spitzenreiter sind die Medien mit 75% der Webseiten.

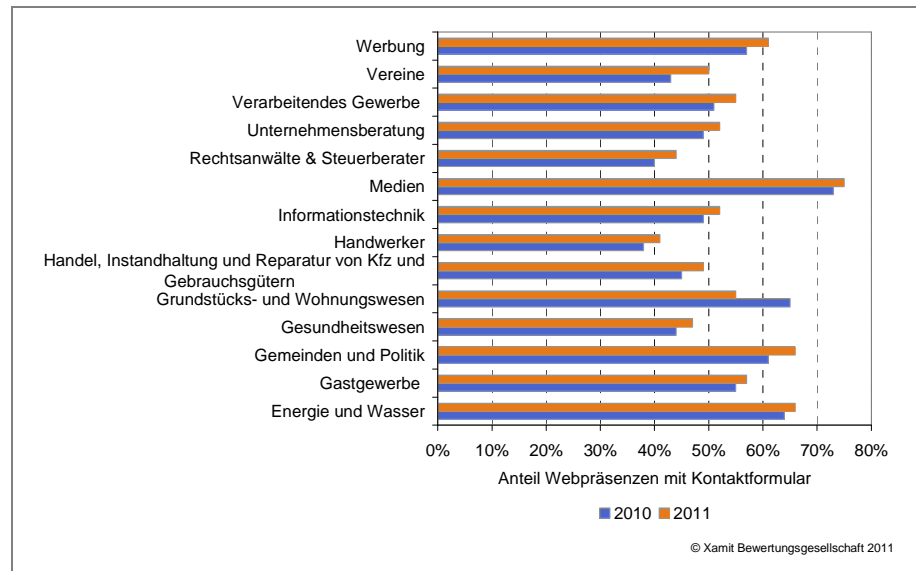


Abbildung 6: Einsatz von Kontaktformularen nach Branchen

Information über die Verarbeitung der persönlichen Daten nimmt insgesamt zu

Uns interessierte, wie die Betreiber mit den anfallenden personenbezogenen Daten umgehen. Von den Webpräsenzen mit Kontaktformular informieren 35% (2010: 29%) über ihren Umgang mit den erhobenen Daten. 65% (2010: 71%) nutzen ein Kontaktformular ohne Datenschutzerklärung. In Summe werben jedoch immer mehr Betreiber um Vertrauen in ihren Umgang mit den eingegebenen persönlichen Daten. Abbildung 7 zeigt die Verteilung nach Branchen.

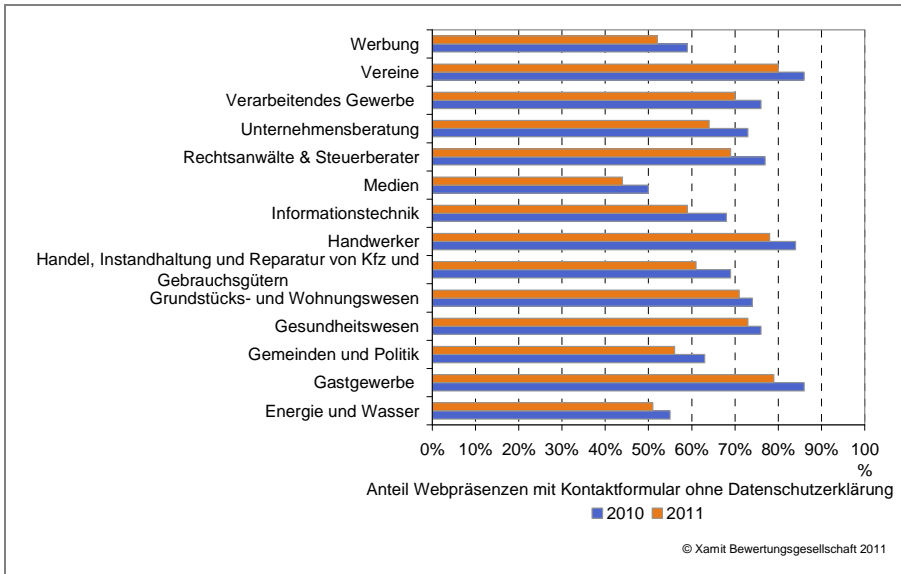


Abbildung 7: Anteil von Kontaktformularen ohne Datenschutzerklärung nach Branchen

4.5 Facebook Like-Button: Gefällt uns gar nicht

Die Nutzung des Facebook-Like-Buttons ist rasant gestiegen. 2010 verwendeten 0,6% der Webpräsenzen den Like-Button. 2011 sind es bereits 6,6% – rund eine Verzehnfachung innerhalb eines Jahres.

Einbindung des Facebook Like-Buttons auf Webseiten steigt rasant

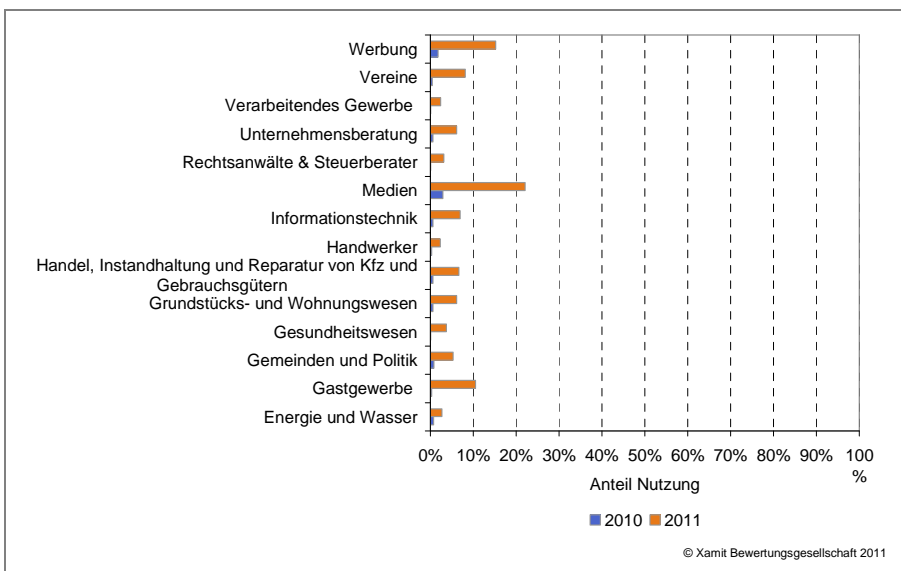


Abbildung 8: Nutzung Facebook-Like-Button nach Branchen

Abbildung 8 zeigt die Nutzung des Like-Buttons in den einzelnen Branchen. Überdurchschnittlich viele Like-Buttons waren auf Seiten von Medien (22,1%) zu finden, gefolgt von Werbung (15,2%) sowie dem Gastgewerbe (10,5%). Insbesondere Medienseiten sind ihrer Funktion gemäß besonders publikumsstarke Seiten und haben be-

Medien, Werbung und Gastgewerbe nutzen den Like-Button am häufigsten.

sonders umfangreiche Webauftritte. Daher betrifft ein Datenschutzverstoß auf diesen Seiten naturgemäß sehr viele Surfer.

5 Das XAMIT Datenschutzbarometer 2011

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

Messung des
Datenschutznieaus

- 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,
- AdSense ohne Datenschutzerklärung einbinden,
- unsichere PHP-Versionen bei Online-Shops einsetzen,
- 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.

Anzahl der
Beanstandungen in Relation
zur Anzahl der untersuchten
Webseiten.

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.

82 Beanstandungen pro 100 Webpräsenzen

Insgesamt haben wir 82 Verstöße oder Gründe zur Beanstandung auf jeweils 100 untersuchten Webpräsenzen gefunden. 2010 waren es 73. Das ist eine Steigerung um 12%. Abbildung 9 vergleicht die Verstöße 2010 mit 2011. Die Steigerung um 12% verdeckt, dass die Nutzung des Facebook Like-Buttons explosionsartig um 957% zugenommen hat.

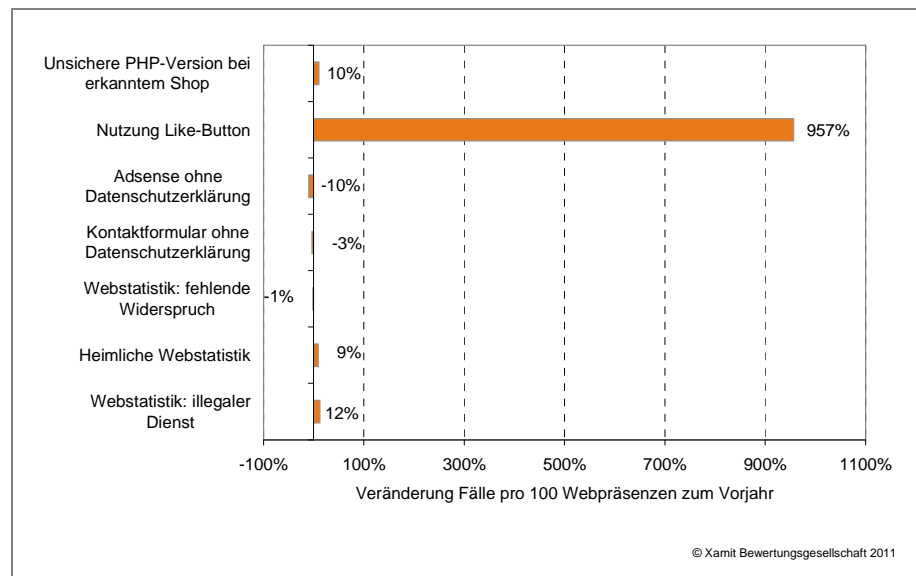


Abbildung 9: Entwicklung der Verstöße und Beanstandungen im Vergleich zum Vorjahr

Bei Fachleuten haben die Verstöße nochmals zugenommen

Spitzenreiter sind seit 2008 die Datenschutzmultiplikatoren. In diesem Jahr mit 104 Verstößen (2010: 96 Verstöße) pro 100 Webpräsenzen (Abbildung 10), 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.

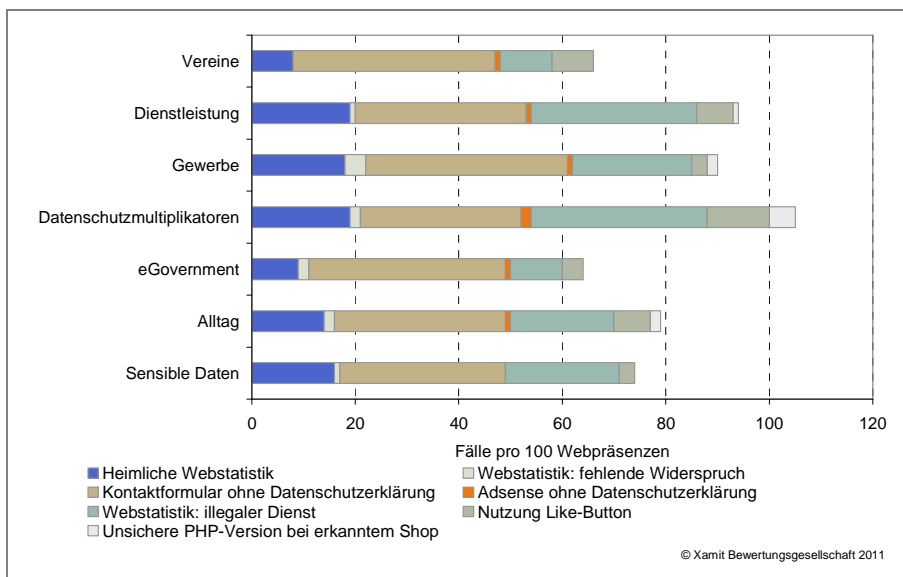


Abbildung 10: Verstöße und Beanstandungen nach Klassen

Eine regionale Verteilung nach Bundesländern zeigt Abbildung 11. Hamburg bleibt mit 99 Verstößen per 100 Webseiten wie im Vorjahr Spitzenreiter. Berlin folgt dicht auf mit 97 Verstößen. Sachsen belegt wie im Vorjahr den 3. Platz mit 89 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.

