

Datenschutz & Compliance

Newsletter für den Datenschutz



SaphirIT

DATENSCHUTZ · COMPLIANCE

Ausgabe Juni 2021 | Seite 229 - 233

INHALT

SEITE 229

Fragebogen der Aufsichtsbehörden zur Umsetzung des Schrems II – Urteils

SEITE 231

Neue Cookie Regelung in Sicht? Überblick zum TTDSG

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Juni 2021.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Fragebogen der Aufsichtsbehörden zur Umsetzung des Schrems II - Urteils

Verzeichnis von Verarbeitungstätigkeiten steht im Fokus

In unserem letzten Sondernewsletter von diesem Monat haben wir Sie darauf hingewiesen, dass verschiedene Aufsichtsbehörden in Deutschland sich zusammengeschlossen haben und die Umsetzung des Schrems II - Urteils mittels Fragebögen überprüfen werden.

Die Fragebögen liegen uns inzwischen vor.

Daraus geht unter anderem hervor, dass die Aufsichtsbehörden bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten eine zweckgebundene kleinteilige Aufteilung der Verfahren fordern.

So fordern die Aufsichtsbehörden beispielsweise für die datenverarbeitenden Prozesse **Bewerberportale, Konzerninterner Daten-**

verkehr, Mailhoster, Tracking und Webhoster eigene Verfahren.

Dieses Verständnis der Aufsichtsbehörden ist sehr weitreichend und geht über das hinaus, was wir bisher für erforderlich hielten.

Legt man diese Auffassung zu Grunde müssten im Unternehmen alle Datenverarbeitungsprozesse erneut dahingehend analysiert werden, ob eine kleinteiligere Darstellung im Verzeichnis von Verarbeitungstätigkeiten möglich bzw. notwendig ist. Eine Verarbeitungsbeschreibung „Homepage“ reicht danach nicht aus.

In der Literatur wird dagegen teilweise eine andere Auffassung vertreten. Diese geht eher davon aus, dass viele Verarbeitungsvorgänge durchaus zusammengefasst werden können.

So beispielsweise diese beiden Auffassungen:

„Wegen einer zu uferlosen Ausweitung entgegen dem Wortlaut der Legaldefinition unter „jeden (...) Vorgang“ [sind] nicht sämtliche Tätigkeiten zu verstehen, die dann in dem Verzeichnis zu erfassen sind (Wächter, Datenschutz Unternehmen, 5. Aufl. 2017, B Datenschutzkontrolle 363). Dieses Verständnis ist zu kleinteilig [...]“ (BeckOK DatenschutzR/Spoerr, 36. Ed. 1.5.2021 Rn. 6, DS-GVO Art. 30 Rn. 6).

„Der Pflichtige darf mehrere Verarbeitungen in einem Verarbeitungsverzeichnis bündeln. Das

deutet auch Abs. 1 S. 1 lit. b an: Er lässt es in der Sache zu, dass die Verarbeitung mehrere Zwecke verfolgen kann („die Zwecke der Verarbeitung“). Das impliziert, dass das Verarbeitungsverzeichnis unterschiedliche Zweckrichtungen erfassen kann. Alles andere wäre für Verantwortliche und Auftragsverarbeiter auch wenig praktikabel.“ (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 30 Rn. 5).

Rechtsprechung liegt zu dieser Frage noch nicht vor.

Auch wenn die Frage daher noch nicht einheitlich beantwortet ist, empfiehlt es sich die Auffassung der Aufsichtsbehörde nicht zu ignorieren. Sie sollten daher Ihre bisherigen Verarbeitungsbeschreibungen dahingehend prüfen, ob diese nicht mehrere datenverarbeitende Prozesse enthalten. Dienen diese dann mehreren Zwecken wäre zu entscheiden, ob insoweit nicht eine Aufspaltung in mehrere Verarbeitungsbeschreibungen erfolgen sollte. Bei mehreren Prozessen mit gemeinsamem Zweck oder auch ähnlichen Datenarten käme noch am ehesten eine Verbindung in einer Verarbeitungsbeschreibung in Betracht.

Die bislang in Ihren Verarbeitungsbeschreibungen noch nicht enthaltenen Datenverarbeitungsprozesse, wären entsprechend zu behandeln. Sprechen Sie uns hierzu gerne an.

Neue Cookie Regelung in Sicht?

Überblick zum TTDSG

Der Datenschutz-Aktivist Max Schrems hat mit seiner gemeinnützigen Datenschutz-Organisation „noyb“ die größte Beschwerdewelle seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) gestartet.

Die Organisation überprüft mittels einer eigens entwickelten Software Cookie-Banner. Findet die Software einen rechtswidrigen Cookie-Banner, so werden automatisch Beschwerden generiert und an die betroffenen Unternehmen versandt.

Schrems führt hierzu aus: *„Nach der DSGVO müssen Nutzer:innen eine simple Ja/Nein-Option haben. Da die meisten Banner diesen Anforderungen nicht entsprechen, hat noyb eine Software entwickelt, die verschiedene Arten von rechtswidrigen Cookie-Bannern erkennt und automatisch Beschwerden generiert.“*

Unternehmen haben nach Erhalt der Beschwerde einen Monat Zeit ihre Banner den gesetzlichen Anforderungen anzupassen. Im Falle des Unterbleibens einer Anpassung will noyb die Beschwerden an die Aufsichtsbehörden weiterleiten.

Ziel von noyb ist es die größten europäischen Webseiten zu überprüfen und bis zu 10.000 Beschwerden zu generieren.

Die Organisation teilt mit, eine erste Überprüfung habe ergeben, dass 81 % der Cookie-Banner nicht einmal einen „Ablehnen-Button“ enthielten. Bei 73 % der Webseiten würden irreführende Farben und Kontraste verwendet.

