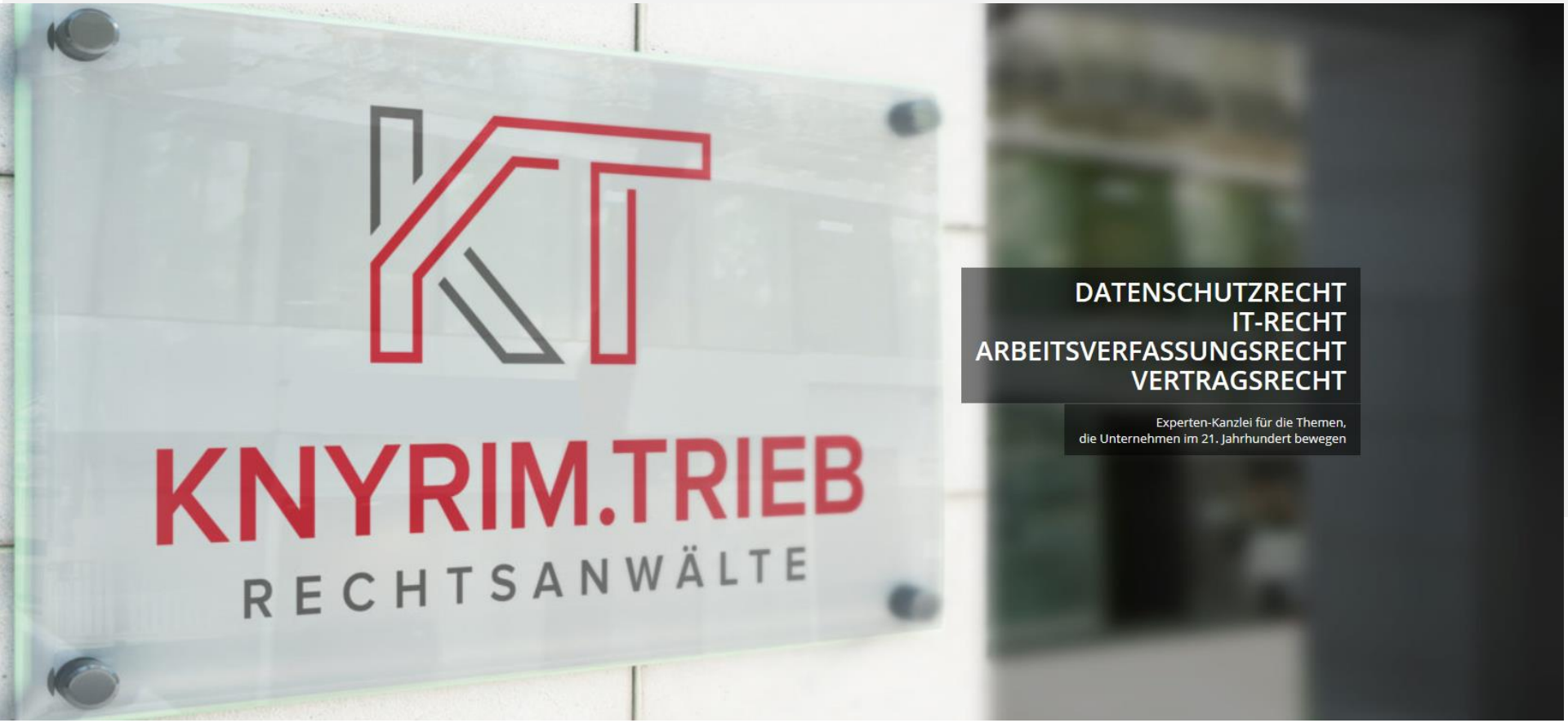
KNYRIM.TRIEB
RECHTSANWÄLTE



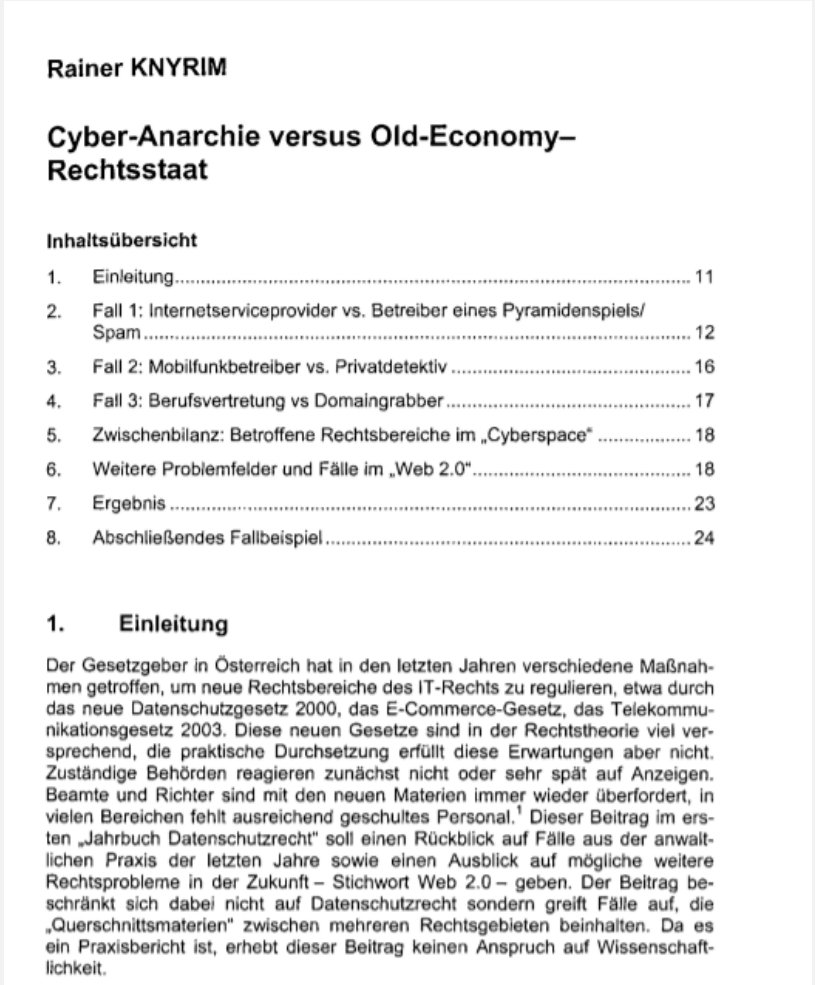

KNYRIM.TRIEB
RECHTSANWÄLTE
Willkommen
Da
Anfrage
Sehr geehrte Interessenten!
Leider müssen wir Ihnen mitteilen, dass wir bis Juni 2018 mit Projekten zur Datenschutz-Grundverordnung so ausgelastet sind, dass wir keine Anfragen neuer Mandanten mehr übernehmen können. Diesbezügliche Anfragen bleiben aus Zeitgründen unbeantwortet.
Wir bitten um Verständnis!
Knyrim Trieb Rechtsanwälte