In Hamburg, Berlin und Sachsen wurden die meisten Beanstandungen festgestellt

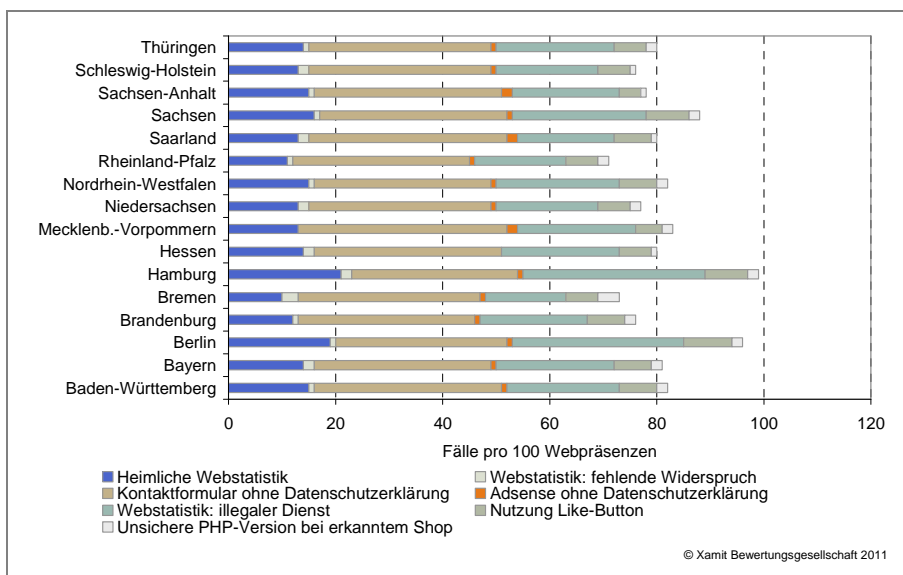


Abbildung 11: Verstöße und Beanstandungen nach Bundesländern

Wie wir in Abbildung 12 sehen können, liegen die meisten Verstöße zwischen 70 und 80 pro 100 Webpräsenzen in insgesamt neun Bundesländern. „Bestes“ Ergebnis aller Länder erzielt Rheinland-Pfalz mit insgesamt 71 Verstößen bzw. Gründen zur Beanstandung.

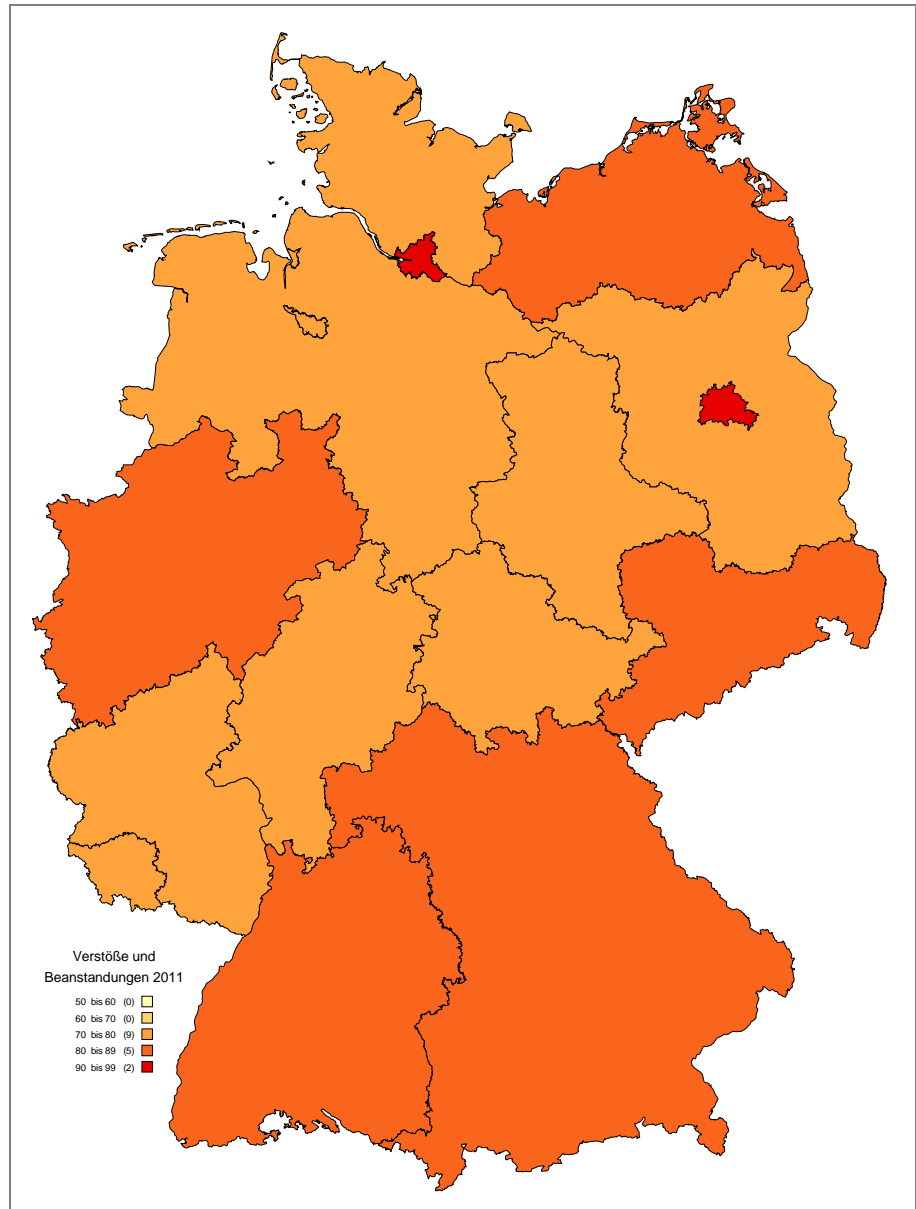


Abbildung 12: Verstöße und Beanstandungen nach Bundesländern. Die Zahlen in Klammern zeigen die Anzahl an Bundesländern, die den entsprechenden Werten zugeordnet sind.

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.

Für die meisten Aufsichtsbehörden war 2011 eine Zäsur. Ihre jeweiligen Landesparlamente haben sie in die „vollständige“ Unabhängigkeit entlassen, um dem Urteil des Europäischen Gerichtshofs vom 9. März 2010 Rechnung zu tragen (Kapitel 6.1). In der Folge änderte sich für einige Behörden die Personalausstattung, für manche auch die Zuständigkeit (Kapitel 6.2).

Alle Aufsichtsbehörden publizieren periodisch Tätigkeitsberichte, in denen sie wichtige Aspekte ihrer Arbeit darstellen.⁴⁵ Der Schwerpunkt der Berichte liegt auf der inhaltlichen Darstellung der behördlichen Tätigkeit und einer Diskussion von Entwicklungen im Datenschutz. Statistische Aussagen zur Tätigkeit fehlen meistens. Deshalb haben wir die Aufsichtsbehörden dieses Jahr zusätzlich zur Stellenausstattung nach statistischen Angaben zu ihrer Tätigkeit befragt (Kapitel 6.3).

6.1 Unabhängig sollt ihr sein

Am 9. März 2010 hat der Europäische Gerichtshof geurteilt, dass die Überwachung der Verarbeitung personenbezogener Daten in Deutschland bei privaten Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen zu sehr der staatlichen Kontrolle unterworfen sei (Aktenzeichen: C-518/07). Die Datenschutzaufsicht müsse „völlig unabhängig“ von staatlicher Kontrolle werden.⁴⁶

Wir befragten die Aufsichtsbehörden, seit wann sie im Sinne des Urteils unabhängig sind. Fehlende Antworten haben wir – soweit es möglich war – durch eigene Recherchen ergänzt (mit * gekennzeichnet). Inwieweit die jeweiligen gesetzlichen Regelungen dem Urteil des Europäischen Gerichtshofs entsprechen, ist teilweise strittig: Die zuständige EU-Kommissarin Vivianne Reding sieht die Unabhängigkeit des Brandenburgischen Landesdatenschutzbeauftragten als nicht vollständig an.⁴⁷ Wir nehmen in der folgenden Darstellung keine in-

⁴⁵ Eine Sammlung aller Berichte pflegt ZAFTDa der Technischen Hochschule Mittelhessen: <http://www.thm.de/zaftda/index.php>

⁴⁶ Heise online (2010): EuGH: "Völlige Unabhängigkeit" der Datenschutzaufsicht zu gewährleisten [Update]. URL: <http://www.heise.de/newsticker/meldung/EuGH-Voellige-Unabhaengigkeit-der-Datenschutz-aufsicht-zu-gewaehrleisten-Update-949673.html>. Letzter Zugriff: 2010-11-04.

⁴⁷ http://www.daten-speicherung.de/data/Kommission_Unabhaengigkeit_07-04-2011.pdf. Letzter Zugriff: 2011-11-18.

haltliche Bewertung vor. Tabelle 1 beinhaltet die Daten für den Beginn der Unabhängigkeit (Stand: 2. 12. 2011).

Bundesland	Unabhängig seit
Baden-Württemberg	1. April 2011
Bayern	1. August 2011
Berlin	16. Februar 2011
Brandenburg	k. A.
Bremen	17. November 2010*
Hamburg	14. Juni 2011
Hessen	1. Juli 2011
Mecklenburg-Vorpommern	1. Juni 2011*
Niedersachsen	Sommer 2011*
Nordrhein-Westfalen	16. Juli 2011
Rheinland-Pfalz	9. März 2011
Saarland	1. Juni 2011*
Sachsen	k. A.
Sachsen-Anhalt	1. Oktober 2011
Schleswig-Holstein	30. September 2011
Thüringen	Gesetzgebungsverfahren läuft
Bund	Keine konkrete Planung

Tabelle 1: Unabhängigkeit der Datenschutzaufsicht.

*: Angaben beruhen auf eigenen Recherchen.

13 Aufsichtsbehörden wurden 2010 und 2011 unabhängig

Abbildung 13 zeigt, dass 13 Bundesländer das Urteil in 2010 und 2011 umgesetzt haben. In einem Bundesland lief das entsprechende Gesetzgebungsverfahren zum Zeitpunkt der Befragung noch. Zu zwei Bundesländern liegen uns keine Informationen vor. Eine Umsetzung im Bund scheint nicht geplant zu sein.

