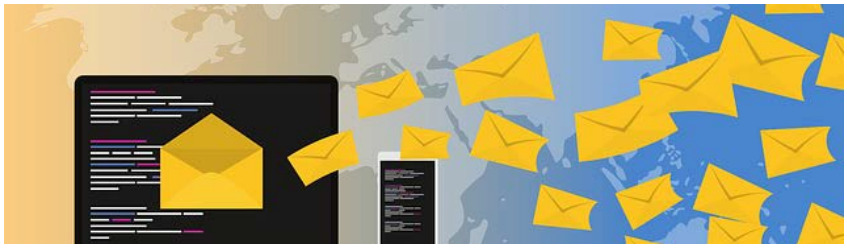
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg



Inhalt

Liebe Leserinnen und Leser,

nach dem ereignisreichen Jahr 2018 versuchen wir alle, wieder in den „Normalmodus“ hineinzufinden – und das fällt angesichts der ungebrochenen Nachfrage nach unserem gemeinsamen Thema Datenschutz nicht leicht. Ein Blick auf die Statistik unserer Dienststelle verrät, dass der Run auf die Beratungen, aber auch die Beschwerden und Datenpannenmeldungen auf höchstem Niveau bleiben.

Um so wichtiger, dass wir mit unserem Mantra „BeratenBeratenBeraten“ inzwischen nicht nur eine große Zahl von Themenfeldern abdecken (hier im Newsletter finden sich etwa unsere aktuellen Hinweise zum Umgang mit Passwörtern, Ratschläge zu Werbung und viele weiter Informationsmaterialien), sondern auch immer größere Adressatenkreise erreichen: „Datenschutz geht zur Schule“ ist nur ein neues Feld, auf dem sich der LfDI inzwischen engagiert, mit dazu zählt natürlich auch die inzwischen auf über 3.500 Follower angewachsene Twittergemeinde und die große Schar an Abonnenten dieses Newsletters.

2019 ist aber auch das Jahr der Kontrollen - bei der Vorstellung meines Tätigkeitsberichts im Januar 2019 hatte ich es ja bereits angekündigt. Im vergangenen Jahr, in dem die Europäische Datenschutz-Grundverordnung EU-DSGVO wirksam wurde, lag der Schwerpunkt der Tätigkeit der Datenschützer eindeutig auf der Beratung: Wir haben in über 200 Veranstaltungen mehr als 20.000 Bürgerinnen und Bürger sowie Mitarbeiterinnen und Mitarbeiter von Unternehmen und Behörden geschult, in tausenden von Einzelfällen haben wir beraten und unterstützt. Jetzt ist es unsere Aufgabe, den Erfolg unserer Arbeit zu überprüfen. Effektiven Datenschutz verlangt nicht nur die

EU-DSGVO, er wird auch von all jenen Unternehmen und Behörden eingefordert, die sich schon seit langer Zeit und mit großem Einsatz um den Datenschutz bemühten. Wer beim Datenschutz ‚auf Lücke‘ setzt, darf daraus keinen Vorteil gegenüber der datenschutzkonformen Konkurrenz ziehen – das ist schon ein Gebot der Fairness!

Wichtig ist mir dabei das Folgende: Kontrollen sind nicht gleichbedeutend mit Sanktionen oder gar Bußgeldern. Auch bei unseren umfangreichen Maßnahmen bleibt die Beratung und der Hinweis auf Verbesserungsmöglichkeiten das Mittel der Wahl. Strafen werden auch künftig nur bei gravierenden Verstößen und dann ausgesprochen, wenn klare Rechtsverletzungen nicht beseitigt werden. Ebenso wichtig ist: Ehrenamtlich tätige Vereine und kleine Firmen ohne größere Datenverarbeitungen stehen nicht im Fokus unserer Kontrollaktion. Auch in dieser Hinsicht bewahren wir Augenmaß!

In diesem Sinne wünsche ich Ihnen viel Spaß beim Lesen!
Ihr Stefan Brink

Dienststellenstatistik für 2018

BERATUNGSANFRAGEN

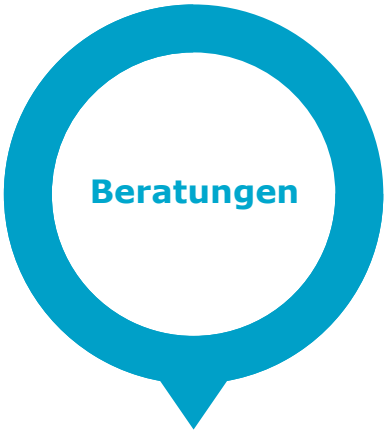
Die Auswirkungen der Datenschutzgrundverordnung (DS-GVO) auf den Geschäftsbetrieb der Dienststelle waren erheblich. In den reinen Statistikzahlen kommt dies nur unvollständig zum Ausdruck. Gleichwohl zeigt sich auch daran, dass die Datenschutzaufsicht mehr denn je gefordert ist, den Ansprüchen betroffener Bürgerinnen und Bürger ebenso gerecht zu werden wie derjenigen von Wirtschaft, Verbänden, Behörden und nicht zuletzt der Politik.