DSGVO

Privacy Peak
Wie die Gipfel
im Datenschutzrecht
immer unbezwingbarer werden

RA Dr. Rainer Knyrim
Knyrim Trieb Rechtsanwälte Wien
IT-Rechtstag 2018

Cyber-Probleme Anno 2008…



Rainer KNYRIM

Cyber-Anarchie versus Old-Economy– Rechtsstaat

Inhaltsübersicht

1. Einleitung

Der Gesetzgeber in Österreich hat in den letzten Jahren verschiedene Maßnahmen getroffen, um neue Rechtsbereiche des IT-Rechts zu regulieren, etwa durch das neue Datenschutzgesetz 2000, das E-Commerce-Gesetz, das Telekommunikationsgesetz 2003. Diese neuen Gesetze sind in der Rechtstheorie viel versprechend, die praktische Durchsetzung erfüllt diese Erwartungen aber nicht. Zuständige Behörden reagieren zunächst nicht oder sehr spät auf Anzeigen. Beamte und Richter sind mit den neuen Materien immer wieder überfordert, in vielen Bereichen fehlt ausreichend geschultes Personal.[1] Dieser Beitrag im ersten „Jahrbuch Datenschutzrecht" soll einen Rückblick auf Fälle aus der anwaltlichen Praxis der letzten Jahre sowie einen Ausblick auf mögliche weitere Rechtsprobleme in der Zukunft – Stichwort Web 2.0 – geben. Der Beitrag beschränkt sich dabei nicht auf Datenschutzrecht sondern greift Fälle auf, die „Querschnittsmaterien" zwischen mehreren Rechtsgebieten beinhalten. Da es ein Praxisbericht ist, erhebt dieser Beitrag keinen Anspruch auf Wissenschaftlichkeit.

Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2008

… mit düsteren Visionen…

7. Ergebnis

Die Beispiele in diesem Beitrag zeigen, dass der Gesetzgeber zwar bemüht ist, den „Old-Economy-Rechtsstaat" durch „moderne" Normen zu bereichern, die auch den „Cyberspace" regeln sollen, dass in der Praxis die Umsetzung und Anwendung dieser Bestimmungen jedoch verbesserungswürdig sind. Verbesserungswürdig sind etwa die Zuständigkeitsverteilungen bei der Sanktionierung dieser „modernen" Normen, etwa die Zentralisierung der Vollziehung der Straftatbestände des Datenschutzrechtes oder E-Commerce-Gesetzes bei spezialisierten Stellen, anstatt diese auf unzählige Bezirksverwaltungsbehörden zu zerstreuen,[34] wo sich Personen mit nicht ausreichender Schulung und Kenntnis der Materie damit „herumschlagen" müssen. Ebenso verbesserungsfähig ist die Ausstattung der zuständigen Stellen mit geschultem Fachpersonal, etwa der Datenschutzkommission, die seit Jahren unter akutem Personalmangel leidet und immer mehr zum peinlichen personellen Schlusslicht unter den europäischen Datenschutzbehörden wird.[35] Unbedingt verbessert werden muss auch der Rechtsschutz bei den typischerweise internationalen Sachverhalten im Internet. Dazu müssten eine verbesserte Zusammenarbeit zwischen den Gerichten und Strafverfolgungsbehörden in diesem Bereich stattfinden sowie einfachere, klare und effizientere Zuständigkeiten geschaffen werden. Dies, was natürlich ein schwieriges Unterfangen ist, auf globaler Ebene.

…und der Scherbenhaufen 2018

KURIER

NIEDERÖSTERREICH
MITTWOCH
11. APRIL 2018
NR. 98 / 1,50 €
KURIER.at

UNABHÄNGIGE TAGESZEITUNG FÜR ÖSTERREICH

Wankender Riese

Fake News bis Datenmissbrauch. Das Eingeständnis des Mark Zuckerberg: „Es tut mir leid. Es war mein Fehler. Ich trage die Verantwortung."

THEMA 6, 7

HEUTE

DEUTSCHLAND

Neuer Chef für Volkswagen

Umbau im Autokonzern: Markenchef Diess (Bild) gilt als heißester Nachfolge-Kandidat für Müller.

WIRTSCHAFT 13

ANALYSE

Chinesische Kunst: Radikal kompatibel

Die Kunst-Superstars im Reich der Mitte: Brutale Arbeiten mit Tieren und riesige Installationen.

KULTUR 25

WETTER

Bezugsort St. Pölten

21° 23° 21°

MI DO FR

Oft sonnig

Der Südwind bleibt lebhaft, dazu einige Wolken und Sonnenschein.

WETTER 30

INHALT

WELTWIRTSCHAFT

NIEDERÖSTERREICH-SCHLAGZEILEN


profil
Das unabhängige Nachrichtenmagazin Österreichs
Nr. 15 • 49. Jg. • 9. April 2018
DIE BVT-AFFÄRE
Kriminalfall?
Rachekomplott?
Politische Verschwörung?
Eine Zwischenbilanz.
IST
facebook
BÖSE?
ODER SIND
WIR SELBST
SCHULD AM
DATENSKANDAL?
€ 3,95
SAUDI-ARABIEN
Reportage aus einem Königreich
im rasenden Umbruch
ROBERT TREICHLER
„Wie man Israels Geburtstag
feiern soll"
www.profil.at

Kurier, Ausgabe vom 4. April 2018.