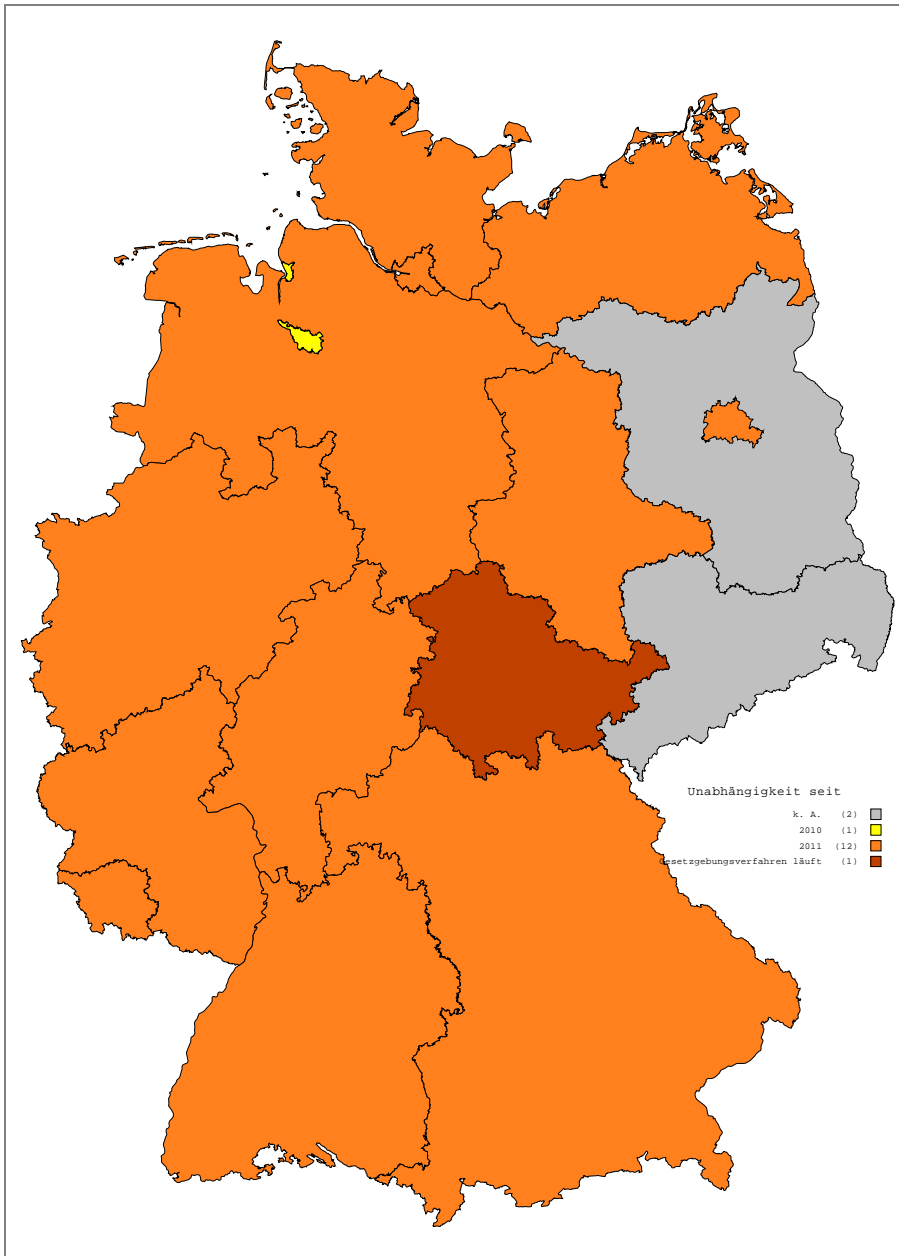


Abbildung 13: Unabhängigkeit der Datenschutzaufsicht.

Über den öffentlichen Bereich führt traditionell der jeweilige Landesbeauftragte für den Datenschutz die Aufsicht. Inzwischen ist in 14 Bundesländern der jeweilige Landesdatenschutzbeauftragte ebenfalls für den nicht-öffentlichen Bereich zuständig. Ein Vorteil für Bürger, die nun einen einzigen Ansprechpartner für ihre Belange erhalten, egal, ob es sich um Fragen zu öffentlichen oder nicht-öffentlichen Stellen handelt. Je mehr öffentliche Stellen auf eGovernment setzen, desto stärker gleichen sich die Datenschutzprobleme von öffentlichem und nicht-öffentlichem Bereich.

In zwei Bundesländern sind anstelle des Landesbeauftragten andere Behörden für den nicht-öffentlichen Bereich zuständig:

- Bayern: Bayerisches Landesamt für Datenschutzaufsicht
- Thüringen: Thüringer Landesverwaltungsamt

Im Zuge der Umsetzung des EuGH-Urteils soll die Zuständigkeit des Thüringer Landesverwaltungsamts auf den Landesdatenschutzbeauftragten von Thüringen übergehen. Das Gesetzgebungsverfahren war zum Zeitpunkt der Befragung noch nicht abgeschlossen.

6.2 Personelle Ausstattung im Jahr 2011

Wie schon 2009 und 2010 haben wir alle den Ländern unterstehenden Aufsichtsbehörden und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit angeschrieben und ihre Stellenanzahl erfragt.⁴⁸ 89% der Behörden haben geantwortet. Für folgende Bundesländer liegen vollständige Angaben vor:

- Baden-Württemberg
- Bayern
- Berlin
- Hamburg
- Hessen
- Mecklenburg-Vorpommern
- Nordrhein-Westfalen
- Rheinland-Pfalz
- Sachsen
- Sachsen-Anhalt
- Schleswig-Holstein
- Thüringen
- Bund

Alle Zahlen geben Vollzeitstellen wieder. Wenn Antworten zwischen besetzten Stellen und Planstellen differenzieren, nehmen wir die Planstellen, da sie die maximal mögliche Ausstattung widerspiegeln.

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 Baden-Württemberg, Mecklenburg-Vorpommern und Nordrhein-Westfalen gegenüber dem letzten Jahr zu. Schleswig-Holstein wuchs bei befristeten Stellen. Rheinland-Pfalz

⁴⁸ 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.

konnte gegenüber 2009 einen Stellenzuwachs verzeichnen (für 2010 liegen uns keine Angaben vor). Hessen reduzierte sein Personal. Eine Stelle hat uns dieses Jahr zum ersten Mal geantwortet. Daher können wir bei dieser keine Aussage zur Veränderung gegenüber dem Vorjahr treffen. Neben einer Veränderung der Stellenanzahl ist eine Verschiebung vom öffentlichen und zum nicht-öffentlichen Bereich zu beobachten. Die Aufsichtsbehörden tragen damit der gestiegenen Bedeutung des nicht-öffentlichen Bereichs Rechnung.

Das Datenschutzrecht kennt für öffentliche und nicht-öffentliche Stellen unterschiedliche Regeln (vgl. Kap. 6.3.3). Um die Stellenanzahl in Relation zu einigen Kennzahlen zu setzen unterteilen wir die Stellen in öffentliche und nicht-öffentliche Stellen. Einige Aufsichtsbehörden arbeiten ausschließlich in einem der beiden Bereiche, so dass wir deren Stellen dem jeweiligen Bereich einfach zuordnen können. Tabelle 2 zeigt die Verteilung der Stellen nach Bundesländern.

Das Datenschutzrecht unterscheidet in öffentliche und nicht-öffentliche Organisationen

Anmerkungen zur Berechnung

Für einige Behörden wurden die Vorjahreswerte korrigiert, da bei früheren Meldungen zuviel Personal (Informationsfreiheit) oder zuwenig Personal (unterstützende Stellen) angegeben wurde. Einige Stellen, u. a. 30% der Stellen für den nicht-öffentlichen Bereich des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, sind befristet. Hier stellt sich die Frage, ob der Stellenzuwachs zwischen 2010 und 2011 von Dauer sein wird.

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz hat uns neben Vollzeitstellen auch drei Teilzeitstellen angegeben. Wir haben diese jeweils als 0,5 Vollzeitstellen interpretiert, so dass wir die gemeldeten Vollzeitstellen um 1,5 erhöht haben. Die über das Jahr verteilt beschäftigten sieben Referendare haben wir mit einer durchschnittlichen Beschäftigungsdauer von drei Monaten angenommen. Damit ergeben sich $3 \times 7 = 21$ Personenmonate, die 1,75 Vollzeitstellen entsprechen.

a: Bei Aufsichtsbehörden, die beide Bereiche abdecken, verteilen wir die Stellen – sofern wir keine anderen Angaben erhalten haben – $2/3$ zu $1/3$ zugunsten des öffentlichen Bereichs. Damit nehmen wir ein wesentlich günstigeres Verhältnis an, als bei den anderen bereichsspezifischen Aufsichtsbehörden zu beobachten ist. Diese Zahlen sind mit „a“ gekennzeichnet.

b, c: Bei den Stellen, die uns zwar im Jahr 2009 oder 2010 geantwortet haben, aber nicht in diesem Jahr, nehmen wir die Zahlen von 2009 bzw. 2010 als Berechnungsgrundlage. Nach unserer Erfahrung sind dadurch keine nennenswerten Fehlzusammenhänge zu erwarten. Diese Zahlen sind mit „b“ für 2010 und „c“ für 2009 gekennzeichnet.

d: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verfügt zusätzlich zu den bereichsspezifischen Stellen über 7,6 Stellen, die beide Bereiche unterstützen. Wir haben diese nach unserem Schlüssel $2/3$ zu $1/3$ zu Gunsten des öffentlichen Bereichs verteilt und den jeweiligen gemeldeten bereichsspezifischen Werten hinzuaddiert. Diese Werte sind mit „d“ gekennzeichnet.

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 für beide Bereiche zusammen ohne Abordnungen über 25,5 Planstellen, die wegen des Aufstockungsanspruchs von teilzeitarbeitenden Beamten nicht vollständig besetzt werden können.

Bundesland	Nicht-öffentlicher Bereich 2011 (2010)		Öffentlicher Bereich 2011 (2010)	
Baden-Württemberg	9,2 ^e	(8,1 ^e)	17,0 ^e	(17,0 ^e)
Bayern	12,0	(k. A.)	26,0	(26,0)
Berlin	11,2 ^a	(11,2 ^a)	22,8 ^a	(22,8 ^a)
Brandenburg	7,3 ^{a, b}	(-)	14,7 ^{a, b}	(-)
Bremen	k. A.	(k. A.)	k. A.	(k. A.)
Hamburg	6,9 ^d	(6,9 ^d)	8,9 ^d	(8,9 ^d)
Hessen	10,7	(12,47 ^c)	24,5	(24,5)
Mecklenburg-Vorpommern	6,0	(1,0)	10,0	(13,0)
Niedersachsen	11,5 ^b	(-)	6,0 ^b	(-)
Nordrhein-Westfalen	26,75	(14,4 ^a)	21,75	(29,3 ^a)
Rheinland-Pfalz	6,6 ^a	(4,6 ^{a, c})	13,7 ^a	(9,4 ^{a, c})
Saarland	k. A.	(k. A.)	10,0 ^c	(-)
Sachsen	7,3	(7,3 ^a)	14,7	(14,7 ^a)
Sachsen-Anhalt	1,0 ^c	(1,0)	15,0	(15,0)
Schleswig-Holstein	9,25	(5,5)	13,0	(13,5)
Thüringen	2,0	(2,0)	13,0	(13,0)
Gesamt gemeldet	120,0		231,5	

Tabelle 2: Personalausstattung Kernpersonal der Datenschutzaufsicht 2011 verteilt auf öffentliche und nicht-öffentliche Stellen

Die Dienststelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat 2011 81 Stellen Kernpersonal für den öffentlichen Bereich und 10 Stellen Kernpersonal für den nicht-öffentlichen Bereich zur Verfügung. Dafür stehen 2011 keine Praktikanten und Referendare mehr zur Verfügung. Das bedeutet eine Stellenverlagerung von 13 Praktikanten und Referendaren aus 2010 hin zu 10,5 zusätzlichen Stellen Kernpersonal für den öffentlichen Bereich und 2,5 zusätzlichen Stellen Kernpersonal für den nicht-öffentlichen Bereich.