DATENPANNEN

Außerordentliche Steigerungsraten waren bei den Meldungen von Datenpannen zu verzeichnen. Diese haben sich im Jahr 2018 mit 774 Meldungen mehr als verzehnfacht. Zu erklären ist dies einerseits dadurch, dass die Meldepflicht jetzt erstmals auch für Behörden gilt. Zum anderen hat die Drohung mit empfindlichen Geldbußen sicher auch dazu beigetragen, dass die bisher im privaten Bereich schon bestehende Pflicht nun ernster genommen wird.

3902

Vergleicht man die Zahlen der in den letzten beiden Jahren jeweils eingegangenen Beschwerden, ergibt sich eine Steigerung insgesamt um ca. 30 Prozent. Während die Beschwerden über Behörden annähern konstant blieben, nahmen sie im privaten Bereich im Vergleich zum Vorjahr um ca. 50 Prozent deutlich zu. Insbesondere in diesem Bereich scheint die intensive Öffentlichkeitsarbeit meiner Dienststelle ebenso wie die mediale Berichterstattung rund um das Thema Datenschutz-Grundverordnung Früchte getragen und das Datenschutzbewusstsein der Bürgerinnen und Bürger geschärft zu haben.



4440

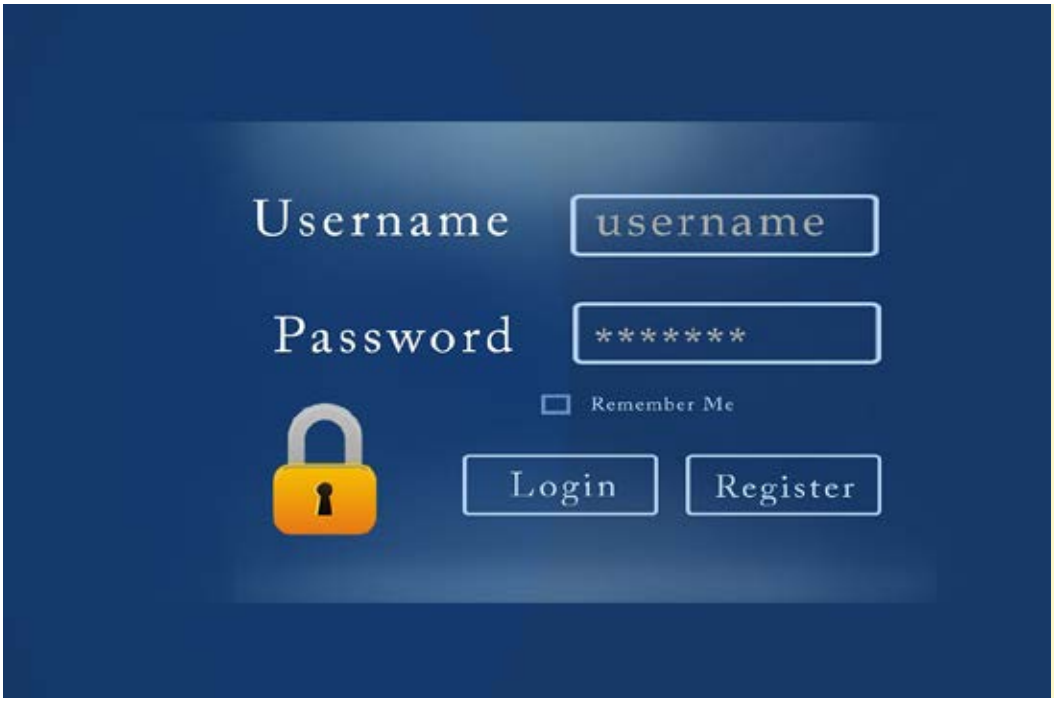
Massiv zugenommen hat die Zahl der Beratungen. Hier ergibt sich im Vergleich zu 2017 im Behördenbereich eine Steigerungsrate von 50 Prozent, im privaten Bereich sogar um 270 Prozent. In diesen Zahlen kommt deutlich die Unsicherheit im Umgang mit der neuen Rechtsordnung zum Ausdruck.

Vor allem kleine und mittlere Unternehmen und Vereine sowie im öffentlichen Bereich die Gemeinden waren dabei Hauptadressaten unserer Beratungstätigkeit.

HINWEISE ZUR MELDUNG VON DATENPANNEN

Auf unserer Webseite unter https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/ bieten wir **Verantwortlichen** die einfache Möglichkeit an, die Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO, umgangssprachlich „Datenpanne“ genannt, online vorzunehmen.

Bitte beachten Sie, dass nicht jede Verletzung des Schutzes personenbezogener Daten zu einer Meldepflicht nach Art. 33 DS-GVO führt. Entscheidend ist vor allem die Annahme, dass die Verletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erläuterungen hierzu und allgemein zur Meldepflicht mit anschaulichen Praxisbeispielen können Sie den Leitlinien des Europäischen Datenschutzausschusses entnehmen.



Top-Tipp: Passwort-Safe verwenden

Niemand kann sich hunderte Passwörter merken. Daher ist es sinnvoll, Passwörter in einem Passwort-Safe zu speichern. Entsprechende Programme wie KeePass(https://keepass.info/) gibt es als Freie- und Open-Source-Software kostenlos, bei einigen Betriebssystemen werden auch bereits welche mitgeliefert (z. B. der Schlüsselbund unter MacOS).