Behebung von Problemen dauert noch Jahre

Krise. Neben dem Vertrauensverlust kämpft das Unternehmen mit sinkendem Aktienkurs

„Wir werden uns aus diesem Loch herausgraben, aber es wird einige Jahre dauern.“

Mark Zuckerberg

Keine Lösung in Sicht

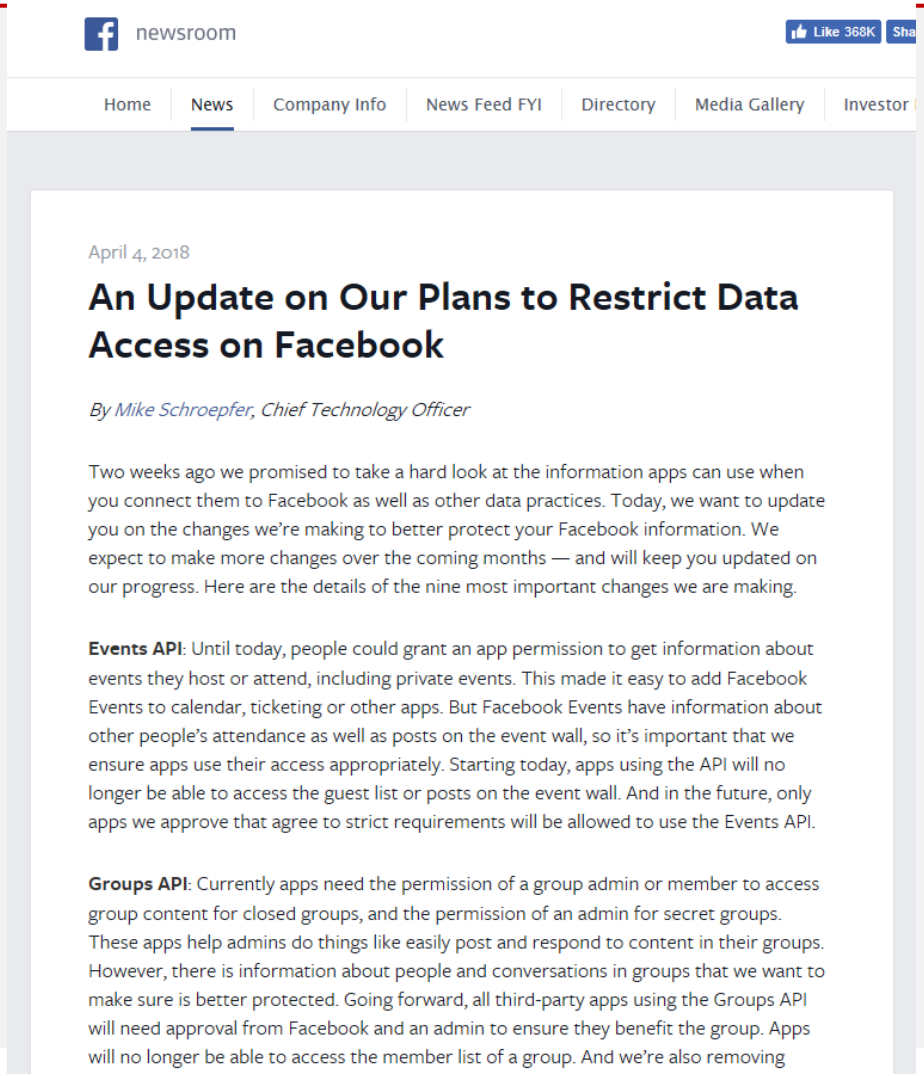
– FLORIAN CHRISTOF

Was man bei sozialen Netzwerken beachten sollte

– FLORIAN CHRISTOF

„Dauert noch Jahre“… willkommen in Europa nach dem 25.5.2018

Auf dem Weg zu neuen Höhen…



newsroom

Like 368K Sha

Home | News | Company Info | News Feed FYI | Directory | Media Gallery | Investor

April 4, 2018

An Update on Our Plans to Restrict Data Access on Facebook

By Mike Schroepfer, Chief Technology Officer

Two weeks ago we promised to take a hard look at the information apps can use when you connect them to Facebook as well as other data practices. Today, we want to update you on the changes we're making to better protect your Facebook information. We expect to make more changes over the coming months — and will keep you updated on our progress. Here are the details of the nine most important changes we are making.

