Themenabend der Braunschweiger Linux-User-Group

Bundesdatenschutzgesetz
-
Neu

2019

Themenabend: Bundesdatenschutzgesetz-Neu Vorstellung

Ein Vortrag

von

Marius Schwarz

Themenabend: Bundesdatenschutzgesetz-Neu

Was macht das BDSG-NEU eigentlich?

Themenabend: Bundesdatenschutzgesetz-Neu

Die Europäische Datenschutzgrundverordnung

enthält Optionen zu nationalen Anpassungen.

Themenabend: Bundesdatenschutzgesetz-Neu

Das Bundesdatenschutz-Neu regelt

diese „Optionen“ für Deutschland.

Themenabend: Bundesdatenschutzgesetz-Neu

Das Bundesdatenschutz-Neu regelt

diese „Optionen“ für Deutschland.

… mit 89 Paragraphen 

Themenabend: Bundesdatenschutzgesetz-Neu

ACHTUNG:
KAUDERWELSCH

Themenabend: Bundesdatenschutzgesetz-Neu

Begriffklärung:

PBD = Personenbezogene Daten

„Besondere Kategorien“ = z.B. Medizinische Unterlagen, Versicherungsdaten, Kreditdaten, Strafakten

Themenabend: Bundesdatenschutzgesetz-Neu

Beispiel:

Artikel 32

Informationspflichten bei der Erhebung von PBD

bei der Person

Themenabend: Bundesdatenschutzgesetz-Neu

§ 32 Informationspflicht bei Erhebung von PBD bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck gemäß der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,

Themenabend: Bundesdatenschutzgesetz-Neu

Raten Sie mal wer da gemeint sein könnte ...

Themenabend: Bundesdatenschutzgesetz-Neu

Die Post

Themenabend: Bundesdatenschutzgesetz-Neu

genauer: Die Postkarte

Themenabend: Bundesdatenschutzgesetz-Neu

oder auch Unterschriftensammler in der Innenstadt.

Themenabend: Bundesdatenschutzgesetz-Neu

Artikel 1 - BDSG-NEU

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten .... es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Themenabend: Bundesdatenschutzgesetz-Neu

Artikel 2 – EU DS GVO
Sachlicher Anwendungsbereich

Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

...

c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

Themenabend: Bundesdatenschutzgesetz-Neu

Artikel 2 - Videoüberwachung

Falls Sie vorhaben Ihr Grundstück zu überwachen,
machen Sie offiziell einen öffentlichen Parkplatz mit eingeschränktem Zeitplanung daraus,
dann dürfen Sie zum Schutz von Leib und Leben mit Video überwachen.

Themenabend: Bundesdatenschutzgesetz-Neu

EU DSGVO Artikel 9

Verarbeitung besonderer Kategorien von PBD

BDSG-NEU Artikel 22

Themenabend: Bundesdatenschutzgesetz-Neu

Gesundheitswesen

Themenabend: Bundesdatenschutzgesetz-Neu

Erlaubt, …

b) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Absatz 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,

Themenabend: Bundesdatenschutzgesetz-Neu

EU DSGVO Artikel 9

Verarbeitung besonderer Kategorien von PBD
durch nichtöffentliche Stellen

BDSG-NEU Artikel 24

Themenabend: Bundesdatenschutzgesetz-Neu

§ 24 Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen ist zulässig, wenn

1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder

Themenabend: Bundesdatenschutzgesetz-Neu

Arbeitsverhältnis

Themenabend: Bundesdatenschutzgesetz-Neu

§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Themenabend: Bundesdatenschutzgesetz-Neu

Arbeitgeber dürfen also PBD der Arbeitnehmer speichern,

wenn ein

Tarifvertrag oder eine Betriebsvereinbarung

das benötigt oder vorsieht.

Themenabend: Bundesdatenschutzgesetz-Neu

Fangfrage: Tarifvertrag

Und wenn der Mitarbeiter gar nicht in der Gewerkschaft ist/war?

Themenabend: Bundesdatenschutzgesetz-Neu

Fangfrage: Betriebsvereinbarung

.. wenn der Zweck der Vereinbarung die Speicherung von Daten ist, und nicht die Folge des Zwecks der Vereinbarung ?

Themenabend: Bundesdatenschutzgesetz-Neu

§ 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) … Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Themenabend: Bundesdatenschutzgesetz-Neu

...Deutschland, Forschungsland...

Themenabend: Bundesdatenschutzgesetz-Neu

§ 27 Datenverarbeitung zu wissenschaftlichen … und zu statistischen Zwecken

(1) … die Verarbeitung besonderer Kategorien PBD im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche Forschungszwecke.

Themenabend: Bundesdatenschutzgesetz-Neu

§ 27 Datenverarbeitung zu wissenschaftlichen … und zu statistischen Zwecken

(2) Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die ***Auskunftserteilung*** einen unverhältnismäßigen Aufwand erfordern würde.

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

Wenn Sie Daten von Menschen verarbeiten wollen,

ohne das die was machen können,

gründen Sie ein Forschungsinstitut.

Themenabend: Bundesdatenschutzgesetz-Neu

Kreditwesen

Themenabend: Bundesdatenschutzgesetz-Neu

§ 30 Verbraucherkredite

(2) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 1 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 37 bleibt unberührt.