Viele Web-Browser unterstützen die Speicherung von Passwörtern – diese sollten aber mit einem Master-Passwort abgesichert werden.

Hinweise zum Umgang mit Passwörtern

Passwortsicherheit ist ein zentrales Thema bei technisch-organisatorischen Datenschutz-Maßnahmen. Passwörter sind immer noch ein zentrales Element zur Authentisierung von Nutzern, wie z.B. bei der Anmeldung bei einem Web-Dienst oder Computer. Aus diesem Grund bieten wir sowohl Nutzern eine Hilfestellung bei der Auswahl von sicheren Passwörtern als auch Diensteanbietern, Entwicklern und Administratoren Hinweise für die Aufstellung von Passwort-Richtlinien und die Speicherung von Passwörtern in Anwendungen.

Die Anmeldung mittels Nutzername und Passwort an Computern, bei Web-Diensten, Internet-of-Things- bzw. Smart-Home-Geräten und vielem anderen stellt das gängigste Verfahren zur Authentifizierung dar. Diese Authentifizierungsmethode ist damit oftmals das wesentliche oder gar einzige Sicherheitselement, das vor dem Zugriff durch Unbefugte schützt.

Es sind aber nicht nur Nutzer in der Pflicht, sichere Passwörter zu wählen. Administratoren und Hersteller müssen sichere Vorgaben machen, Passwörter sicher speichern und sollten moderne Techniken wie Zwei-Faktor-Authentifizierung anbieten.

Unsere Empfehlungen:

- *Starke Passwörter wählen*
- *Passwörter niemals doppelt verwenden*
- *Passwort-Safe verwenden*
- *Keine Wörter aus Wörterbüchern verwenden*
- *Passwörter nicht weitergeben*
- *Nur bei Kompromittierung ändern*
- *Sichere Passwörter auch auf Smartphones*
- *Standard-Passwörter immer ändern*
- *Lügen bei Sicherheitsfragen*
- *Zwei-Faktor-Authentifizierung aktivieren*
- *Zwei-Faktor-Authentifizierung aktivieren*

Die erster-Buchstabe-Methode

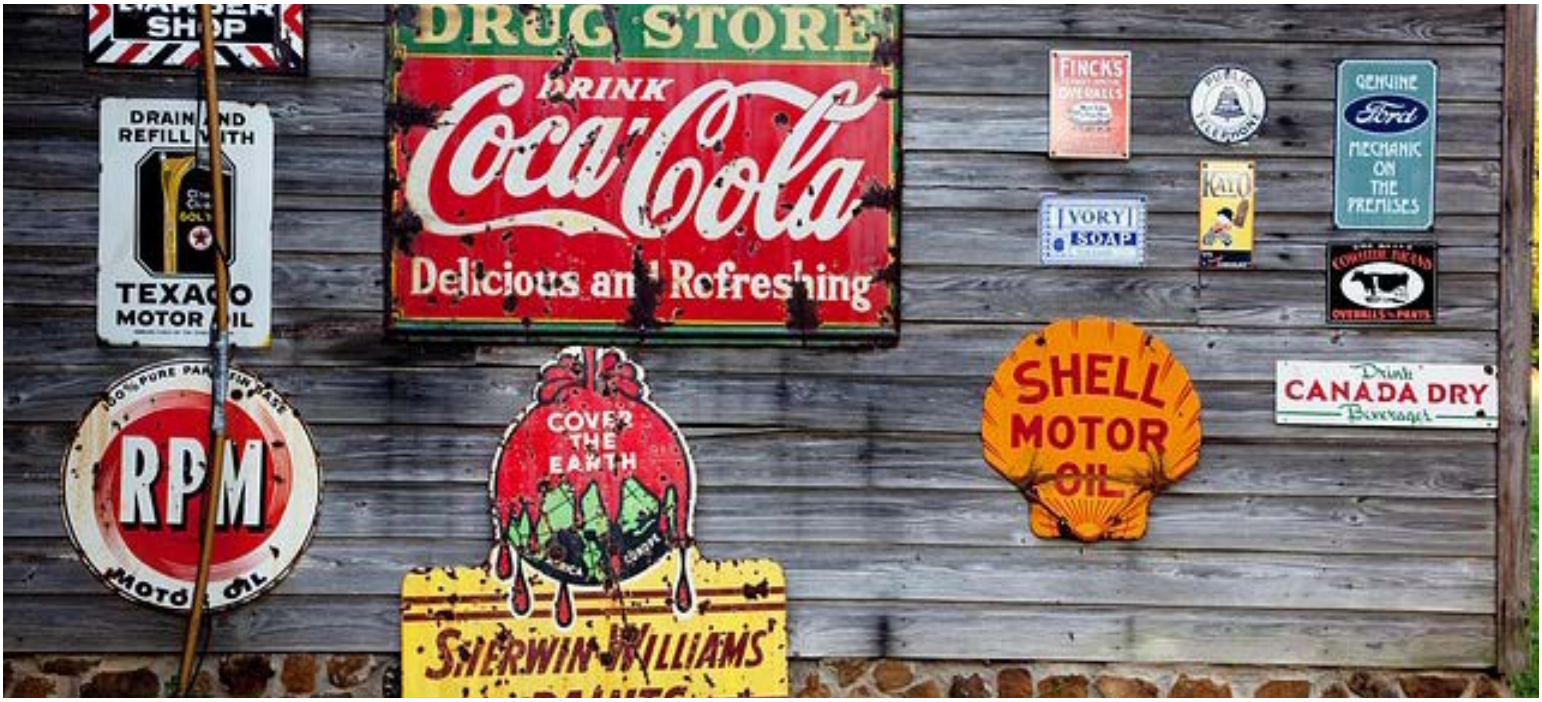
Denken Sie sich einen Satz aus, den Sie sich gut merken können und nehmen von jedem Wort den ersten oder einen markanten Buchstaben:

Ich muss mir selbst 1 tollen Satz ausdenken, das hier 1st nur eines von 42 Beispielen.