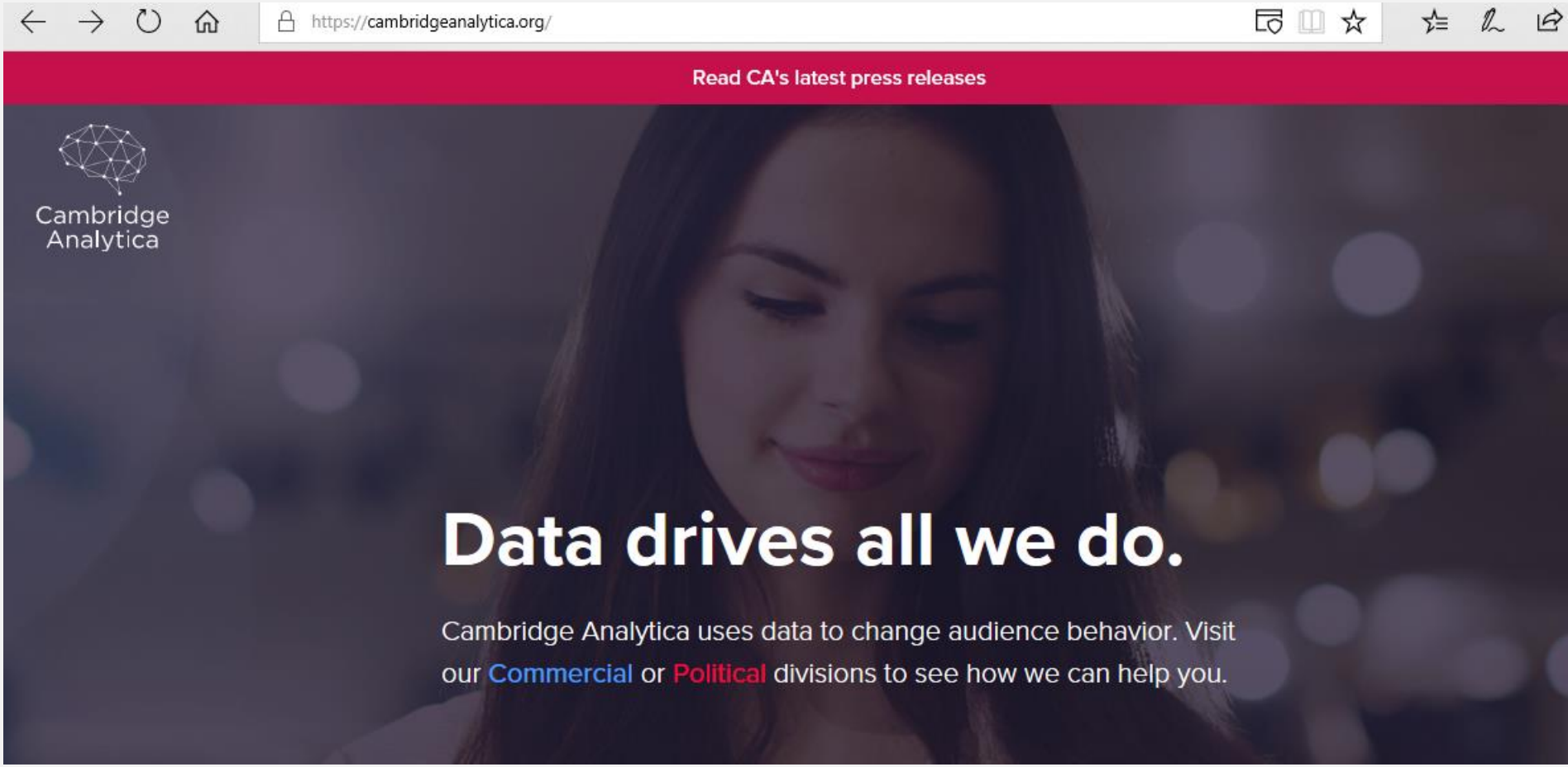
Events API: Until today, people could grant an app permission to get information about events they host or attend, including private events. This made it easy to add Facebook Events to calendar, ticketing or other apps. But Facebook Events have information about other people's attendance as well as posts on the event wall, so it's important that we ensure apps use their access appropriately. Starting today, apps using the API will no longer be able to access the guest list or posts on the event wall. And in the future, only apps we approve that agree to strict requirements will be allowed to use the Events API.