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

- die Stellen für den öffentlichen Bereich zu der Anzahl an Beschäftigten im öffentlichen Sektor (Bund⁴⁹, Land und Gemeinden) ins Verhältnis,
- die Stellen für den nicht öffentlichen Bereich zu der Anzahl an Beschäftigten im Privatsektor ins Verhältnis.⁵⁰

⁴⁹ Die Bundesbehörden gehören nicht zum Aufgabenbereich der hier betrachteten Aufsichtsbehörden. Deshalb zeichnen unsere Berechnungen ein zu optimistisches Bild.

⁵⁰ Stand: 2007. Quelle:

http://statistik.arbeitsagentur.de/cae/servlet/contentblob/101072/publicationFile/42755/Monat_sbericht-201010.pdf;jsessionid=72480BB26CD1FCF2FED43B4B3677DCA7

Bezogen auf die Unternehmensanzahl von 3.591.265⁵¹ (ohne Vereine, Parteien und andere Organisationen) stehen bundesweit für die Datenschutz-Aufsicht nur 3,6 Stellen pro 100.000 Unternehmen zur Verfügung.

Die Datenschutzaufsicht hat 3,6 Stellen pro 100.000 Unternehmen zur Verfügung

Abbildung 14 zeigt deutlich, dass für den öffentlichen Bereich wesentlich mehr Stellen pro 100.000 Beschäftigter zur Verfügung stehen als für die Kontrolle von Unternehmen, Vereinen und Parteien.

Für die Kontrolle von Behörden steht wesentlich mehr Personal zur Verfügung als für die Kontrolle von Unternehmen

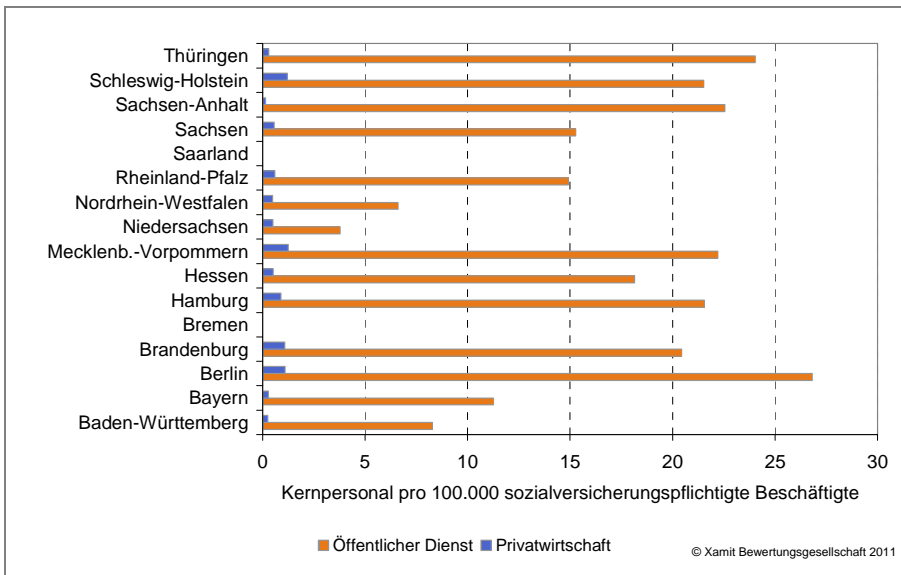


Abbildung 14: Kernpersonal pro 100.000 sozialversicherungspflichtig Beschäftigter

Abbildung 15 zeigt die Stellenverteilung pro 100.000 sozialversicherungspflichtig Beschäftigter für den nicht-öffentlichen Bereich nach Bundesländern.

⁵¹ Quelle: http://www.statistik-portal.de/Statistik-Portal/de_enterprise.asp?reg=00. Letzter Zugriff: 2010-11-18.

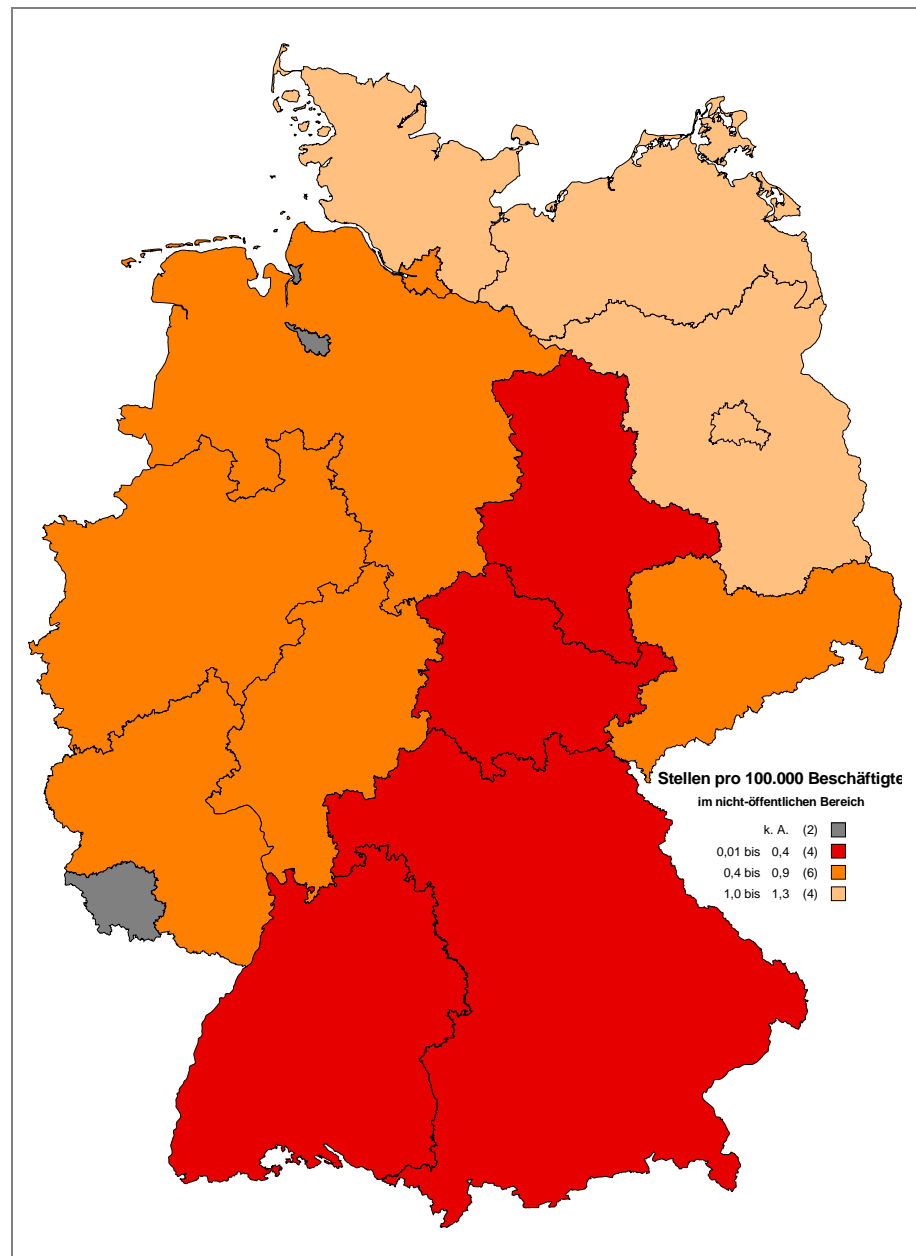


Abbildung 15: Stellenverteilung im nicht-öffentlichen Bereich in Relation zur Anzahl sozialversicherungspflichtiger Beschäftigter. Die Zahlen in Klammern zeigen die Anzahl an Bundesländern, die den jeweiligen Werten entsprechen.

6.3 Tätigkeiten und Erfolge

Zum Tätigkeitsspektrum einer Datenschutzaufsichtsbehörde zählen in der Praxis:

- Datenschutzberatung und Bearbeitung von Eingaben (Kapitel 6.3.1),
- Kontrolle (Kapitel 6.3.2) und
- Sanktionen (Kapitel 6.3.3).

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 2010, die wir in Kapitel 6.3.4 vorstellen, werfen ein Schlaglicht auf weitere Tätigkeiten.

6.3.1 Datenschutzberatung und Eingaben im Jahr 2010

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:

Aufsichtsbehörden sind Ansprechpartner für Bürger sowie für private und öffentliche Stellen

- **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 neun Aufsichtsbehörden liegen uns statistische Angaben für das Jahr 2010 vor. Zwei Aufsichtsbehörden führen nach eigenen Angaben keine Statistik. Weitere fünf konnten die Angaben aufgrund des Aufwandes nicht ermitteln. Für zwei Aufsichtsbehörden haben wir einige statistische Angaben aus den Tätigkeitsberichten, Pressemitteilungen und anderen Quellen selbst recherchiert.

Aufsichtsbehörden messen ihre internen Vorgänge nach unterschiedlichen Verfahren. Die einen erfassen jeden Kontakt mit der Behörde,

Aufsichtsbehörden messen ihre internen Vorgänge nach unterschiedlichen Verfahren, daher sind sie nicht vergleichbar

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.