Das resultierende Passwort:
Imms1tSa,dh1nev42B.

Nehmen Sie aber keinen Satz, den jemand anderes erraten kann, der irgendetwas mit Ihnen oder Ihrem Umfeld zu tun hat. Wenn Sie als Satz einen bekannten Spruch, eine Liedzeile oder ein Gedicht nehmen, verfälschen Sie den Inhalt etwas.

Den vollständigen Beitrag zu diesem Thema können Sie hier abrufen:
https://www.baden-wuerttemberg.datenschutz.de/hinweise-zum-umgang-mit-passwoertern/



Was Sie gegen unerwünschte Werbung tun können

Datenschutzrechtlich relevant ist Werbung immer nur dann, wenn sich diese ausdrücklich mit Namen (evtl. auch mit Anschrift) oder E-Mail-Adresse an Sie richtet. Nicht persönlich adressierte Postwurfsendungen in Ihrem Briefkasten oder Beilagenwerbung in Ihrer Zeitung oder in einer Zeitschrift fallen daher **nicht** unter das Datenschutzrecht.

Was kann ich gegen Werbung per Briefpost tun?

Werbewiderspruch

Werbung per Briefpost ist im Regelfall auch ohne Ihre vorherige Einwilligung im Rahmen einer Abwägung nach Art. 6 Absatz 1 Satz 1 Buchstabe f der Datenschutz-Grundverordnung (DS-GVO) erlaubt. Sie haben aber stets das Recht, Werbung per Briefpost gegenüber dem werbenden Unternehmen mit Wirkung für die Zukunft zu widersprechen. Dieses Recht ist in Art. 21 Absatz 2 DS-GVO geregelt und umfasst auch den Widerspruch gegen Profiling.

Beispielformulierung für einen Werbewiderspruch:

Hiermit widerspreche ich gemäß Art. 21 Absatz 2 DS-GVO der Verarbeitung meiner Daten für Zwecke der Werbung sowie der Profilbildung und bitte daher um die sofortige Sperrung meiner Daten.

Ein ausführlicheres Muster finden Sie auf unserer Internetseite.

Wenn Sie der Werbung widersprochen haben, darf Ihnen das jeweilige Unternehmen keine Werbung mehr zusenden. Bereits gedruckte und/oder versendete Werbung ist allerdings noch für einen gewissen Zeitraum hinzunehmen.

Kommt das Unternehmen Ihrem Werbewiderspruch nicht nach, können Sie bei uns eine Beschwerde gegen das Unternehmen einlegen.

Eintragung in eine sog. „Robinsonliste“

Um Werbung per (Brief-)Post von vornherein zu begrenzen, können Sie Ihre Anschriftendaten in eine sog. Robinsonliste eintragen. Eine Robinsonliste ist eine Art Schutz- bzw. Sperrliste vor Werbung.

Der Eintrag ist auf der Internetseite www.ichhabediewahl.de/?cid=39 kostenlos möglich.

Eine andere Robinsonliste finden Sie im Internet.

Was kann ich gegen Werbung per Telefonanruf oder SMS/MMS tun?

Telefonwerbung (und Werbung per SMS/MMS) gegenüber Verbrauchern wird gesetzlich besonders restriktiv behandelt: Nur bei vorheriger ausdrücklicher Einwilligung in die entsprechende Datenerhebung und Nutzung zu Werbezwecken ist die Werbung am Telefon zulässig (§ 7 Absatz 2 Nr. 2 des Gesetzes gegen den unlauteren Wettbewerb, UWG). Dabei muss die Einwilligung vor dem Werbeanruf eingeholt werden.

Anrufe zu Zwecken der Markt- und Meinungsforschung sind zulässig, wenn tatsächlich ein entsprechendes „echtes“ Forschungsinstitut dahintersteht. Diese Anrufe zu Zwecken der Markt- und Meinungsforschung dürfen jedoch nicht mit der Einwilligung in Telefonwerbung verbunden werden. Kundenzufriedenheitsabfragen per Telefon ohne vorherige Einwilligung sind rechtswidrig. Wichtig: Bei unerwünschter Telefonwerbung immer sofort das Telefonat beenden und nicht in ein Gespräch verwickeln lassen!