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

Bekommen Sie keine Auskunft,
wieso Ihr Kredit abgelehnt wurde,

sollten Sie sich fragen in welcher Terrorzelle Sie tätig sind,
ohne es zu wissen.

Themenabend: Bundesdatenschutzgesetz-Neu

§ 30 Verbraucherkredite

(1) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

Glückwunsch,
Ihre Kreditwürdigkeit wurde erfolgreich internationalisiert.

Themenabend: Bundesdatenschutzgesetz-Neu

…Artikel 31 oder WTF!…

Themenabend: Bundesdatenschutzgesetz-Neu

§ 31 Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften

(1) Die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur zulässig, wenn

1. die Vorschriften des Datenschutzrechts eingehalten wurden,

Themenabend: Bundesdatenschutzgesetz-Neu

d.h. es ist nur legal, wenn man sich an Gesetze hält.

Themenabend: Bundesdatenschutzgesetz-Neu

Wir sind verloren! :D

Themenabend: Bundesdatenschutzgesetz-Neu

Wenn wir in den USA leben würden, und ...

Themenabend: Bundesdatenschutzgesetz-Neu

§ 34 Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn

… oder
2. die Daten
…
b) **ausschließlich Zwecken der Datensicherung oder der Datenschutz-kontrolle dienen**

Themenabend: Bundesdatenschutzgesetz-Neu

Wer hat damit noch ein Problem?

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

„Was wir haben, behalten wir durch Umwidmung.“

Themenabend: Bundesdatenschutzgesetz-Neu

§ 35 Recht auf Löschung

Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht.

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

Wenn es zu schwer ist, die Daten wieder zu löschen,
dürfen Sie bleiben.

Themenabend: Bundesdatenschutzgesetz-Neu

Pro-Tipp

Keramikfliesen mit eingefrästen oder geätzten Inhalten sind sehr beliebt zur Langzeitdatenspeicherung in Höhlen und Berkwerken bis zu 30.000 Jahre Haltbarkeit (schätzt man).

Themenabend: Bundesdatenschutzgesetz-Neu

§ 37 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Das Recht gemäß Artikel 22 Absatz 1 der Verordnung (EU) 2016/679, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Artikel
22 Absatz 2 Buchstabe a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und

1. dem Begehren der betroffenen Person stattgegeben wurde

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

Wenn die Personen bekommen hat, was sie wollte,
darf sie nicht protestieren.

Themenabend: Bundesdatenschutzgesetz-Neu

Meint

Wenn die Personen bekommen hat, was sie wollte,
darf sie nicht protestieren!

Warum sollte sie auch?

Themenabend: Bundesdatenschutzgesetz-Neu

§ 42 Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder

2. auf andere Art und Weise zugänglich macht

und hierbei **gewerbsmäßig** handelt.

Themenabend: Bundesdatenschutzgesetz-Neu

§ 42 Strafvorschriften

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt,
sich oder einen anderen zu bereichern oder einen Anderen zu schädigen.

Themenabend: Bundesdatenschutzgesetz-Neu

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Themenabend: Bundesdatenschutzgesetz-Neu

§ 44 Klagen gegen den Verantwortlichen oder Auftragsverarbeiter

(1) Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person können bei dem Gericht des Ortes erhoben werden, an dem sich eine Niederlassung des Verantwortlichen oder Auftragsverarbeiters befindet. Klagen nach Satz 1 können auch bei dem Gericht des Ortes erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat.

Themenabend: Bundesdatenschutzgesetz-Neu

§ 38 Datenschutzbeauftragte nichtöffentlicher Stellen

Wenn mindestens 10 Personen mit der ständigen Verarbeitung von PBD beschäftigt sind oder

Sie mit Daten hantieren, die eine hohe Wahrscheinlichkeit beinhalten die Rechte und Freiheiten von Personen zu gefährden oder

Sie geschäftsmäßig Daten übermitteln.

Themenabend: Bundesdatenschutzgesetz-Neu

zum Abschluss

Themenabend: Bundesdatenschutzgesetz-Neu

§ 64 Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, …

...ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

Themenabend: Bundesdatenschutzgesetz-Neu

„Für die Bundesverwaltung hat das BSI einen Mindeststandard zum Einsatz von TLS entwickelt, der für die Stellen des Bundes verbindlich umzusetzen ist:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll_node.html

Dieser Mindeststandard referenziert die technische Richtlinie TR-02102-2 und fordert für die Bundesverwaltung den Einsatz von TLS 1.2 mit PFS.“

Quelle: Anfrage an das BSI Februar 2018

Themenabend: Bundesdatenschutzgesetz-Neu

```
[000.106]       Connected to server
[000.292]  <-- 220 ESMTP
[000.293]   --> EHLO www6.CheckTLS.com
[000.399]  <-- 250-newsletter.bund.de
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250 DSN
[000.399]       TLS is not an option on this server
[000.400]   --> MAIL FROM:<test@checktls.com>
[000.506]  <-- 250 2.1.0 Ok
[000.506]       Sender is OK
[000.506]   --> QUIT
[000.612]  <-- 221 2.0.0 Bye
```

Quelle: Test vom 13. März 2019

Themenabend: Bundesdatenschutzgesetz-Neu

Danke für Ihre Aufmerksamkeit