UIMCommunic@tion

04/2019

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

DSGVO längst nicht überall umgesetzt

Seit dem 25. Mai 2018 wird die EU-Datenschutz-Grundverordnung angewandt. Ein knappes Jahr mit der DSGVO liegt somit hinter allen Beteiligten. Grund genug zu schauen, was sich verändert hat, ob tatsächlich hohe Strafen verhängt wurden und ob die Regeln innerhalb und außerhalb der EU zu mehr Datenschutz in Unternehmen geführt haben. „Mit der DSGVO gilt erstmals in der EU ein unmittelbar anwendbares europäisches Datenschutzrecht. Die europaweite rechtliche Harmonisierung ist vor dem Hintergrund globaler Verarbeitung personenbezogener Daten ein datenschutzrechtlicher Quantensprung", unterstreicht der erfahrene Datenschutzfachmann Dr. Jörn Voßbein von der UIMC.

Die DSGVO hat nicht nur die öffentliche Verwaltung und private Wirtschaft beschäftigt, sondern ist mit der allgemeinen Diskussion schon fast in den alltäglichen Sprachgebrauch eingegangen. Die Betrachtung konkreter Entwicklungen liefert die Belege:

Seit Anwendungsbeginn der DSGVO hat sich die Anzahl von Beschwerden und Anfragen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) stark erhöht. Im Jahre 2017 und den ersten fünf Monaten des Jahres 2018 erreichten den Bundesbeauftragten durchschnittlich ca. 400 Beschwerden und Anfragen pro Monat. In den Monaten Juni bis Dezember 2018 stieg diese Zahl rasant auf etwa 1370 pro Monat an. Schwerpunkte bei den Bürgereingaben bildeten die Betroffenenrechte auf Datenauskunft und Datenlöschung. Auch der Datenschutzbeauftragte des Landes Nordrhein-Westfalen konnte nach Inkrafttreten der DSGVO keinen Arbeitsmangel feststellen: 12.000 schriftliche Anfragen im Jahr 2018 und dazu rund 140 Anrufe pro Tag.

Es steht außer Frage: Die DSGVO war für in der EU tätige Unternehmen ein entscheidender Wendepunkt im Umgang mit Daten. Sie hat die Messlatte für die Datenerfassung und verarbeitung gegenüber der vorhergehenden Datenschutzrichtlinie angehoben und große, mittelständische und kleine Unternehmen gleichermaßen an ein einheitliches Regelwerk gebunden. Die Stichworte Auftragsverarbeitung, Informationspflichten, Risikobewertung und Datenschutz-Folgenabschätzung sowie die Meldung von Datenpannen sollten spätestens seit Mai 2018 in jedem Unternehmen präsent sein.

„Leider müssen wir immer wieder erfahren, dass es immer noch Behörden und Unternehmen gibt, die mit der Umsetzung der DSGVO nicht einmal begonnen haben" berichtet Dr. Voßbein aus seinen Erlebnissen, der dafür kein Verständnis hat: „Eine derart weitreichende Einführung neuer Regeln führt naturgemäß auch zu Unsicherheiten, aber zu Untätigkeit darf sie nicht führen."

Auf einen Verstoß gegen die Regelungen der DSGVO sollte man es nicht ankommen lassen. Denn auch die Höhe der Strafen wurde mit der DSGVO massiv nach oben verändert. Wo zuvor das deutsche BDSG einen maximalen Bußgeldbetrag von 300.000 Euro vorgesehen hatte, gilt nun ein Maximalbetrag von 20 Millionen Euro, beziehungsweise von 4 % des weltweiten Jahresumsatzes. Bußgelder wurden von den Behörden schon verhängt, wenn auch nicht in jener Höhe wie zunächst befürchtet. Laut einem Bericht des Europäischen Datenschutzausschusses (EDPB – European Data Protection Board) lässt sich die Gesamtsumme auf 56 Mio. Euro beziffern. Sie relativiert sich, wenn man erfährt, dass das größte Bußgeld von der französischen Datenschutzbehörde CNIL mit 50 Mio. Euro gegen den Internetgiganten Google verhängt wurde. Eine Abmahnwelle, wie im Mai 2018 noch befürchtet und danach oftmals herbeigeschrieben, hat es allerdings nicht gegeben. „Was man jedoch nicht vergessen darf", so ergänzt Datenschutzfachmann Dr. Heiko Haaz, „dass auch die Aufsichtsbehörden sich erst richtig ‚aufstellen' und Personal aufbauen mussten. Somit ist in den nächsten Jahren mit einer höheren Kontrolldichte und intensiveren Bußgeldern zu rechnen."