Beschwerde bei der Bundesnetzagentur einlegen

Unzulässige Telefonwerbung wird von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (kurz: Bundesnetzagentur; im Internet: http://www.bundesnetzagentur.de verfolgt. Nutzen Sie daher bei Belästigungen durch Telefonanruf/SMS/MMS die Beschwerdemöglichkeiten der Bundesnetzagentur:

- *bei unerlaubter Telefonwerbung: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/UnerlaubteTelefonwerbung/unerlaubtetelefonwerbung-node.html*
- *bei Rufnummernmissbrauch: http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Verbraucher/ Rufnummernmissbrauch/rufnummernmissbrauch-node.html*

Beschwerde bei einem Verbraucherverband einreichen

Sie könnten sich an einen nach dem UWG klagebefugten Verband wenden, z.B. an die Verbraucherzentrale (beschwerdestelle@spam.vzbv.de), um eine Beschwerde wegen möglichen Verstoßes gegen § 7 Absatz 2 Nr. 2 (bei Anruf) oder Nr. 3 (bei Fax, E-Mail) UWG einzureichen.

Was kann ich gegen Werbung per E-Mail tun?

Werbung per E-Mail ist grundsätzlich immer rechtswidrig (unzumutbare Belästigung im Sinne von § 7 Absatz 1 und Absatz 2 Nummer 3 UWG), wenn Sie nicht vorher darin eingewilligt haben. Wichtig: Voraussetzung für eine datenschutzrechtliche Relevanz ist aber, dass die betroffene E-Mail-Adresse einen Personenbezug aufweist, also in der Regel zumindest vor oder nach dem @ einen Nachnamen enthält. E-Mail-Adressen wie poststelle@email-dienst.de, briefkasten@email-dienst.de oder maultasche@email-dienst.de sind nicht personenbezogen und auch nicht personenbeziehbar.
Allerdings gibt es im Hinblick auf das Einwilligungserfordernis bei E-Mail-Werbung eine wichtige Ausnahme: Nach § 7 Absatz 3 UWG ist E-Mail-Werbung an Bestandskunden auch ohne Ihre vorherige Einwilligung erlaubt, wenn der Werbende (also das Unternehmen) schriftlich alle nachfolgenden Voraussetzungen nachweisen kann:

- *Das werbende Unternehmen hat Ihre E-Mail-Adresse im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von Ihnen (als Kunden) erhalten (es muss also ein Vertrag zwischen Ihnen und dem werbenden Unternehmen geschlossen worden sein).*
- *Das werbende Unternehmen verwendet Ihre E-Mail-Adresse für Werbung für eigene ähnliche Waren oder Dienstleistungen,*
- *Sie haben der Verwendung Ihrer E-Mail-Adresse für Werbezwecke bislang nicht widersprochen und*
- *Sie wurden bei der Erhebung der E-Mail-Adresse und werden bei jeder EMail-Werbung klar und deutlich darauf hingewiesen, dass Sie der E-MailWerbung jederzeit widersprechen können, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen (in der Regel ist hiermit ein Abmeldelink in der Werbe-E-Mail gemeint).*

Gegen diese durch Gesetz privilegierte und erlaubte, einwilligungsfreie E-MailWerbung an Bestandskunden können Sie natürlich jederzeit gegenüber dem werbenden Unternehmen widersprechen (siehe oben Teil 1 Nr. 1). Sollte das werbende Unternehmen die oben genannten vier Voraussetzungen nicht einhalten, können Sie hiergegen bei uns eine Beschwerde einreichen.

Das vollständige Dokument
"Was Sie gegen unerwünschte Werbung tun können " können Sie hier abrufen:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/Merkblatt-LfDI-Was-Sie-gegen-unerwünschte-Werbung-tun-können-2-Aufl-Februar-2019.pdf

Das Kurzpapier der Datenschutzkonferenz "Verarbeitung personenbezogener Daten für Werbung" kann hier aufgerufen werden:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/07/DSK_KPNr_3_Werbung.pdf

Ihre Handlungsmöglichkeiten gegen unerlaubte E-Mail-Werbung sind:

1. Werbe-Mail als Spam markieren

Eine unerwünschte Werbe-E-Mail können Sie in fast jedem E-Mail-Programm als Spam markieren. Das Mailsystem merkt sich diese Markierung, so dass Sie vom selben Absender keine weitere E-Mail-Werbung mehr erhalten werden.

2. Beschwerde bei einem Verbraucherverband einreichen

Sie könnten sich an einen nach dem UWG klagebefugten Verband wenden, z.B. an die Verbraucherzentrale (beschwerdestelle@spam.vzbv.de), um eine Beschwerde wegen möglichen Verstoßes gegen § 7 Absatz 2 Nr. 2 (bei Anruf) oder Nr. 3 (bei Fax, E-Mail) UWG einzureichen.

3. Beschwerde bei der Datenschutzaufsichtsbehörde einreichen

Soweit eine Möglichkeit besteht, den Absender der Werbe-Mail herauszufinden, können Sie uns – möglichst online – eine Beschwerde zuschicken: https://www.badenwuerttemberg.datenschutz.de/online-beschwerde/

4. Beschwerde bei der Internet-Beschwerdestelle einreichen

Nutzen Sie die Möglichkeit, sich unter http://www.internetbeschwerdestelle.de/de/beschwerde/einreichen/e-mail-und-spam.html gegen den (in Deutschland sitzenden) Versender unerwünschter E-Mail-Werbung zu wenden.