Schrems führt hierzu aus: *„Nur 3 % aller Nutzer wollen die Cookies tatsächlich akzeptieren, aber mehr als 90 % können dazu verleitet werden, auf den Akzeptieren Button zu klicken.“*

Möglicherweise hat der Cookie Wahnsinn aber bald ein Ende. noyb veröffentlichte zusammen mit dem Sustainable Computing Lab („CSL“) der Wirtschaftsuniversität Wien einen Vorschlag für ein automatisches Browser Signal, welches das Ende der Cookie-Banner bedeuten könnte. Es handelt sich um das sog. Advanced Data Protection Control („ADPC“)

Es geht um einheitliche und simple Pop-up Fenster, wo alle Daten zur Verarbeitung freigegeben werden können oder eben nicht.

Schrems erklärt den Vorschlag wie folgt:

„ADPC erlaubt intelligentes Management von Datenschutzanfragen. Ein Nutzer könnte etwa sagen, ‚bitte frage mich erst, wenn ich auf der Seite mehrmals war‘ oder ‚frage mich nach 3 Monaten wieder‘. Ebenso ist es möglich, gleichartige Anfragen zentral zu beantworten. ADPC ermöglicht, die Flut von Datenanfragen sinnvoll zu managen.“

Rechtsgrundlage vom Bundestag geschaffen?

Der Bundestag hat am 20.05.2021 das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) verabschiedet.

Dieses könnte als Grundlage für ein mögliches Verfahren, wie es *noyb* fordert, dienen.

Das TTDSG führt die bereichsspezifischen Datenschutzregeln aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) in einem Gesetz zusammen und aktualisiert diese.

§ 25 TTDSG regelt nun ausdrücklich die Vorgaben des Art. 5 Abs. 3 ePrivacy-Richtlinie, mit deren Umsetzung der Bundesgerichtshof sich in seinem Cookie-Einwilligung II - Urteil beschäftigt hatte (BGH, Urteil vom 28. Mai 2020 - I ZR 7/16).

§ 26 TTDSG gibt der Bundesregierung die Möglichkeit Rechtsverordnungen zu erlassen, die die Anforderungen an technische Anwendungen zur Einbindung und Verwaltung der Cookie-Einwilligung sowie die Akkreditierungsvoraussetzungen derer Anbieter festlegen.

Unter diese Definition könnten z.B. auch Personal Information Management Systeme (PIMS) oder Single-Sign-on-Lösungen fallen.

PIMS sind „Systeme, die natürlichen Personen mehr Kontrolle über ihre personenbezogenen

Daten geben sollen. Mittels PIMS haben Menschen die Möglichkeit, ihre personenbezogenen Daten in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wann und mit wem sie es wünschen. Anbieter von Onlinediensten und Werbetreibende werden mit den PIMS interagieren müssen, wenn sie beabsichtigen, die Daten natürlicher Personen zu verarbeiten. Dadurch können ein am Menschen orientierter Ansatz in Bezug auf personenbezogene Informationen und auch neue Geschäftsmodelle entstehen.“ (https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de)

Je nachdem wie die technischen Anforderungen ausfallen ist es denkbar, dass PIMS auf die vom *noyb* veröffentlichten Spezifikationen des ADPC aufbaut.

Auf ein Problem weist jedoch der Sachverständige zum Entwurf des TTDSG in seiner Stellungnahme hin.

„Zunächst ist fraglich, ob und wie PIMS-Anbieter überhaupt die Anforderungen an eine wirksame Einwilligung erfüllen können. Art. 4 Nr. 11 DSGVO und Art. 7 DSGVO stellen an eine wirksame Einwilligung eine Vielzahl von Anforderungen, darunter „für den bestimmten Fall“, „in informierter Weise“ und „in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“. Aus Erwägungsgrund 32 DSGVO folgt außerdem, dass Pauschaleinwilligungen unwirksam sind. [...] Dieses Problem kann nur dadurch überwunden werden, dass der Gesetzgeber selbst regelt,

dass (bzw. unter welchen Bedingungen) eine PIMS-gestützte Einwilligung immer wirksam sein soll – und zwar unabhängig von der Frage, ob die Anforderungen der DSGVO im Einzelfall erfüllt sind oder nicht. Dies wäre jedoch eine Abweichung von Anforderungen der DSGVO bzw. ePrivacy-RL. Da diese Rechtsakte zum Recht der EU gehören, kann dies nur der EU-Gesetzgeber erreichen.“ (Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), BT-Drucksache 19/27441).

Wie sich die Sache in Zukunft entwickeln wird ist zum jetzigen Zeitpunkt noch nicht abzusehen.

Es besteht aber jedenfalls die Möglichkeit, dass PIMS die in Kritik stehenden Cookie Banner in Zukunft ablösen wird.

Zumindest das ständige Einwilligen und die Unklarheit auf Seiten der Webseitenbetreiber wäre damit behoben.

Es bleibt jedoch abzuwarten, ob die Behörden eine solche Einwilligung nach PIMS als wirksam im Sinne der DSGVO ansehen werden.

Gerne sehen wir Ihre Cookie-Banner an und prüfen, ob diese den derzeitigen rechtlichen Rahmenbedingungen entsprechen.

Falls Sie unseren Newsletter in Zukunft nicht mehr erhalten möchten, schicken Sie bitte eine kurze E-Mail an info@saphirit.de

SaphirIT GmbH
Sutthausen Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de



Unsere jeweils aktuellen Datenschutzinformationen finden Sie unter
<https://www.saphirit.de/datenschutz.html>