veröffentlicht von **Dr. Sebastian Kraska**

Datenschutz-Grundverordnung: Desaster oder Grund zu feiern?

Eine Bestandsaufnahme im Interview mit Rechtsanwalt und Diplom-Kaufmann Dr. Sebastian Kraska, Gründer und Geschäftsführer der **IITR Datenschutz GmbH**.

Die DSGVO gilt seit bald drei Jahren. Ist die DSGVO aus Ihrer Sicht ein Erfolg?

Das hängt stark von den Erwartungen ab, die man persönlich mit der Einführung der DSGVO verbunden hat. Persönlich würde ich ein gemischtes Fazit ziehen. Das Bewusstsein bei den Unternehmen ist gewachsen, dass diese sich um die Grundthemen datenschutzrechtlicher Vorgaben kümmern müssen. Auch die Erwartung der Kunden an funktionierende Datenschutz-Prozesse ist gestiegen. Zugleich hat die DSGVO konstruktive Mängel, welche die Handhabe gerade bei datengestützten Geschäftsmodellen erschweren.

So ringen wir zum Beispiel in der Praxis immer noch mit ganz unterschiedlichen **Vorstellungen bei der Anonymisierung von Daten**. Und auch im Bereich der Erforschung Künstlicher Intelligenz wäre es durch eine **alternative Ausgestaltung der Erlaubnistatbestände** möglich gewesen, moderne Informationsgesellschaft und Datenschutz **besser miteinander zu verbinden**.

Worauf sollten Unternehmer in der Praxis achten?

Es gilt nach wie vor die Empfehlung, das **"Kleine 1x1"** des Datenschutzes zu adressieren. Die DSGVO hat eine Reihe von Basis-Themen geschaffen, welche Unternehmen unbedingt befolgen sollten und bei deren Nichtbefolgung auch von Seiten der Aufsichtsbehörden wenig Nachsicht zu erwarten ist. Diese Basis-Themen sind:

- Schaffung einer Datenschutzrichtlinie oder eines Datenschutzhandbuches
- Dokumentation der Kern-Systeme im Verzeichnis der Verarbeitungstätigkeiten
- Verträge mit Dritt-Dienstleistern an die Datenverarbeitungsvorgänge ausgelagert werden
- Einhaltung von Mindest-Standards im Bereich Informationssicherheit
- Webseiten-Datenschutzerklärung und Betroffeneninformation
- Bestellung Datenschutzbeauftragter und Meldung bei der Aufsichtsbehörde
- Schulung von Beschäftigten
- Prozess zur Durchführung einer Datenschutz-Folgenabschätzung
- Beachtung der 72-Stunden-Melde-Frist im Datenverlustfall
- Strukturierte Beantwortung von Betroffenen-Anfragen (Auskunft, Löschung etc.)

Zu beachten ist auch, dass Unternehmen unter der DSGVO verpflichtet sind, die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen zu können (so genannte "Rechenschaftspflicht" aus Art. 5 DSGVO). Wie weit diese im Detail geht [ist umstritten]8https://rsw.beck.de/rsw/upload/ZD/ZD_01-2018_-_Beitrag_Veil_1.pdf) - die Aufsichtsbehörden zumindest leiten daraus eine Art "faktischer Beweislastumkehr" zu Lasten der Unternehmen ab.

Wie können Sie Unternehmen bei den DSGVO-Anforderungen helfen?

Wir bieten verschiedene Möglichkeiten, Unternehmen unterschiedlicher Größe und variierendem Datenschutz-Niveau zu unterstützen:

- **Datenschutz-Kit**: kleinere Unternehmen bis 40 Beschäftigte unterstützen wir mit dem preisgerechten Datenschutz-Kit. Neben der Bestellung des Datenschutzbeauftragten stellen wir den Unternehmen auch eine Datenschutz-Plattform zur Verfügung. Unter unserer Anleitung können Unternehmen hier die datenschutzrechtlichen Anforderungen weitestgehend in Eigenleistung erbringen. Vertiefende Fragen können individuell geklärt werden. eLearning für die Beschäftigten und regelmäßige Webinare runden das Angebot ab.
- **Datenschutz-Management-System "Compliance-Kit 2.0" für den Mittelstand**: orientiert an der ISO-Norm für Datenschutz-Management-Systeme (ISO27701) bietet wir ein Datenschutz-Management-System zum Einsatz durch interne Datenschutz-Abteilungen und andere externe Datenschutzbeauftragte.
- **Externer Datenschutzbeauftragter für den Mittelstand**: bei Bedarf unterstützen wir auch

mittelständische Unternehmen als externer Datenschutzbeauftragter und implementieren dort Prozesse zur Erfüllung der datenschutzrechtlichen Vorgaben.

