UIMCommunic@tion

11/2019

Ausgabe für Deutschland

*Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert*

## Wie stelle ich ein „berechtigtes Interesse“ fest?

Nicht erst seit der Einführung der DSGVO kann eine rechtmäßige Verarbeitung von personenbezogenen Daten rechtmäßig sein, soweit sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.“ Die DSGVO verlangt ein „berechtigtes Interesse“ für die Verarbeitung personenbezogener Daten. Die Schwierigkeit dieser Begrifflichkeit liegt auf der Hand: Wo fängt „berechtigtes Interesse“ an und wo hört es auf? Was ist überhaupt ein „berechtigtes Interesse“? Wie muss eine Interessenabwägung vorgenommen werden? „Eine sorgfältige Prüfung ist unerlässlich, um datenschutzkonform zu handeln“, meint Datenschutzfachmann Dr. Heiko Haaz und ergänzt: „Und jeder Fall muss individuell betrachtet werden.“

Eine Interessenabwägung ist kein Hexenwerk, aber es gilt einige Grundregeln zu beachten. „Die Hinzuziehung von Hilfskriterien kann die Prüfung in Stufe drei erleichtern. Grundsätzlich ist es zwar so, dass das berechtigte Interesse weit zugunsten des Unternehmens zu interpretieren ist“, erläutert UIMC-Partner Dr. Haaz unter Zugrundelegen der Erwägungsgründe. Doch kann die „Waage“ bei der Interessensabwägung durch die Stufe 3 wieder dazu führen, dass eine Datenverarbeitung nicht zulässig ist.

Eine ausführliche Darstellung finden Sie unter https://www.uimc.de/kommunikation/uimcommunication/

## Zweistellige Millionenstrafen jetzt auch in Deutschland realistisch – Vor- & Nachteile des neuen Bußgeldbemessungsmodells

Die deutschen Datenschutzbehörden haben sich auf ein Modell zur Berechnung von Bußgeldern geeinigt. Damit wird die Bemessung von Bußgeldern nach der DSGVO künftig auf eine neue Grundlage gestellt. Das Modell sieht eine einheitliche und vorhersehbare Berechnung von Bußgeldern bei Verstößen gegen die EU-Datenschutz-Grundverordnung vor. „Das Modell sorgt für mehr Klarheit, Transparenz und Nachvollziehbarkeit. Für Unternehmen wird ein Risikomanagement möglich, aber auch notwendig“, sagt Datenschutzexperte Dr. Voßbein, der die deutschlandweite Regelung für Unternehmen und die Anliegen des Datenschutzes zwar positiv wertet, „aber die Strafhöhe weiterhin mit ‚Augenmaß‘ festgelegt werden sollte“. Denn bisher blieben deutsche Unternehmen und Vereine bei Sanktionen aufgrund von Datenschutzverstößen im weltweiten Vergleich weitestgehend verschont. Im Vergleich zu Ländern wie Frankreich, Großbritannien oder den USA waren die Strafgeldzahlungen in Deutschland von geringer Natur. Damit wird es nun vorbei sein. Aber nicht nur deshalb lohnt eine genaue Betrachtung des verabredeten Modells.

„Der Aufbau und die Sicherstellung einer gut funktionierenden Datenschutzorganisation und des Datenschutzmanagementsystems sind zur Verringerung des Bußgeldrisikos unerlässlich“, rät UIMC-Geschäftsführer Dr. Jörn Voßbein zum Handeln. Mit dem neuen Rechenmodell könnten zweistellige Millionenbeträge auch bald in Deutschland verhängt werden. Das neue Bußgeldmodell ist bereits jetzt durch die nationalen Datenschutzbehörden verbindlich anzuwenden. Europaweit wird noch an einem einheitlichen Bußgeldkatalog gearbeitet. Die deutschen Behörden engagieren sich sehr dafür, die nationalen Maßstäbe europaweit zur Anwendung zu bringen. Hier muss die weitere Entwicklung abgewartet werden.

Eine ausführliche Darstellung finden Sie unter https://www.uimc.de/kommunikation/uimcommunication/

## FAQ: Ausführliche Praxishilfe zur Interessensabwägung

Wie oben dargestellt, ist eine Interessensabwägung keine triviale Fragestellung. Daher haben wir eine ausführliche Praxishilfe erstellt, in der auch drei verschiedene Beispiele ausführlich dargestellt werden. Diese finden in unserem eCollege-Kurs „FAQ“: https://www.uimcollege.de > Meine Kurse.

Dieser Kurs ist im **neuen eCollege** für alle User freigeschaltet, die einen Account zu einem Schulungskurs haben. Sie haben noch keinen Zugang? Dann informieren Sie sich unter https://www.uimc.de/seminareschulungen/ecollege.