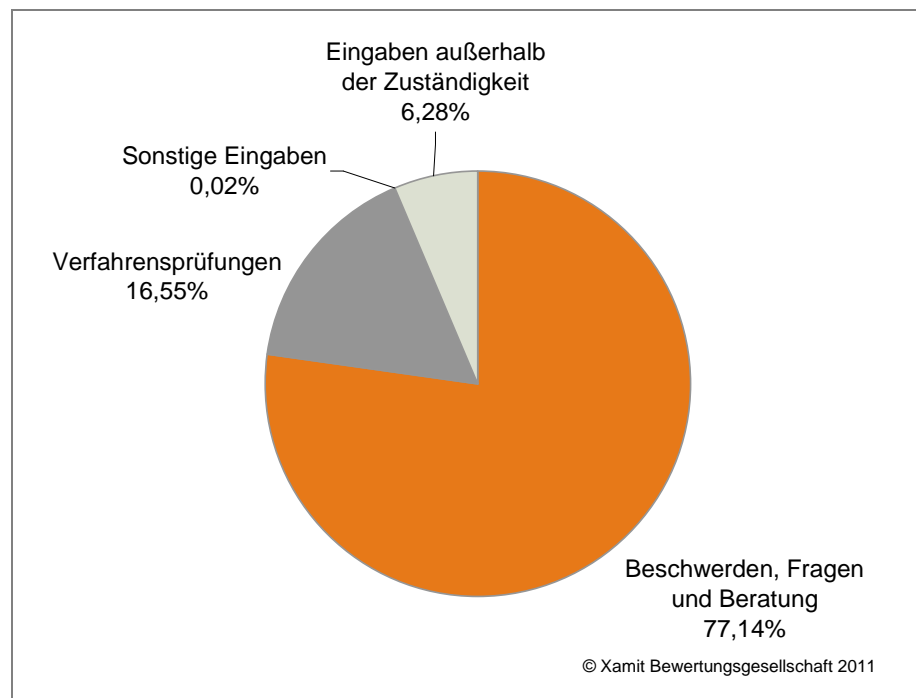


Abbildung 16: Verteilung der Eingaben

Insgesamt wurden uns 44.127 Eingaben gemeldet. Für eine weitere Behörde haben wir zusammen 3.000 Eingaben in Veröffentlichungen gefunden. Von den zusammen 47.127 Eingaben lassen sich 17.141 inhaltlich nicht weiter unterteilen. Von den übrigen 29.986 Eingaben bilden Beschwerden, Fragen und Beratung mit 77% den Schwerpunkt. Verfahrensprüfungen folgen mit knapp 17% (Abbildung 16).

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.

Vorgestellte Zahlen spiegeln nur einen Bruchteil der tatsächlich zu bearbeitenden Vorgänge wieder

6.3.2 Kontrollen im Jahr 2010

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.

Kontrollen prüfen die Einhaltung ausgewählter Datenschutzvorschriften

Sieben Behörden haben unsere Fragen zur Anzahl der Kontrollen im Jahr 2010 beantwortet. Die übrigen Behörden gaben an, keine Statistik zu führen oder dass die Ermittlung mit zu hohem Aufwand verbunden sei. Auch bei dieser Frage ist die Vergleichbarkeit nicht durchgängig gegeben, da bspw. eine Behörde eine Kontrolle ohne Begehung vor Ort auch unter den Eingaben (Kapitel 6.3.1) erfasst.

Vier Behörden führten zwischen sechs und 22 Vor-Ort-Kontrollen bei nicht-öffentlichen Stellen durch. Für öffentliche Stellen fehlt teilweise die statistische Erfassung. Das ULD kontrollierte ca. 60 öffentliche und ca. 40 nicht-öffentliche Stellen vor Ort. Die meisten Vor-Ort-Kontrollen führte der Bundesbeauftragte mit ca. 108 für beide Bereiche zusammen durch. Vor-Ort-Kontrollen sind personalintensiv, weshalb sie zurückhaltend eingesetzt werden.

Zusätzlich zu den Vor-Ort-Kontrollen überprüfte das ULD 410 öffentliche und 430 nicht-öffentliche Stellen. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit erhöht seine Kontrollhäufigkeit mit seinem Konzept der schriftlichen Prüfungen deutlich. Dieses bezieht sich in erster Linie auf den betrieblichen Datenschutzbeauftragten. So wurden im Jahr 2010 360 Kontrollen im öffentlichen Bereich und 946 Kontrollen im nicht-öffentlichen Bereich durchgeführt, obwohl seine Behörde zu den kleineren Aufsichtsbehörden gehört (s. Kap. 6.2). Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen hat seine Kontrollen ebenfalls deutlich ausgeweitet. Zusätzlich zu zahlreichen weiteren Kontrollen befragte er postalisch 1.000 Unternehmen, ob sie einen Datenschutzbeauftragten bestellt hätten. 10% der Unternehmen sind ihrer gesetzlichen Pflicht nicht nachgekommen.

6.3.3 Sanktionen im Jahr 2010

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.

Sanktionen helfen, gesetzliche Vorschriften durchzusetzen

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

Sanktionsinstrumente der Aufsichtsbehörden

- 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. Die Datenschutzaufsichtsbehörde von Großbritannien, „Information Commissioner’s Office“, verfügt hier über deutlich stärkere Sanktionen: Bspw. verhängte sie wegen des Verlusts eines unverschlüsselten Notebooks mit sensiblen personenbezogenen Daten 70.000 GBP gegen Hounslow Council als Auftraggeber der Datenverarbeitung und 80.000 GBP gegen Ealing Council als Auftragnehmer.⁵² Beides sind öffentliche Stellen.

Jedes Bundesland regelt autonom, welche Sanktionen eine Aufsichtsbehörde verhängen darf

Welche Sanktionen eine Aufsichtsbehörde verhängen darf, regelt jedes Bundesland autonom. Bspw. erhielt der Landesbeauftragte für den Datenschutz Baden-Württemberg mit der Neuregelung der Datenschutzaufsicht zum 1. April 2011 nicht das Recht, Datenschutzverstöße mit einem Bußgeld zu ahnden. Dafür ist das Regierungspräsidium Karlsruhe zuständig,⁵³ das im Unterschied zum Datenschutzbeauftragten nicht unabhängig ist.

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

⁵² Information Commissioner’s Office (2011). URL: http://www.ico.gov.uk/what_we_cover/taking_action/~media/documents/library/Data_Protection/Notices/ealing_council_monetary_penalty_notice.ashx und http://www.ico.gov.uk/what_we_cover/taking_action/~media/documents/library/Data_Protection/Notices/london_borough_of_hounslow_monetary_penalty_notice.ashx. Letzter Zugriff: 2011-11-21.

⁵³ Der Landesbeauftragte für den Datenschutz Baden-Württemberg (2011): Noch eine Zäsur - Datenschutz aus einer Hand in Baden-Württemberg. Pressemitteilung. URL: http://www.baden-wuerttemberg.datenschutz.de/lfd/pm/2011/03_31.htm. Letzter Zugriff: 2011-11-21.

der übrigen Behörden erfassen nach eigenen Angaben diese Tätigkeiten nicht statistisch. Tabelle 3 zeigt die Ergebnisse.

Bundesland	Beanstandungen öffentl. Bereich	Beanstandungen nicht-öffentl. Bereich	Untersagte Verfahren nicht-öffentl. Bereich
Bund	ca. 30		0
Bayern	k. A.	149	k. A.
Hamburg	k. A.	k. A.	ca. 18
Hessen	1	330	
Schleswig-Holstein	ca. 40	ca. 100	k. A.
Thüringen	6	15	3

Tabelle 3: Beanstandungen und untersagte Verfahren

Ein betrieblicher Datenschutzbeauftragter wurde von keiner der teilnehmenden Behörden abberufen. 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 Interessenkonflikte 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.⁵⁴ Es stellt die Fachkunde und Zuverlässigkeit sicher. Darauf verpflichtete Datenschutzbeauftragte erfüllen damit die Anforderungen des Düsseldorfer Kreises an den betrieblichen Datenschutzbeauftragten.⁵⁵

Acht Aufsichtsbehörden haben uns die Anzahl und Summe der verhängten Bußgelder mitgeteilt. Die damalige Aufsichtsbehörde für den nicht-öffentlichen Bereich von Baden-Württemberg hat 2010 ein verhängtes Bußgeld öffentlich bekannt geben.⁵⁶ Wir nehmen dieses als untere Grenze für die verhängten Bußgelder von Baden-Württemberg an, da uns der Landesbeauftragte für den Datenschutz Baden-Württemberg bedingt durch die Zusammenlegung der Datenschutzaufsicht keine genaueren Angaben geben konnte.

⁵⁴ URL: https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/leitbild/bvd-leitbild-2011.pdf.
Letzter Zugriff: 2011-11-22.

⁵⁵ 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: 2011-11-22.

⁵⁶ Heise Online (2010): Drogeriekette wegen Datenschutzverstoßes bestraft. 12.01.2010. URL: <http://heise.de/-902638>. Letzter Zugriff: 2011-11-22.

In 2010 wurden Bußgelder in Höhe von mindestens 554.740 Euro in Summe verhängt

Im Jahr 2010 wurden insgesamt mehr als 50 Bußgelder (eine Behörde gab nur die Summe und nicht die Anzahl an) von mindestens 554.740 Euro in Summe verhängt. Davon sind mindestens 389.490 Euro rechtskräftig. Tabelle 4 zeigt eine Rangliste der verhängten Bußgelder nach Bundesländern in absteigender Reihenfolge. Dabei macht der erste Rang (Hamburg) 37% der Gesamtsumme an Bußgeldern in 2010 aus.

Rang	Bundesland
1	Hamburg
2	Baden-Württemberg
3	Nordrhein-Westfalen
4	Berlin
5	Hessen
6	Schleswig-Holstein
7	Bayern
8	Thüringen
9	Sachsen-Anhalt
k. A.	Übrige Bundesländer
Keine Sanktionsbefugnis	Bund

Tabelle 4: Rangliste der verhängten Bußgelder (rechtskräftige und nicht rechtskräftige) gegen nicht-öffentliche Stellen nach Bundesländern

Zwischen September 2004 und August 2008, d. h. in einem Zeitraum von vier Jahren, wurden bundesweit zusammen 158 Bußgelder in Höhe von 269.395 Euro verhängt.⁵⁷ Im September 2008 verhängten 12 Aufsichtsbehörden Bußgelder in Summe von 1,5 Mio. Euro gegen 35 Vertriebsgesellschaften von Lidl (Abbildung 17).⁵⁸ Eine Rekordsumme, die jedoch die britische Finanzaufsicht mit einem Bußgeld von 2,8 Mio. Euro gegen die Versicherung Zurich Insurance PLC wegen des Verlusts eines Datenträgers mit Daten von 46.000 Kunden weit übertraf.⁵⁹

In 2009 wurden die Bußgeldhöchstgrenzen für Datenschutzverstöße angehoben und neue Tatbestände geschaffen

Durch die Novelle des BDSG vom 1. September 2009 wurden nicht nur die Bußgeldhöchstgrenzen angehoben, sondern auch neue Bußgeldtatbestände, bspw. bei rechtswidriger Nutzung personenbezogener Daten, geschaffen. Im Jahr 2010 verhängten allein neun Aufsichtsbehörden mindestens 554.740 Euro. Abgesehen vom Rekordbußgeld gegen Lidl im Jahr 2008 wurden im Jahr 2010 insgesamt deutlich mehr Bußgelder verhängt als im Zeitraum von 2004 bis 2008 zusammen.

⁵⁷ 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.

⁵⁸ 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: 2011-11-18.

⁵⁹ Die Welt (2010): Millionenstrafe wegen Panne. URL: <http://www.welt.de/die-welt/wirtschaft/article9183202/Millionenstrafe-wegen-Panne.html>. Letzter Zugriff: 2011-11-18.

