FRT CONSULT GMBH
IT Dienstleistungen & Business Dienstleistungen

frtpartner

Telefon: 09221 / 900 - 0
Telefax: 09221 / 900 - 111
Kontakt: info@frtconsult.de
Adresse: Kurt-Schumacher-Str. 23
95326 Kulmbach

Datenschutz-Newsletter IV / 2019

Aktuelles rund um den Datenschutz

14,5 Millionen Euro Bußgeld wegen Verstöße gegen die DSGVO

Das Immobilienunternehmen Deutsche Wohnen SE hat laut einer Mitteilung des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 05. November 2019 für die Speicherung personenbezogener Daten von Mietern ein System zur Archivierung verwendet, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu löschen. Eine Prüfung der Zulässigkeit und Erforderlichkeit erfolgte dabei nicht.

Die Aufsichtsbehörde stellte diese Verstöße bereits im Jahr 2017 fest und wies die Gesellschaft auf diese Missstände hin. Auch in einem erneuten Prüftermin mehr als 1,5 Jahre später konnte die rechtmäßige Verarbeitung der personenbezogenen Daten nicht sichergestellt werden.

Daraufhin erließ die Behörde einen Bußgeldbescheid in Höhe von 14,5 Millionen Euro wegen Verstößen gegen Art. 5, 25 Abs. 1 DSGVO.

Die Entscheidung ist nicht rechtskräftig. Die Gesellschaft hat in einer Pressemitteilung vom 05. November 2019 angekündigt, den Bescheid gerichtlich überprüfen zu lassen.

Der Aufbau eines Datenschutzkonzeptes ist wesentlich günstiger!

Konzept zur Bußgeldzumessung

Um für die Bußgeldbemessung wie beispielsweise die oben genannte eine nachvollziehbare, faire und einzelfallgerechte Lösung zu finden, haben die Datenschutzaufsichtsbehörden des Bundes und der Länder ein Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen erlassen.

Demgemäß erfolgt die Bußgeldzumessung in fünf Schritten:

1. Zuordnung des Unternehmens zu einer Größenklasse, die sich am Vorjahresumsatz orientiert;
2. Bestimmung einer Untergruppe anhand des mittleren Jahresumsatzes;
3. Festlegung des wirtschaftlichen Grundwerts, indem der mittlere Jahresumsatz der Untergruppe durch 360 Tage geteilt wird;
4. Multiplikation des Grundwerts mit einem Faktor, der sich am Schweregrad der Tat orientiert und
5. Anpassung des Betrags anhand aller für und gegen den Betroffenen sprechenden Umstände.

Durch dieses Berechnungsmodell, das für alle deutschen Behörden verbindlich ist, können die Bußgeldrahmen der DSGVO ausgeschöpft werden, was für Unternehmen zu großen wirtschaftlichen Risiken führen

kann, wenn sie sich nicht DSGVO-konform verhalten.

Google Analytics auf Unternehmenswebsites

Die Aufsichtsbehörden mehrerer Bundesländer sind mit einer Beschwerdeflut konfrontiert.

Hintergrund ist der nicht datenschutzkonforme Einsatz von Google Analytics auf Unternehmenswebsites. Die Beschwerden umfassen über 200.000 Anwender.

Google Analytics ist das derzeit populärste Webanalyse-Tool weltweit.

Der kostenlose Dienst von Google kann für seine Nutzer die statistische Auswertung ihrer Seite übernehmen und untersucht unter anderem die Herkunft der Besucher, ihre Verweildauer auf einzelnen Seiten, und Bereiche, in denen der Benutzer am meisten klickt. Damit ist es Google möglich, ein umfassendes Benutzerprofil von Besuchern einer Webseite zu erzeugen.

Datenschutzrechtlich ist das Tool schon lange umstritten.

Best-Practice-Lösung beim Einsatz von Google Analytics war bis jetzt die aktive IP-Anonymisierung und die Möglichkeit eines Opt-Outs (Widerspruchsmöglichkeit).

Der Einsatz von Tracking erfolgte aufgrund der berechtigten Interessen der Websitebetreiber gem. Art. 6 Abs. 1 lit. f DSGVO.

Der Europäische Gerichtshof (EuGH) hat in der Rechtssache Planet49 (Adresshändler und Gewinnspielbetreiber) entschieden, dass das Setzen von Cookies, die nicht unbedingt erforderlich sind, der aktiven Einwilligung des Internetnutzers bedarf. Dies gilt unabhängig davon, ob es sich bei den abgerufenen Informationen um personenbezogene Daten handelt oder nicht.