Bitte beachten Sie, dass Sie bei E-Mail-Werbung neben dem Text der E-Mail möglichst auch den vollständigen E-Mail-Header (also mit allen sichtbaren und unsichtbaren E-Mail-Kopfzeilen, für Näheres siehe https://de.wikipedia.org/wiki/Header_(E-Mail)) vorlegen müssen, wenn Ihre Sache dort Erfolg versprechend bearbeitet werden soll.

Quelle Photo: erschienen in der Rhein-Neckar-Zeitung vom 6. Februar 2019, Photograph: Helmut Pfeifer

Datenschützer erobern die Schulen

Schulstunden der etwas anderen Art wurden im Februar 2019 durch die Mitarbeiterinnen und Mitarbeiter der Datenschutz-Aufsichtsbehörden in verschiedenen Bundesländern angeboten.

Es handelt sich hierbei nicht um ein redaktionelles Versehen – tatsächlich wurden im Rahmen einer gemeinsamen länderübergreifenden Aktion und in Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. Schülerinnen und Schüler mit dem Themengebiet Datenschutz vertraut gemacht.

Mit in Kraft treten der Europäischen Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 besteht mit Artikel 57 Absatz 1 lit. b DS-GVO ein gesetzlicher Auftrag, dem sich alle Datenschutzaufsichtsbehörden in ganz Europa stellen müssen.

Damit wird die Verpflichtung zum Schutz der Rechte von Kindern erstmalig in einer europaweit geltenden Rechtsgrundlage für Datenschutz explizit festgeschrieben.

Unabhängig von dieser gesetzlichen Forderung und diesem Novum in der Rechtslandschaft, kann der Schutz von Kindern und Jugendlichen gar nicht hoch genug angesiedelt werden, handelt es sich doch um die Schutzbedürfigsten in unserer Gesellschaft. Datenschutz bedeutet nicht nur Schutz der persönlichen Freiheit, sondern insbesondere auch Kinder- und Jugendschutz, so der Landesbeauftragte für Datenschutz von Baden-Württemberg, Dr. Stefan Brink. Als Vater ist ihm der Kinder- und Jugendschutz ein großes Anliegen. Besonderes Augenmerk legt er dabei darauf, nicht zu verbieten, sondern die Kinder und Jugendlichen stark zu machen, damit sie Risiken erkennen und so in die Lage versetzt werden, bewusst zu agieren und bewusst und gut informiert zu entscheiden.

Pünktlich zum Safer Internet Day bekam die Initiative „Datenschutz geht zur Schule“ des BvD damit tatkräftige Unterstützung von den Aufsichtsbehörden in Baden-Württemberg, Bayern, Niedersachen und Rheinland-Pfalz.

Es wurde deutlich, dass kostenfreie Angebote nachdrücklich zu hinterfragen sind. Ist der kostenlos angebotene Messengerdienst tatsächlich kostenlos? Aus welchem Grund bieten viele Unternehmen Kundenkarten und damit verbunden Rabatte und Treueprämien an?

Schnell wurde klar, dass in der heutigen Zeit kein Unternehmen etwas zu verschenken hat.
Überraschend deutlich wurde für die Dozentinnen und Dozenten, dass die „Datenkrake“ Facebook nahezu keine Bedeutung in dieser Altersklasse hat – Facebook nutzen nur die Erwachsenen, also meine Eltern oder meine Großeltern. Und wer will schon eine Freundschaftsanfrage seiner Tante – so das Feedback der Schülerinnen und Schüler.

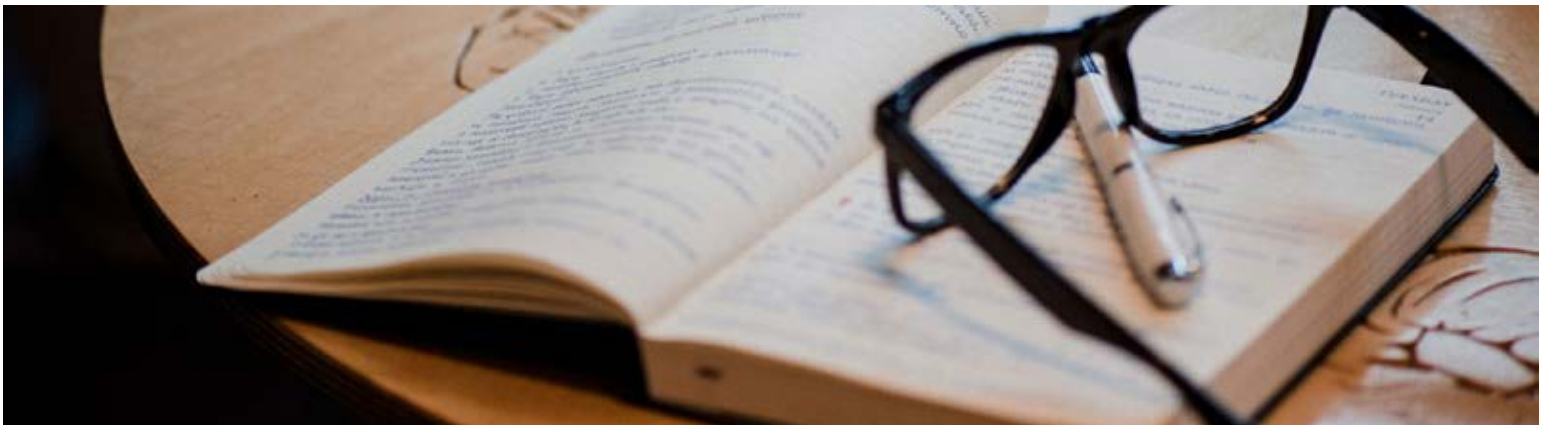
Die begeisterten Rückmeldung der Jugendlichen, der Lehrerinnen und Lehrern, der Schulleiterinnen und Schulleitern, der Dozentinnen und Dozenten der jeweiligen Aufsichtsbehörden sowie das Presseecho in den regionalen Tageszeitungen haben deutlich gemacht, wie wichtig und sinnvoll es ist, Kinder und Jugendliche im Umgang mit ihren personenbezogenen Daten im Internet zu sensibilisieren und, welche Herausforderung es auch darstellt, dieses Thema mit einem zielgruppengerechten Wortschatz zu erläutern.