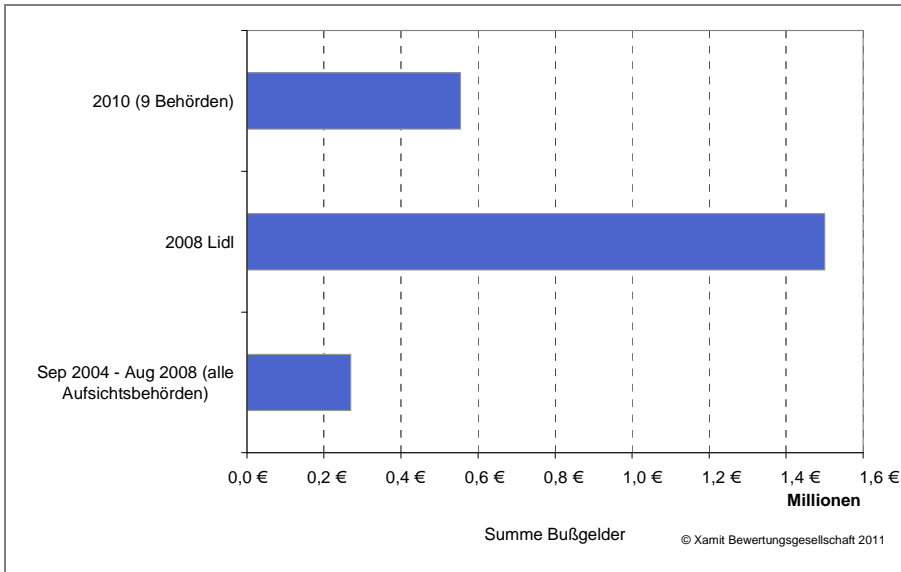


Abbildung 17: Vergleich Bußgelder 2004-2008 mit 2010

6.3.4 Erfolge im Jahr 2010

Vier Aufsichtsbehörden haben uns ihre größten Erfolge 2010 mitgeteilt. Diese werfen ein Schlaglicht auf weitere Tätigkeiten, die Aufsichtsbehörden ausüben.

2010 und 2011 sind für die meisten Aufsichtsbehörden durch eine personal und zeitintensive Zusatzbelastung gekennzeichnet: Umsetzung des EuGH-Urteils zur vollständigen Unabhängigkeit (Kapitel 6.1). Für die Umsetzung mussten (und müssen teilweise noch) die Landesdatenschutzgesetze novelliert werden, d. h. Entwürfe müssen erstellt und kommentiert und zahlreiche politische Gespräche geführt werden. Da der EuGH die Art und Weise der Umsetzung nicht vorgegeben hat, bleibt Raum für politische Gestaltung, die zu einer Stärkung oder Schwächung (bspw. fehlende Bußgeldzuständigkeit) der Aufsichtsbehörden führen kann. War die Aufsicht in dem jeweiligen Bundesland vorher auf zwei Aufsichtsbehörden verteilt, stand und teilweise steht die ebenfalls Ressourcen zehrende Zusammenlegung zu einer Behörde an. Vor diesem Hintergrund spricht der Hessische Datenschutzbeauftragte, Prof. Dr. Michael Ronellenfitsch, sicherlich seinen Kollegen aus der Seele, wenn er seinen größten Erfolg in 2010 so beschreibt:

„Die Überzeugung der Politik, bzw. des Parlaments, dass eine Zusammenlegung der Datenschutzaufsicht im öffentlichen und nicht-öffentlichen Bereich und die Ausstattung mit völliger Unabhängigkeit erforderlich ist.“

Aufsichtsbehörden wirken nicht nur im Verborgenen, sondern auch öffentlich. Öffentlichkeit ist ein Weg, auch auf die Datenschutzrisiken von politischen Entscheidungen, wie z. B. ELENA, hinzuweisen. Dieses ist eine Möglichkeit der Prävention von Datenschutzverstößen.

Der Prozess der Unabhängigwerdung der Aufsichtsbehörden band in 2010 und 2011 viele Ressourcen

Der hessische Datenschutzbeauftragte

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Herr Ulrich Lepper, schreibt:

Der nordrhein-westfälische
Datenschutzbeauftragte

„Für 2010 möchte ich keinen Erfolg besonders hervorheben. Zwar sind einige meiner Auffassungen bestätigt worden (z. B. zu den Themen Vorratsdatenspeicherung oder ELENA), jedoch nicht in einem direkten Zusammenhang so, dass ich sie maßgeblich mir als Erfolg anrechnen möchte. Ordnungswidrigkeitsverfahren mit hohen Bußgeldern sind zwar bemerkenswert, ich sehe sie aber nicht als Erfolg. Erfolgreich bin ich dann, wenn Datenschutzmängel wegen meiner Tätigkeit beseitigt werden. Das war auch 2010 vielfach der Fall. Erfolgreich bin ich aber auch dann, wenn wegen meiner Tätigkeit schon gar keine potenziellen Datenschutzmängel auftreten. Dieser Erfolg lässt sich allerdings selten kausal nachweisen.“

Der Landesbeauftragte für Datenschutz Schleswig-Holstein, Dr. Thilo Weichert, nennt drei Erfolge, die die Bandbreite seiner Tätigkeiten beleuchten:

Der schleswig-holsteinische
Datenschutzbeauftragte

- „Datenschutz bei der hausarztzentrierten Versorgung“⁶⁰
- LDSG-Änderungsvorschläge⁶¹
- ULD-Konzept⁶²

Der erste Erfolg zeigt exemplarisch, dass eine Durchsetzung von Datenschutzgesetzen nicht ohne Sanktionen und gerichtliche Unterstützung auskommt. Um eine hausarztzentrierte Versorgung in Schleswig-Holstein aufzubauen, wurde in einem Schiedsverfahren ein Vertrag zwischen den Leistungserbringern (Hausärzteverband Schleswig-Holstein, Ärztegenossenschaft) und einigen Krankenkassen (AOK NordWest, IKK Landesverband Nord, Landwirtschaftlichen Krankenkasse Schleswig-Holstein und Hamburg) abgeschlossen. Dieser Vertrag sah vor, dass die Patientendaten von einem Dienstleister, der Hausärztlichen Vertragsgemeinschaft (HÄVG), elektronisch verarbeitet werden sollten. Gesetzlich ist eine solche Datenverarbeitung nur im Rahmen einer „sozialrechtlichen Auftragsdatenverarbeitung“ möglich, für die es gesetzliche Anforderungen gibt. Ein wesentliches Element ist die Kontrolle des Auftraggebers über die Datenverarbeitung. Diese Kontrolle sei nach einem Beschluss des Obergerichtes Schleswig-Holstein⁶³ durch den Vertrag nicht gegeben. Vielmehr verstoße der 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 Landes-zentrums für Datenschutz Schleswig-Holstein (ULD) an den Hausärz-

⁶⁰ Details siehe https://www.datenschutzzentrum.de/material/tb/tb33/kap04_5.htm#453. Letzter Zugriff: 2011-12-06.

⁶¹ Details siehe <https://www.datenschutzzentrum.de/material/tb/tb33/kap01.htm#11>. Letzter Zugriff: 2011-12-06.

⁶² Details siehe <https://www.datenschutzzentrum.de/material/tb/tb33/kap01.htm#12>. Letzter Zugriff: 2011-12-06.

⁶³ Schleswig-Holsteinisches Obergericht. Beschluss vom 12.01.2011, Az. 4 MB 56/10 und 14 B43/10.

teverband Schleswig-Holstein „dafür zu sorgen, dass keine von den Hausärzten im Zusammenhang mit der Durchführung des Vertrages erhobenen personenbezogenen Daten der Patienten an die HÄVG oder an andere in dem genannten Vertrag vorgesehene Unterauftragnehmer weitergegeben werden.“⁶⁴

Onlinedienste und elektronische Datenverarbeitung sind untrennbar miteinander verbunden. Die Frage nach einem datenschutzgerechten Umgang mit personenbezogenen Daten stellt sich für diese Dienste daher mit besonderer Bedeutung. Hinzu kommt, dass jeder Staat unter datenschutzkonformem Umgang mit persönlichen Daten etwas anderes versteht. Dies ist eine Herausforderung für grenzüberschreitende Dienste. Gerade Anbieter aus Staaten mit geringerem Datenschutzniveau tun sich oft schwer, die hiesigen Anforderungen zu verstehen, ernst zu nehmen und letztlich auch umzusetzen. Hier ist in den letzten Jahren eine neue Aufgabe für Aufsichtsbehörden entstanden. Stellvertretend für deutsche Bürger verhandeln sie mit ausländischen Anbietern populärer Dienste, um diese zu einer gesetzeskonformen Gestaltung zu bewegen. Sie helfen, das Machtungleichgewicht, das zwischen Konzernen mit einem Milliardenumsatz und Konsumenten besteht, zu reduzieren. Diese Unternehmen betreiben oftmals sehr beliebte Dienste, für die es aus unterschiedlichen Gründen keine vergleichbare Alternative gibt. Deshalb hilft der simple Rat, sich durch Kauf- oder Nutzungsverweigerung zu schützen, nicht weiter. Eine in diesem Kontext engagierte Behörde ist die des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Prof. Dr. Johannes Caspar. Er beschreibt seinen Erfolg so:

„Vereinbarung mit Google über die (Vorab-) Widerspruchsmöglichkeit bei Google Street View“.

Der hamburgische Datenschutzbeauftragte

Diese Aufgaben werden in Zukunft weiter an Bedeutung gewinnen. Beispiele aus der jüngsten Zeit:

- Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit beanstandet die Biometriedatenbank, die Facebook von seinen Nutzern pflegt, um hochgeladene Fotos automatisch mit Namen der abgebildeten Personen versehen zu können. Er droht Facebook rechtliche Konsequenzen an.⁶⁵
- Das Unabhängige Landeszentrum für Datenschutz verhandelt mit Facebook über eine datenschutzkonforme Ausgestaltung des Facebook Like-Buttons.⁶⁶ Gleichzeitig geht die Behörde

⁶⁴ ULD (2011): 33. Tätigkeitsbericht des ULD (2010). Landtagsdrucksache 17/1220. URL: https://www.datenschutzzentrum.de/material/tb/tb33/kap04_5.htm#453. Letzter Zugriff: 2011-12-06.

⁶⁵ Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (2011): Biometrie-Datenbank von Facebook weiterhin rechtswidrig. Pressemitteilung vom 10.11.2011. URL: <http://www.datenschutz-hamburg.de/news/detail/article/biometrie-datenbank-von-facebook-weiterhin-rechtswidrig.html>. Letzter Zugriff: 2011-11-22.

⁶⁶ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2011): ULD: „Dialog mit Facebook hindert nicht Durchsetzung des Datenschutzes“. Pressemitteilung vom 30.09.2011. URL: <https://www.datenschutzzentrum.de/presse/20110930-facebook-datenschutz-durchsetzen.html>. Letzter Zugriff: 2011-11-22.