- **eLearning für Datenschutz und Informationssicherheit**: mehr als 250.000 Schulungen zu den Themen Datenschutz und Informationssicherheit wurden bereits über unsere eLearning-Plattform durchgeführt, mit deren Hilfe die Beschäftigten in der Breite zu den Grundanforderungen des Datenschutzes sensibilisiert werden können.
- **Audit-Plattform PSE für den Datenschutz**: mit Hilfe unserer webbasierten Audit-Plattform PSE (Privacy Status Evaluation) kann mit vertretbarem Aufwand der Datenschutz-Status in Unternehmen messbar gemacht werden.

Steht der Datenschutz der Bekämpfung der Pandemie im Weg?

In der Politik und der öffentlichen Diskussion **mehren sich die Stimmen**, dass der zu strenge Datenschutz der erfolgreichen Pandemie-Bekämpfung im Wege stünde. Die Aufsichtsbehörden - insbesondere der Bundesbeauftragte für Datenschutz und Informationsfreiheit Herr Professor Kelber - tritt dem regelmäßig **mit guten Argumenten** entgegen . Welche Verbreitung würde eine App finden, die Kontakt-Daten individualisierbar auf einem zentralen System speichern würde? Würden wir dann auch konsequenterweise in Kauf nehmen, **zur Installation der App und dem Mitführen des Smartphones** verpflichtet zu werden?

Auch das Teilen von Gesundheitsdaten mit Impfstoff-Herstellern würde nicht am Datenschutz scheitern: nach Einschätzung von Professor Dr. Petri , Bayerischer Landesbeauftragter für Datenschutz, unterscheidet sich z.B. die israelische Gesetzeslage zur Datennutzung durch Krankenversicherungen und Forschungsdatenzentren nicht sehr von der deutschen. "Manchen hierzulande erscheine aber der technische und organisatorische Aufwand für die Datennutzung zu hoch und so schöben sie den Verzicht darauf gerne auf den Datenschutz."

Und wenn die **Benachrichtigung für Impf-Termine** angeblich am Datenschutz scheitert und eine Live-Übertragungen einer **Pressekonferenz des Robert-Koch-Instituts** untersagt wird so bleibt festzuhalten: dies liegt nicht am Datenschutz, sondern einer **nicht zielführenden Auslegung** der datenschutzrechtlichen Vorgaben.

Wie blicken Sie auf die aufsichtsrechtliche Landschaft in Deutschland?

Länder und Bund diskutieren weiter eine mögliche **Zentralisierung der Datenschutz-Aufsichtsbehörden** für den Unternehmensbereich im Bund. Während der Bund eine volle Zentralisierung der aufsichtsrechtlichen Strukturen zu favorisieren scheint würden einige der Länder eher eine stärkere Formalisierung der internen Abstimmungen in der Datenschutz-Konferenz bevorzugen.

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit richtet seinen Blick dabei nicht nur nach Deutschland, sondern auch nach Brüssel: so hat Professor Kelber kurz nach seiner Amtseinführung eine **Harmonisierung der Aufsichtsbehörden auf europäischer Ebene** gefordert, um insbesondere den großen Tech-Firmen ein aus seiner Sicht adäquates Gegengewicht bei der Datenschutz-Aufsicht gegenüber stellen zu können

Viele Unternehmen haben 2020 ihre Beschäftigten ins Home-Office geschickt. Welche datenschutzrechtlichen Aspekte spielen in dem Zusammenhang eine Rolle?

Der plötzliche Wechsel ins Home-Office im März 2020 hat gezeigt, welche Unternehmen ihre IT-Infrastruktur im Griff hatten. Mit etwas Abstand betrachtet sollten Unternehmen insbesondere folgende Aspekte adressieren:

- Sämtliche Geräte im Home-Office sollten verschlüsselt sein
- Alle datenhaltenden Systeme sind mit Multi-Faktor-Authentifizierung abzusichern
- Die Beschäftigten sind gesondert auf die Einhaltung datenschutzrechtlicher Anforderungen im Home-Office zu schulen sowie zu verpflichten.

Es war erwartet worden, dass 2020 das Jahr der Datenschutz-Bußgelder wird. Hat sich diese Erwartung eingestellt?