Konkret wurden allein in Baden-Württemberg insgesamt rd. 600 Schüler und Schülerinnen in Stuttgart, Esslingen, Ditzingen, Walldorf, Bad Friedrichshall, Ludwigsburg, Ettlingen, Lorch und Pforzheim mit der gemeinsamen und länderübergreifenden Aktion der Aufsichtsbehörden in Kooperation mit dem BvD erreicht.
Deutlich wurde jedoch auch, dass der Bedarf an den Schulen viel, viel höher ist, als wir mit unserer Aktion befriedigen konnten.

Fazit unserer länderübergreifenden Aktion:
Wir werden weitermachen!

Weitere Informationen finden Sie unter:
https://www.bvdnet.de/datenschutz-geht-zur-schule/

Für Lehrkräfte:
www.bvdnet.de/datenschutz-geht-zur-schule



Weitere Informationsmaterialien

Betroffenenrechte

Schützen Sie Ihre Privatsphäre!

Wir leben in einer Welt, in der täglich Unmengen von Daten verarbeitet werden. Die Digitalisierung ist unser steter Begleiter. Bei nahezu jedem Kontakt, den Sie mit Unternehmen und anderen Organisationen haben, müssen Sie personenbezogene Daten wie Ihren Namen, Ihre Adresse und Ihr Geburtsdatum mitteilen. Auch online teilen Sie Ihre Daten, z.B. wenn Sie eine Website besuchen, im Internet surfen, etwas online einkaufen, soziale Medien nutzen oder dann, wenn Sie eine E-Mail senden.
Der Datenaustausch macht unser Leben einfacher, bequemer und verbundener.
Aber stets gilt: Ihre Daten sind und bleiben Ihre Daten.
Ihre Daten gehören zu Ihnen, und daher ist es wichtig, dass Ihre personenbezogenen Daten nur so verwendet werden, wie Sie es gestattet haben oder erwarten würden und dass der Datenaustausch in sicheren Bahnen verläuft. Unser Datenschutzrecht gewährleistet, dass alle personenbezogenen Daten ordnungsgemäß und rechtmäßig verwendet werden.

https://www.baden-wuerttemberg.datenschutz.de/betroffenenrechte/

Beschäftigtendatenschutz

Auch die 3. Auflage unseres praxisbezogenen Ratgebers spiegelt die interessante und vielfältige Arbeit aus dem Bereich des Beschäftigtendatenschutzes wider und präsentiert echte Fälle und deren Lösung.

https://www.baden-wuerttemberg.datenschutz.de/ratgeber-zum-beschaeftigtendatenschutz-3-auflage/

Einsatz von Bodycams durch private Sicherheitsunternehmen

Auch private Sicherheitsunternehmen rüsten ihre Beschäftigten mittlerweile mit Bodycams aus. Als Gründe führen sie z.B. Schutz der Beschäftigten vor Übergriffen, Beschaffung von Beweismitteln für zivilrechtliche Ansprüche oder eine abschreckende bzw. deeskalierende Wirkung an. Dem Einsatz von Bodycams stehen allerdings datenschutzrechtliche Bedenken entgegen.

https://www.baden-wuerttemberg.datenschutz.de/einsatz-von-bodycams-durch-private-sicherheitsunternehmen/

Videoüberwachung durch öffentliche Stellen

Grundsätzlich hat jeder Mensch das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mit einer Kamera beobachtet oder aufgezeichnet wird. Im Alltag ist Videoüberwachung dennoch weit verbreitet. Täglich greift diese Form der Datenverarbeitung in das Recht auf informationelle Selbstbestimmung ein, ohne dass die Mehrzahl der Überwachten dafür einen Anlass gegeben hat. Mit großer Streubreite wird aufgezeichnet, um welche Uhrzeit, an welchem Tag, in welchem Zustand, mit welchem Erscheinungsbild, wie lange und an welchem Ort sich ein Betroffener aufhält, wie er diesen Bereich nutzt, wie er sich dort verhält und ob er allein oder in Begleitung ist. Bereits eine einfache Überwachungsanlage verarbeitet in erheblichem Umfang personenbezogene Daten, ohne dass der Großteil der Informationen für den Überwachenden je eine Rolle spielt.