Ein Tracking ohne vorherige Einwilligung der Nutzer wird in Zukunft nicht mehr hingenommen werden.

Eine Überprüfung der Unternehmenswebsites sollte ins Auge gefasst werden.

Windows 10 und der Datenschutz

Mit einem Prüfschema der Datenschutzkonferenz (DSK) sollen Verantwortliche, die Windows 10 einsetzen oder dies in Zukunft beabsichtigen, in die Lage versetzt werden, eigenständig die Einhaltung der rechtlichen Vorgaben der DSGVO in ihrem konkreten Fall zu prüfen.

Unter anderem weist das Prüfungsschema darauf hin, dass die Frage der Rechtmäßigkeit einer Übertragung von personenbezogenen Daten in ein Drittland wie die USA, sich nach der 2-Stufen-Prüfung richtet.

Durch das allgemeine Verbot mit Erlaubnisvorbehalt benötigt das Übermitteln der Telemetriedaten auf der ersten Stufe eine Rechtsgrundlage. Einer solchen bedarf es dann nicht, wenn der Verantwortliche durch technische Maßnahmen die Datenübermittlung an Microsoft bereits unterbunden hat und diese angemessen im Sinne des Art. 25 DSGVO ist.

Nach diversen Gutachten sind nur netzwerkbasierte Maßnahmen über den Umweg, die direkte Internetverbindung von Windows 10 Systemen zu unterbinden und den Internetzugang über eine Virtualisierungs- oder Terminallösung erfolgen zu lassen, erfolgsversprechend.

Alle Verantwortlichen, denen diese Maßnahme nicht möglich ist, müssen nach einer Rechtsgrundlage suchen.

Die Telemetriedaten von Windows 10 werden verschlüsselt an Microsoft versendet. Dem Verantwortlichen ist es daher kaum möglich, an die Information zu kommen, ob und welche personenbezogenen Daten bei der Übertragung von Diagnosedaten an Microsoft fließen.

Unabhängig davon ergeben sich Probleme mit dem Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO.

Dieser verlangt, dass die Verarbeitung personenbezogener Daten auf ein für die Zwecke der Verarbeitung notwendiges Maß beschränkt werden. Die Diagnosedaten werden aber nach eigenen Angaben von Microsoft für eine ganze Reihe von Funktionen verwendet, welche nach Ansicht der DSK über reine Betriebssystemfunktionalitäten hinausgehen.

Fazit:

Wollen Verantwortliche Windows 10 datenschutzkonform innerhalb Ihres Unternehmens nutzen, muss entweder die Übermittlung von jeglichen Telemetriedaten an Microsoft unterbunden werden oder der Verantwortliche muss mit Microsoft eine individuelle Lösung aushandeln.

Andernfalls bleibt nur noch der Umstieg auf ein anderes Betriebssystem.

Pflicht zur Benennung eines Datenschutzbeauftragten ab 20 Mitarbeiter

Der Bundestag hat mit Zustimmung des Bundesrats im Rahmen des zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (2. DSAnpUG-EU) vom 20.11.2019 eine Änderung des § 28 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) beschlossen.

Ein Datenschutzbeauftragter ist demnach dann zu bestellen, wenn der Verantwortliche oder der Auftragsverarbeiter in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Dabei ist allein die Kopfzahl entscheidend.

Unabhängig davon kann sich die Pflicht zur Bestellung eines Datenschutzbeauftragten auch aus § 38 Abs. 1 S. 2 BDSG oder Art. 37 Abs. 1 DSGVO ergeben (unter anderem bei Datenschutzfolgenabschätzungen, Kerntätigkeit Durchführung von Verarbeitungsvorgängen mit umfangreicher regelmäßiger Überwachung von betroffenen Personen, umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten).

Trotz der Anhebung der Grenze von zehn auf 20 Personen bleibt zu beachten, dass die Verantwortlichen an die Regelungen der DSGVO gebunden sind und auch angesichts der gestiegenen Bußgelder auf fachliche Expertise nicht verzichten sollten.

Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

Thomas Hesz, RA/StB; Marcel Peetz (B.Sc.), StB; Maria Gayer, RAin; Stefan Gräbe
Zertifizierte Datenschutzbeauftragte (TÜV)
Telefon: 09221 / 900 - 0
info@frtpartner.de
www.frtpartner.de