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

**Noch Fragen?**
Treten Sie mit uns in einen Dialog ein!

# UIMCommunic@tion

*Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert*

## Risikoschwelle für Meldepflichtigkeit von Datenpannen

*Sind alle Datenpannen zu melden? Wo ist die Schwelle für Datenschutzverletzungen, die nur zu einem „geringen Risiko" führen und daher nicht meldepflichtig sind?*

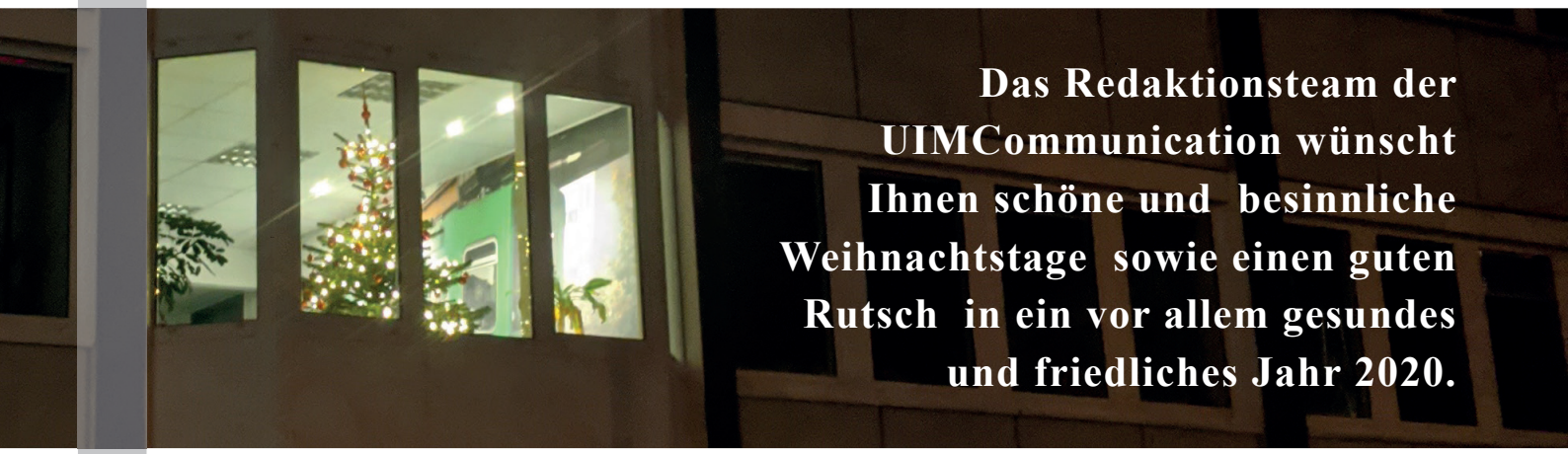
Der Risikobegriff bereitet hier Schwierigkeiten. Die DSGVO kennt nur Risiko und hohes Risiko. Im Kurzpapier 18 der Datenschutzkonferenz wird ausgeführt, dass die Formulierung „nicht zu einem Risiko" in Artikel 33 DS-GVO als „nur zu einem geringen Risiko" gelesen werden kann. **Einen völligen Ausschluss von Risiko gibt es nicht.**

Man muss nicht alles melden. Es ist eine Abwägung zwischen der Schwere des Schadens und der Wahrscheinlichkeit des Schadenseintritts vorzunehmen. Generell gilt: Wenn man feststellt, dass ein mehr als geringes Risiko besteht, dann sollte man melden. Selbst wenn sich das Risiko nicht realisiert hat und der zum Risiko führende Zustand behoben wurde, so ist dennoch zu melden, wenn ein Risiko bestanden hat. Stellt man fest, dass ein hohes Risiko bestanden hat, so ist der Vorfall der Aufsichtsbehörde zu melden und die Betroffenen sind zu informieren. Hierzu ein Beispiel.

» Ein Laptop mit medizinischen Befunden wird einem Arzt entwendet. Die Daten auf der Festplatte des Laptops sind mit einem kryptographischen Verfahren nach dem Stand der Technik sicher verschlüsselt und alle gespeicherten Daten sind in einem Backup vorhanden.

» Eine Offenbarung der auf dem Laptop gespeicherten Befunde würde für die betroffenen Patienten einen hohen Schaden bedeuten. Allerdings ist davon auszugehen, dass der Schadenseintritt höchst unwahrscheinlich ist, wenn die Befunde sicher verschlüsselt sind. Ein Schaden durch den Verlust kann ausgeschlossen werden, da die Daten im Backup weiterhin verfügbar sind. In diesem Falle ist keine Meldung erforderlich.

» Der Datenschutzvorfall und die Ergebnisse seiner Risikoanalyse sind jedoch intern zu dokumentieren und die entsprechenden Maßnahmen zu ergreifen, um einen solchen Vorfall zukünftig zu vermeiden.




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

☐ Vor- & Nachteile des neuen Bußgeldbemessungsmodells

☐ Praxishilfe zur Interessensabwägung

☐ **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.