Filmt eine öffentliche Stelle eine Person, greift sie in deren Grundrecht auf informationelle Selbstbestimmung ein. Rechtmäßig kann dieser Eingriff nur erfolgen, wenn diese Datenverarbeitung die Voraussetzungen einer Rechtsgrundlage erfüllt.

https://www.baden-wuerttemberg.datenschutz.de/videoueberwachung-durch-oeffentliche-stellen/

Allerlei

Ein bunter Mix an Themen.

BEITRÄGE NACH THEMENGEBIETEN

Unter https://www.baden-wuerttemberg.datenschutz.de/beitraege-nach-themengebieten/ haben wir für Sie unsere Beiträge nach Themengebieten aufgeführt

TERMINE

16. Mai 2019, 19:30 Uhr
in Stuttgart
China – mehr als ‚Land des Lächelns'
Kiche St. Maria
Tübingerstraße 36

6. und 7. Juni 2019 in Stuttgart
IFG-Days
(Einladung folgt)

23. - 25. Oktober 2019 in Nürnberg
BvD-Herbstkonferenz zum Datenschutz "Wirtschaft trifft Aufsicht"
(Weitere Informationen zu gegebener Zeit)

KONTAKT

Landesbeauftrager für den Datenschutz
und die Informationsfreiheit
Baden-Württemberg
Königstraße 10 a
70173 Stuttgart

Telefon: 0711/61 55 41 – 0
Telefax: 0711/61 55 41 – 15

poststelle@lfdi.bwl.de

FRAGEN ZUM NEWSLETTER?

Scheiben Sie uns eine E-Mail an
pressestelle@lfdi.bwl.de

Brexit oder No-Brexit – das bleibt hier die Frage!

Zwar hat sich das britische Unterhaus für eine Vermeidung des kalten Brexit und gegen einen „No-Deal-Austritt" ausgesprochen. Dennoch bleibt der Ausgang des Ringens um den Brexit völlig unklar. Den LfDI erreichen täglich Nachfragen, ob grenzüberschreitende Datenverarbeitungen – mit britischen Geschäftspartnern oder Auftragsverarbeitern – bei einem kalten EU-Austritt des United Kingdom (UK) noch möglich bleiben.

Auf diese Frage findet sich die Antworten in der DS-GVO selbst: UK wäre im Fall des kalten Brexit als Drittstaat anzusehen – und zwar ohne jede Übergangs- oder Schonfrist. Als Rechtsgrundlage für die Übermittlung personenbezogener Daten sind dann die Vorgaben für den außereuropäischen internationalen Datenverkehr heranzuziehen.

Das Problem dabei: Die knappe verbleibende Zeit bis Ende März 2019 verhindert, dass alle durch die DS-GVO gebotenen Lösungsmöglichkeiten auch tatsächlich ausgeschöpft werden können. Ein viele Vorteile bringender Angemessenheitsbeschluss der Europäischen Kommission wird vor einem Brexit nicht mehr herbeizuführen sein. Dafür benötigt die Kommission eher zwei Jahre als zwei Monate. Langfristig wird sich der LfDI natürlich für die Einleitung eines solchen Verfahrens zur Prüfung der Angemessenheit des Datenschutzniveaus in Großbritannien einsetzen. Dies bringt nicht nur der Praxis mehr Vorteile und erspart Aufwände, sondern auch mehr Rechtssicherheit für grenzüberschreitende Datenverarbeitungsprozesse im Vereinigten Königreich. Ob die britischen Datenschutzregelungen den Anforderungen der EU zukünftig genügen, muss natürlich konsequent überprüft werden. Auch das wird kein Selbstläufer.

Jedoch verbleiben weitere Möglichkeiten, Datenverarbeitungen auch kurzfristig rechtmäßig durchzuführen. Die europäischen Aufsichtsbehörden bereiten dies bereits vor: So können Konzerne aufatmen, die bereits über sogenannte „Binding Corporate Rules" verfügen. Aber auch für alle anderen Unternehmen wird eine grenzüberschreitende Verarbeitung personenbezogener Daten mit Hilfe von sogenannten Standarddatenschutzklauseln möglich sein. Auch hier gilt aber: Erst genau prüfen, ob diese Mustertexte auf die konkrete Verarbeitungssituation passen und ob die Vertragsparteien alle dort aufgeführten Anforderungen tatsächlich erfüllen. Die Zeiten eines „simulierten" Datenschutzes sind vorbei, es herrscht die EU-DS-GVO!

Die britischen Kollegen informieren umfassend zu allen Fragen um den Brexit: Eine allgemeine Guideline zum „No-Deal-Brexit" findet sich auf der Internetseite der ICO. Diese wird ergänzt durch einen 6-Schritte-Plan, der um einen FAQ-Katalog[1] ergänzt wird.
Zudem wurde das Online-Tool zur Erstellung von Standarddatenschutzklauseln bereits auf den aktuellsten Stand gebracht, das Informationen über die Klauseln selbst und ihre Erstellung bereithält.
Wer sich zusätzlich noch weiter informieren will kann dies auf dem Blog der britischen Kollegen tun.
Auch schwierigste politische Situationen können so mit Hilfe der von der DS-GVO angebotenen Lösungen bewältigt werden. Der Rest ist Hoffen auf eine vernünftige Lösung …

Sämtliche Pressemitteilungen unserer Dienststelle finden Sie auf unsere Webseite unter
https://www.baden-wuerttemberg.datenschutz.de/pressemitteilungen/