- gegen Webseitenbetreiber vor, die den Like-Button verwenden.⁶⁷
- Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen prüft die Verkaufsplattform „Origin“ von Electronic Arts für Computerspiele auf Einhaltung der geltenden Datenschutzvorschriften.⁶⁸ Das US-amerikanische Unternehmen verfügt über eine deutsche Tochtergesellschaft „Electronic Arts GmbH“ mit Sitz in Köln, die – wie in solchen Konstellationen üblich – Ansprechpartner für die Aufsichtsbehörde ist. Da sich Electronic Arts bei der Markteinführung von Origin in den Nutzungsbedingungen zahlreiche Rechte einräumen wollte, die gegen deutsche Datenschutz- und Verbraucherschutzgesetze verstießen, war der Dienst öffentlich in die Kritik geraten.⁶⁹ Electronic Arts hat seine Nutzungsbedingungen daraufhin geändert. Ob die Änderungen ausreichend sind und ob Origin Computernutzer tatsächlich ausspioniert, ist noch nicht abschließend geklärt. Die Verbraucherzentralen haben Electronic Arts abgemahnt.⁷⁰ Das Fachmagazin c't kommt in einer eigenen Untersuchung zu dem Schluss, dass Origin nicht mehr Daten als üblich übertrage.⁷¹ Eine datenschutzrechtliche Bewertung war nicht Gegenstand der c't-Untersuchung. Die Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen steht noch aus. Sollten Datenschutzverstöße festgestellt werden, stehen der Aufsichtsbehörde neben dem Verhandlungsweg auch Sanktionen, wie Untersagung und Bußgelder, zur Verfügung

Durch die Digitalisierung unserer Gesellschaft wird das Datenschutzrecht in Deutschland immer komplexer. Mit der zunehmenden Gefährdung der Privatsphäre, der sich wandelnden Gesetzgebung und der verstärkten Wahrnehmung des Themas „Datenschutz“ bei der Bevölkerung ändern sich auch die Aufgaben der Aufsichtsbehörden. Neben ihrer Funktion aufzuklären und zu beraten, treten weitere ebenso wichtige Aufgaben hinzu, wie z. B. die Durchsetzung von Datenschutzgesetzen gegenüber Unternehmen.

⁶⁷ Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2011): Bisher nur mäßiger Erfolg der ULD-Facebook-Abmahnungen. Pressemitteilung vom 04.11.2011. URL: <https://www.datenschutzzentrum.de/presse/20111104-facebook-abmahnungen.htm>. Letzter Zugriff: 2011-12-02.

⁶⁸ Heise Online (2011): Electronic Arts Deutschland äußert sich zu Spyware-Vorwürfen. 01.11.2011. URL: <http://heise.de/-1369395>. Letzter Zugriff: 2011-11-22.

⁶⁹ Gamestar (2011): Der Teufel im Vertragsdetail. 25.10.2011. URL: [http://www.gamestar.de/spiele/battlefield-](http://www.gamestar.de/spiele/battlefield-3/artikel/analyse_zur_eula_von_ea_origin,45612,2561554.html)

[3/artikel/analyse_zur_eula_von_ea_origin,45612,2561554.html](http://www.gamestar.de/spiele/battlefield-3/artikel/analyse_zur_eula_von_ea_origin,45612,2561554.html). Letzter Zugriff: 2011-12-02.

⁷⁰ Gamestar (2011): Origin - Verbraucherzentrale mahnt Electronic Arts ab. 30.11.2011. URL: <http://www.gamestar.de/news/vermischtes/2562564/origin.html>. Letzter Zugriff: 2011-12-02.

⁷¹ c't (2011): Origin spioniert nicht. 25/2011. S. 42

7 Verzerrter Wettbewerb: Milliardengewinne dank Datenschutzverstöße

Seit 2008 erheben wir im XAMIT Datenschutzbarometer Datenschutzverstöße. In diesem Zeitraum nahmen die Verstöße bis heute um 49% zu (Abbildung 18). Nach Abzug aller Verstöße, die nach 2008 aufgenommen worden sind, wie z. B. der Facebook Like-Button, bleibt immer noch eine Steigerung von 34%.

Seit 2008 haben die Datenschutzverstöße allein im Internet um 34% zugenommen

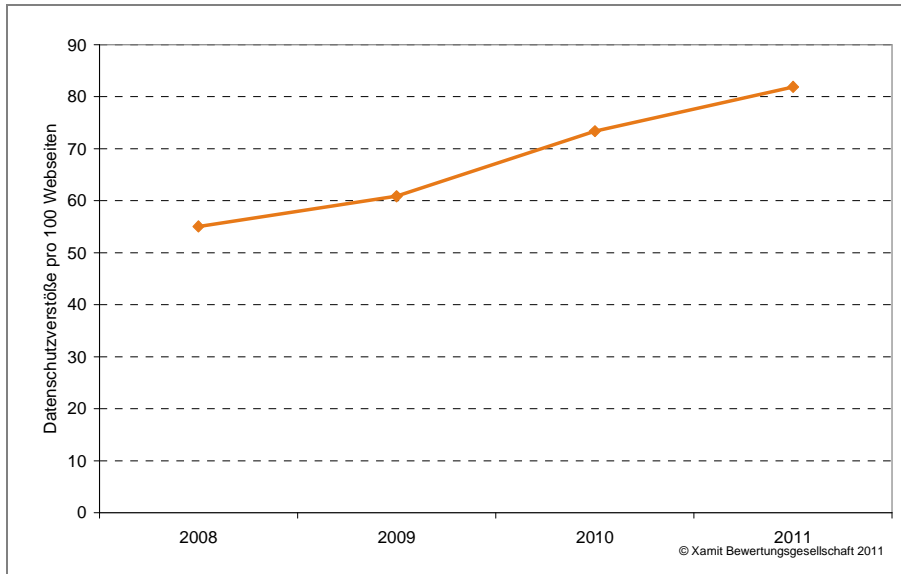


Abbildung 18: Entwicklung des Datenschutzbarometers seit 2008

Ein wesentlicher Teil der Steigerung geht auf die zunehmende Nutzung nicht datenschutzkonformer Webstatistikdienste, insbesondere von Google Analytics ohne Anonymisierung, zurück (vgl. Kapitel 4.3). Was könnten die Ursachen sein? Mangelndes Wissen um die fehlende Datenschutzkonformität scheidet als Erklärung aus, da seit 2008 immer wieder darüber öffentlich berichtet wird. Wirtschaftliche Vorteile liegen indes auf der Hand.

Es werden immer mehr nicht datenschutzkonforme Webstatistik-Dienste genutzt

Wer auf den Einsatz der legalen Version von Google Analytics verzichtet und weiter die nicht konforme Version einsetzt, spart viel Geld. Um die Dimension der eingesparten Kosten aufzuzeigen, wagen wir eine vorsichtige Schätzung, die auf stark vereinfachten Annahmen beruht und keine Kalkulation für den Einzelfall darstellt:

- 500 Euro für die formelle Prüfung des Vertrags zur Auftragsdatenverarbeitung und der in § 11 BDSG vorgeschriebenen Erstkontrolle des Dienstleisters.
- 7,50 Euro pro Webseite, um die Anonymisierung in den Quellcode einzubauen bei einem angenommenen Aufwand von 6 Minuten pro Webseite inkl. Testung und einem marktüblichen Stundensatz von 75 Euro.

- 51%⁷² aller 3.591.265 deutschen Unternehmen⁷³ betreiben eine Webpräsenz.
- In unserer Erhebung haben wir 72 Seiten pro Webseite als durchschnittliche Größe einer Webpräsenz ermittelt.
- Die nicht anonyme Version von Google Analytics wird von 22% der Webpräsenzen verwendet.

Damit werden durch diesen Datenschutzverstoß bundesweit bereits $3.591.265 \times 51\% \times 22\% \times (72 \text{ Seiten} \times 7,50 \text{ Euro/Seite} + 500 \text{ Euro}) = 419.057.530 \text{ Euro}$ erwirtschaftet. Hierbei ist nicht eingerechnet, dass Unternehmen oftmals mehrere Webpräsenzen betreiben, wie z. B. für unterschiedliche Produkte.

Die Umstellung auf einen datenschutzkonformen Webstatistik-Dienst kostet 1.040 Euro pro Webpräsenz

1.040 Euro pro Unternehmen ist eine relativ geringe Summe. Wenn schon eine so einfache Anpassung unterbleibt, wie steht es dann um die Umsetzung komplexerer Datenschutzprozesse?

Ein Verzicht auf den gesetzlich vorgeschriebenen Datenschutzbeauftragten steigert den Gewinn zusätzlich:

Der Verzicht auf den gesetzlich geforderten Datenschutzbeauftragten „spart“ einem Unternehmen im Schnitt 20.000 Euro im Jahr

- Angenommen, ein Datenschutzbeauftragter kostet über alle Unternehmensgrößen und Branchen betrachtet im Mittel pro Jahr 20.000 Euro.
- Bundesweit existieren 306.380 Unternehmen⁷⁴ mit mehr als neun Beschäftigten. Bestellpflichtige Unternehmen mit weniger als zehn Beschäftigten lassen wir der Einfachheit halber unberücksichtigt.
- Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen stellte fest, dass 10% der Unternehmen ihrer gesetzlichen Bestellpflicht nicht nachkommen (Kapitel 6.3.2).

Durch den Verzicht auf den Datenschutzbeauftragten steigern Unternehmen ihren Gewinn – wenn wir die Prozentzahlen für NRW als repräsentativ für alle Bundesländer annehmen – bundesweit um $306.380 \times 10\% \times 20.000 \text{ Euro} = 612.760.000 \text{ Euro}$. Jahr für Jahr. Ein beachtlicher Wettbewerbsvorteil gegenüber gesetzestreuen Unternehmen.

Wer auf seine Arbeitsgrundlage für den Datenschutz, das gesetzlich vorgeschriebene Verfahrensverzeichnis, verzichtet, spart noch mehr. Zusätzlich fehlt dem Unternehmen dann auch der Überblick, welche personenbezogenen Daten überhaupt verarbeitet werden. Damit sind

⁷² Laut Statistischem Bundesamt betreiben 2010 62% aller Unternehmen mit Internetzugang eine Webpräsenz. 82% aller Unternehmen besaßen 2010 einen Internetzugang. Damit betreiben $62\% \times 82\% = 51\%$ aller Unternehmen eine Webpräsenz. Quelle: <http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Content/Statistiken/Informationsgesellschaft/Unternehmen/Tabellen/Content75/AnteilUnternehmenComputernutzung,templateId=renderPrint.psml>. Letzter Zugriff: 2011-11-29.

⁷³ Stand: 2007. Quelle: <http://statistik.arbeitsagentur.de/cae/servlet/contentblob/101072/publicationFile/42755/Monatsbericht-201010.pdf;jsessionid=72480BB26CD1FCF2FED43B4B3677DCA7>

⁷⁴ Stand: 2007. Quelle: <http://statistik.arbeitsagentur.de/cae/servlet/contentblob/101072/publicationFile/42755/Monatsbericht-201010.pdf;jsessionid=72480BB26CD1FCF2FED43B4B3677DCA7>

Zweckänderungen, ausbleibende Löschungen, Sicherheitsprobleme und weitere Datenschutzverstöße vorprogrammiert:

- In unserem Feldtest aus dem Jahr 2009⁷⁵ haben 90% der angeschriebenen Unternehmen, Behörden und Vereine kein Verfahrensverzeichnis zugesandt, obwohl sie dieses Jedermann auf Anforderung zugänglich machen müssen. 5% reagierten mit Gegenfragen oder verstanden das Thema nicht. Wir nehmen deshalb konservativ an, dass 90% der Unternehmen kein Verfahrensverzeichnis führen.
- Der Aufwand, ein Verfahrensverzeichnis zu erstellen, hängt von der Größe des Unternehmens und seinen Abläufen ab. Nehmen wir ohne zu übertreiben an, dass im Mittel über alle Unternehmen, vom Ein-Personenunternehmen bis zum Konzern mit 300.000 Mitarbeitern, ein Verfahrensverzeichnis in zwei Personentagen erstellt wird.
- Einen Personentag setzen wir mit Kosten von 1.000 Euro an.