In 2018 und 2019 haben die Aufsichtsbehörden nach der Einführung der DSGVO vor allem auf Informationsangebote für Unternehmen gesetzt. Und so war die allgemeine Erwartung, dass das Jahr 2020 in der Breite für die auch streitige Durchsetzung datenschutzrechtlicher Vorgaben genutzt werden würde. Nachvollziehbarer Weise haben die Aufsichtsbehörden hier aber aufgrund der Pandemie Augenmaß walten lassen. Dennoch sind in 2020 die **Bußgelder in der Summe bereits auf Rekordhöhen** gestiegen. Für 2021 ist weiter zu erwarten, dass die Aufsichtsbehörden gerade in den von der Pandemie nicht stark betroffenen Industrie-Zweigen ihre Bußgeld-Praxis fortsetzen werden.

Im Sommer 2020 erging ein Urteil des Europäischen Gerichtshofs, nach dem Datentransfers gerade mit den USA kritisch zu sehen sind. Wo steht die Diskussion hier?

Der Europäische Gerichtshof hat das so genannte "Privacy Shield" aufgrund der **Zugriffsmöglichkeiten der US-Behörden gekippt**, nach Maßgabe dessen europäische Unternehmen vereinfacht Daten mit US-Unternehmen teilen durften. Auch wenn formal noch andere Transfer-Alternativen bestehen stellt sich damit die Frage, ob und unter welchen Voraussetzungen Unternehmen aus der EU noch Daten an US-Anbieter (insb. im Cloud- und Telekommunikations-Bereich) übermitteln dürfen. Die europäischen Aufsichtsbehörden befinden sich hier noch in der internen Abstimmung. Die deutschen Aufsichtsbehörden werden in Kürze beginnen, erste **Fragebögen dazu an Unternehmen zu verschicken**. Die Hoffnungen der Industrie richten sich derzeit darauf, dass die EU und die USA ein **Nachfolgekonstrukt in 2021** finden werden.

Das ganze Internet scheint mittlerweile mit Einwilligungsbannern überzogen. Muss das so sein?

Nein, das ist in der Form nicht erforderlich. Es ist **wichtig zu verstehen**: wer nur die Basis-Daten wie Benutzerzahlen und Regionen auswerten möchte kann dies auch weiterhin mit entsprechend datenschutzfreundlichen Tracking-Tools ohne Einwilligung vornehmen. Die meisten Webseiten könnte man daher aus meiner Sicht (wie auch in **unserem Video-Beitrag dargestellt**) wieder von den Bannern befreien.

Die Aufsichtsbehörden haben die Schaffung datenschutzkonformen Webseiten-Trackings Ende 2019 auf die Agenda gesetzt und dies auch durzusetzen begonnen. In der Folge haben die meisten Unternehmen ihr Webseiten-Angebot in 2020 umgestaltet und häufig übereilt auf Werkzeuge zur Einwilligungsabfrage umgeschaltet.

Nur wenn man auf profilbildende oder individualisierte Tracking-Maßnahmen setzt, muss eine Einwilligung eingeholt werden. Hier hat sich der Streit zwischen Aufsichtsbehörden und Unternehmen von der Frage des "ob" auf das "wie" verlagert. Wenn in 2019 noch umstritten war, ob man überhaupt eine Einwilligungslösung benötigt ist nun häufig in Frage, wie das Einwilligungstool zu konfigurieren ist (so zum Beispiel die Frage, ob ein Knopf "Ablehnen" auf derselben Ebene wir der Knopf "Zustimmen" stehen muss).

Auch auf deutscher wie auf europäischer legislativer Ebene wird das Thema diskutiert: so sieht der nun unter portugiesischer Ratspräsidentschaft ins Rennen geschickte Entwurf der ePrivacy-Verordnung weitgehende Möglichkeiten vor, auch ohne Einwilligung profilbildendes Tracking zu ermöglichen. Der nun im Trilog mit dem Europäischen Parlament und der Europäischen Kommission abzustimmende Vorschlag wurde von **Datenschützern entsprechend kritisiert** - ebenso wie die **noch nicht erfolgte Anpassung** von Telekommunikations- und Telemediengesetz an die Vorgaben der DSGVO.

Der Bereich des Webseiten-Tracking und seiner datenschutzkonformen Ausgestaltung bleibt also auch weiterhin im Detail umstritten.

Veröffentlicht von:
Dr. Sebastian Kraska
Rechtsanwalt