Die DSGVO führte aber auch zu einer Menge Stilblüten: Von der sehr öffentlichkeitswirksamen Posse um die Klingelschilder bei der Wiener Wohnen über Ärzte, dessen Wartezimmertüren „aufgrund der DSGVO" nun geschlossen bleiben mussten bis hin zu vermeintlich erforderlichen Einwilligungserklärungen für weitere Datenverarbeitung (obwohl ein gülter Vertrag mit dem Betroffenen vorliegt). Ferner schien vielerorts die Auffassung vertreten worden zu sein, dass für jede Datenübermittlung an einen Vertragspartner ein Vertrag zur Auftragsverarbeitung erforderlich ist. Hierbei hat sich aber (größtenteils auch inhaltlich) gegenüber der vorherigen Rechtsauffassung nichts geändert.

Des Weiteren versuchten Trittbrettfahrer wie z. B. von der „Datenschutzauskunfts-Zentrale" die Verunsicherung von Unternehmen auszunutzen. Auch wenn die Rechte der Betroffenen durch die DSGVO etwas modifiziert wurden, so waren diese Rechte auch in vorherigen Gesetzen enthalten und sind nicht gänzlich neu. Dennoch gilt: Ein Betroffener hat nicht nur das Recht, Auskunft über die über ihn verarbeiteten Daten zu verlangen, sondern auch eine Kopie dieser Daten zu erhalten. Auch sind Daten dann zu löschen, wenn der Zweck für die Datenverarbeitung entfällt (beispielsweise nach Vertragskündigung und den steuerrechtlichen Aufbewahrungspflichten).

Bis zum 25. Mai 2020 soll ein Bericht über die Bewertung und Überprüfung der Verordnung vorgelegt werden. Für Unternehmen bedeutet dies aber nicht, noch ein Jahr zu warten. „Ich bin zwar passionierter Teetrinker, doch würde ich keinem Unternehmer empfehlen, dies mit Abwarten zu kombinieren", ergänzt Dr. Voßbein mit einem Schmunzeln.

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

DSGVO
Was (noch) zu tun ist?!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Informationspflichten

Werden personenbezogene Daten bei der betroffenen Person erhoben, so sind der betroffenen Person die in den Artikeln 13 DSGVO genannten Informationen zum Zeitpunkt der Datenerhebung mitzuteilen. Werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, so sind diese und weitere Informationen innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats, mitzuteilen.

Hierzu finden Sie viele **Mustertexte** zu verschiedenen Betroffenengruppen (Beschäftigte, Kunden etc.) unter **www.Online-Formular-Center.**

Auftragsverarbeitung

Eine Auftragsverarbeitung ist die Inanspruchnahme von externen Dienstleistungsfunktionen durch den Verantwortlichen. Hierbei ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Um zu gewährleisten, dass eine Auftragsverarbeitung nur entsprechend den Weisungen des Unternehmens erfolgt, ist der Abschluss eines Vertrags zwischen Auftraggeber und Auftrag-nehmer notwendig.

Sowohl einen **Selbstauskunftsbogen** (Prüfung der Eignung) als auch verschiedene **Musterverträge** finden Sie unter www.Online-Formular-Center.eu.

Meldepflichten bei Datenpannen

Im Falle einer Datenschutzverletzung ist die Verletzung unverzüglich (d. h. „ohne schuldhaftes Zögern“) – möglichst aber binnen 72 Stunden – der zuständigen Aufsichtsbehörde mitzuteilen. Erfolgt die Meldung nicht innerhalb von 72 Stunden, so ist der Mitteilung außerdem eine Begründung für die Verzögerung beizufügen.

Hierbei ist es zunächst unerheblich, ob der Vorfall intern oder extern stattgefunden hat. Zur Beurteilung, ob ein meldepflichtiger Tatbestand vorliegt, sind sowohl Geschäftsführung als auch der Datenschutzbeauftragte einzubinden.

Einen exemplarischen Prozess nebst **Meldeformularen** und **Checklisten** zur Beurteilung finden Sie unter www.Online-Formular-Center.eu.

Risikobewertung / Datenschutzfolgenabschätzung

Es ist eine Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen durchzuführen. Hierzu sollte das **Verzeichnis von Verarbeitungstätigkeiten** (VvV) ausgefüllt und darauf aufbauend eine Risikobewertung (ggf. unterstützt durch den Datenschutzbeauftragten vorgenommen werden.

Sofern das Ergebnis dieser Risikobewertung ist, dass voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, so muss vor der Inbetriebnahme des Systems vorab eine **Datenschutz-Folgenabschätzung** durchgeführt werden. Unterlagen zum VvV und Risikobewertung finden Sie unter www.Online-Formular-Center.eu.

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ DSGVO längst nicht überall umgesetzt
- ☐ DSGVO: Was ist noch zu tun?
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 946 7726 9200 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: https://communication.UIMC.de

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.