Unternehmen, die auf das vorgeschriebene Verfahrensverzeichnis verzichten, gewinnen einen Wettbewerbsvorteil von $3.591.265 \times 90\% \times 2.000 \text{ Euro} = 6,464 \text{ Mrd. Euro}$. Die jährliche Aktualisierung des Verzeichnisses nicht mit eingerechnet.

Durch das fehlende Verfahrensverzeichnis „gewinnt“ ein Unternehmen durchschnittlich 2.000 Euro

Bereits diese drei Verstöße bedeuten einen zusätzlichen Gewinn von 7,5 Mrd. Euro für nicht datenschutzkonform handelnde Unternehmen. Der tatsächlich erwirtschaftete Vorteil wird jedoch um ein Vielfaches höher liegen. Denn ein Datenschutzbeauftragter hilft in der Regel mit, Datenschutzverstöße zu vermeiden. Wird bewusst auf ihn verzichtet, steigt die Wahrscheinlichkeit für weitere Verstöße im und durch ein Unternehmen deutlich an.

Wettbewerbsverzerrung: 7,5 Mrd. Euro weniger Gewinn für datenschutzkonform handelnde Unternehmen

Privatwirtschaftliche Unternehmen, die mit kommunalen Betrieben im Wettbewerb stehen, leiden unter einem zusätzlichen Wettbewerbsnachteil. Als öffentliche Stelle können kommunale Betriebe bei Datenschutzverstößen oft nur gerügt und nicht stärker sanktioniert werden (Kapitel 6.3.3). Private Unternehmen müssen bei bekannt gewordenen Verstößen Bußgelder zahlen, während kommunale Betriebe keine einschneidenden Sanktionen fürchten müssen.

Unternehmen können sich gegen Wettbewerbsvorteile durch Datenschutzverstöße von Wettbewerbern kaum schützen. Das klassische Instrument, Unterlassungsansprüche auf Basis des Gesetzes gegen den unlauteren Wettbewerb (UWG) geltend zu machen, greift nicht. Denn nach der Konzeption der Gesetze, bekräftigt durch die Rechtsprechung, sind Datenschutzrechte individuelle Schutzrechte und keine den Wettbewerb regelnde Vorschriften.⁷⁶ Leidtragende dieser Wettbewerbsverzerrung sind

⁷⁵ Xamit (2009): Datenschutzbarometer 2009. URL: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>. Letzter Zugriff: 2011-11-29. S. 23.

⁷⁶ Vgl. für die Informationspflichten nach § 13 TMG Berliner Kammergericht Aktenzeichen: 5 W 88/11 vom 29.04.2011.

- 82 Mio. Bundesbürger und
- alle gesetzestreuen Unternehmen.

Gesetze ohne erkennbare Sanktionen entfalten keine Wirkung

Grundrechte zu schützen und für faire Wettbewerbsbedingungen zu sorgen ist eine genuine staatliche Aufgabe. Gesetze ohne praktisch verhängte Sanktionen entfalten i. d. R. keine Wirkung. Deshalb liegt es in den Händen der Datenschutzaufsichtsbehörden, ihre gewonnene Unabhängigkeit zu nutzen, um durch verstärkte Kontrollen und Sanktionen das Vollzugsdefizit zu verringern. Das wäre nicht nur ein Schritt zur Beseitigung der Wettbewerbsverzerrung zwischen gesetzestreuen und den Datenschutz vernachlässigenden Unternehmen. Dies würde gleichzeitig auch den grundgesetzlich gebotenen Datenschutz von Mitarbeitern, Kunden u. a. Betroffenen gewährleisten, den diese Unternehmen bisher aus wirtschaftlichen Erwägungen gering schätzen. Die Versprechen des Landesbeauftragten für Datenschutz und Informationsfreiheit, Ulrich Lepper,⁷⁷ und des hessischen Beauftragten für den Datenschutz, Michael Ronellenfitsch,⁷⁸ die Kontrollen und insbesondere die Vor-Ort-Kontrollen auszuweiten, machen Hoffnung.

Bundes- und Landesregierungen sind in der Pflicht, die Gesetze im Alltag zu vollziehen

Das Vollzugsdefizit verantworten aber auch die Bundesregierung und 16 Landesregierungen. Sie sind in der Pflicht,

- die Aufsichtsbehörden angemessen mit Personal auszustatten, so dass flächendeckende Kontrollen möglich werden,
- einheitliche Sanktionsmöglichkeiten für öffentliche und nicht-öffentliche Stellen zu schaffen und
- allen Aufsichtsbehörden die vollständige Sanktionskompetenz inkl. der Verhängung von Bußgeldern zu übertragen.

Der Vollzug der Datenschutzgesetze zeigt, wie ernst die jeweiligen Regierungen den Schutz von Unternehmen und Bürgern nehmen.

⁷⁷ Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (2011): Unabhängigkeit der Datenschutzaufsicht in NRW beschlossen – Lepper will Kontrolltätigkeit ausweiten und Medienkompetenz stärken. Pressemitteilung vom 30.06.2011. URL: https://www.ldi.nrw.de/mainmenu_Service/submenu_Pressemitteilungsarchiv/Inhalt/PM_Datenschutz/Inhalt/2011/Unabhaengigkeit/Unabhaengigkeit.php. Letzter Zugriff: 2011-11-23.

⁷⁸ Heise Online (2011): Hessischer Datenschützer nimmt Unternehmen verstärkt ins Visier. 23.06.2011. URL: <http://heise.de/-1266607>. Letzter Zugriff: 2011-11-25.

8 Fazit

Auch dieses Jahr haben die im XAMIT Datenschutzbarometer registrierten Datenschutzverstöße im Vergleich zum Vorjahr wieder zugenommen: Wir registrierten 12% mehr Verstöße als noch im letzten Jahr. Treiber sind nicht nur die Nutzung datenschutzwidriger Webstatistikdienste, sondern auch der Einsatz des Facebook Like-Buttons. Seine Verwendung hat explosionsartig zugenommen.

Der Trend zu mehr Verstößen und Beanstandungen im Internet ist ungebrochen

Der seit Jahren zu beobachtende Trend zu immer mehr Datenschutzverstößen ist weiter ungebrochen. Eine Umkehr wird wohl nur durch harte Sanktionen erreicht werden. Denn Datenschutzverstöße lohnen sich für Unternehmen finanziell: Der wirtschaftliche Vorteil durch Datenschutzverstöße summiert sich in der Bundesrepublik auf mehr als 7,5 Mrd. Euro. Die in 2010 verhängten Bußgelder von mindestens 554.740 Euro schöpfen diesen Vorteil jedoch nicht einmal ansatzweise ab.

Wettbewerbsnachteil für datenschutzkonforme Unternehmen von mehr als 7,5 Milliarden Euro



Abbildung 19: Milliarden Gewinne für Unternehmen durch Datenschutzverstöße

Die meisten Aufsichtsbehörden erhielten 2011 die seit 1995 vom Europäischen Gesetzgeber geforderte völlige Unabhängigkeit. Damit können sie nun unbeeinflusst ihre Aufgaben wahrnehmen. Allerdings verfügen nicht alle Aufsichtsbehörden über wirksame Sanktionsinstrumente, um Datenschutzverstöße abzustellen. Der Vollzug der Datenschutzgesetze wird so auf jeden Fall behindert.

Ohne wirksame Sanktions- und Kontrollmechanismen kann Datenschutz nicht gewährleistet werden

Angesichts dieser unveränderten, sich aber in ihren Auswirkungen immer weiter zuspitzenden Lage behält unser Fazit aus dem XAMIT Datenschutzbarometer 2010 seine Aktualität:

„Datenschutzskandale sind mittlerweile an der Tagesordnung und die Aufsichtsbehörden leiden unter extremem Personalmangel, so dass eine flächendeckende Kontrolle

faktisch nicht stattfindet. Was ist also zu tun? Hier ist die Politik gefordert, einen wirksamen Datenschutz durchzusetzen. Dazu gehört insbesondere eine adäquate Ausstattung der zuständigen Aufsichtsbehörden. Wirksamer Datenschutz ist die Voraussetzung, damit Bürger und Konsumenten vertrauen können. Fehlendes Vertrauen führt zu empfindlichen Wohlstandsverlusten, denn Käufe unterbleiben und zudem erhalten nicht datenschutzkonforme Unternehmen ungerechtfertigte Wettbewerbsvorteile.⁷⁹

⁷⁹ XAMIT (2010): XAMIT Datenschutzbarometer 2010, URL: <http://www.xamitleistungen.de/veroeffentlichungen/studien-und-tests/> S. 49.

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 Studien⁸⁰:

- „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 Aufsichtsbehörde⁸¹ oder den Verbraucherzentralen⁸² 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.⁸³
- Bei sensiblen Themen einen Anonymisierungsdienst verwenden.⁸⁴
- Bei Nutzung von Mozilla Firefox die Skripte selektiv mit der Firefox-Erweiterung „noscript“⁸⁵ steuern, so dass Cookies von

⁸⁰ Kostenfreier Download: <http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/index.php>

⁸¹ 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: 2010-12-09.

⁸² URL: <http://www.verbraucherzentrale.de>. Letzter Zugriff: 2010-12-09.

⁸³ Anleitungen für unterschiedliche Browser finden Sie im Internet. Bspw. hier: <http://www.informationelle-selbstbestimmung-im-internet.de/node4.html>. Letzter Zugriff: 2010-12-09.

⁸⁴ Kostenlos und relativ einfach zu installieren ist Jonym (https://www.jondos.org). Von dem Dienst Tor raten wir ab, da er gerne genutzt wird, um Passwörter auszuspähen.

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.

- Das Add on „Ghostery“⁸⁶ 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.

⁸⁵ Zu viele Webpräsenzen benötigen Skripte, um zu funktionieren. Deshalb stößt ein generelles Abschalten schnell an praktikable Grenzen. Bezugsquelle: <http://www.erweiterungen.de/detail/NoScript/>

⁸⁶ Bezugsquelle: <http://www.ghostery.com/>

10 Weitere Studien von XAMIT zum Thema Datenschutz

Alle Studien und ausgewählte Fachbeiträge finden Sie als kostenlosen Download auf unserer Webpräsenz.⁸⁷

Datenschutzbarometer 2010 – Neue Herausforderungen für Datenschützer

XAMIT führte eine umfassende Überprüfung von 26.742 Webpräsenzen von in Deutschland ansässigen Unternehmen, politischen Organisationen, Gemeinden und Vereinen durch. Insgesamt wurden über zwei Millionen Webseiten auf die Einhaltung geltender Datenschutzbestimmungen hin untersucht. Das Ergebnis: Insgesamt wurden 73 Beanstandungen pro 100 deutscher Webpräsenzen festgestellt, eine Steigerung von fast 20 Prozent gegenüber 2009.

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.

⁸⁷ <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

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. FlfF-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