Groups API: Currently apps need the permission of a group admin or member to access group content for closed groups, and the permission of an admin for secret groups. These apps help admins do things like easily post and respond to content in their groups. However, there is information about people and conversations in groups that we want to make sure is better protected. Going forward, all third-party apps using the Groups API will need approval from Facebook and an admin to ensure they benefit the group. Apps will no longer be able to access the member list of a group. And we're also removing

Das ist der Gipfel!

Facebook Login: Two weeks ago we announced important changes to Facebook Login. Starting today, Facebook will need to approve all apps that request access to information such as check-ins, likes, photos, posts, videos, events and groups. We started approving these permissions in 2014, but now we're tightening our review process — requiring these apps to agree to strict requirements before they can access this data. We will also no longer allow apps to ask for access to personal information such as religious or political views, relationship status and details, custom friends lists, education and work history, fitness activity, book reading activity, music listening activity, news reading, video watch activity, and games activity. In the next week, we will remove a developer's ability to request data people shared with them if it appears they have not used the app in the last 3 months.

Oder das?


https://cambridgeanalytica.org/
Read CA's latest press releases
Cambridge Analytica
Data drives all we do.
Cambridge Analytica uses data to change audience behavior. Visit our Commercial or Political divisions to see how we can help you.

Auf dem Weg zum höchsten Berg Europas

- **Informationspflicht nach Art 13**
- Einwilligung
- Datenschutz-Folgenabschätzung

Informationspflicht (Art 13)

- **Abs 1: Der Verantwortliche teilt zum Zeitpunkt der Erhebung Folgendes mit:**
  - Name/Kontaktdaten des Verantwortlichen (Datenschutzbeauftragten);
  - Zwecke der Datenverarbeitung;
  - Rechtsgrundlagen: Datenverarbeitung (ggf. Offenlegung überwiegender berechtigter Interessen);
  - (Kategorien von) Übermittlungsempfängern
- **Abs 2: Folgende weitere Informationen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:**
  - Speicherdauer von Daten oder Kriterien für Bestimmung derselben;
  - Hinweis auf Betroffenenrechte (inkl. Hinweis auf Beschwerderecht);
  - Hinweis auf Widerrufsrecht von Zustimmungserklärungen;
  - Hinweis auf Logik und Auswirkungen einer automationsunterstützten Entscheidungsfindung;
  - Bei geplanter weiterer Verwendungszwecken -> **neue Informationspflicht!**

Laut Art 29-Datenschutzgruppe ist auch Abs 2 immer verpflichtend!

Art 29-Gruppe, Guidelines on Transparency, WP 260, 12 zu Abs 1 und 2

"For clarity, WP29's position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject."

Art 29-Gruppe, WP 260, 14 zu Zeitpunkt der Information

"As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided "at the time when personal data are obtained". In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:

- The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, "having regard to the specific circumstances in which the personal data are processed" (Article 14.3(a)).

Art 29-Gruppe, WP 260, 13 zu Text-Tests

"In order to help identify the most appropriate modality for providing the information, in advance of "going live", data controllers may wish to trial different modalities by way of user testing (e.g. hall tests) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/ approach chosen to convey the information is the most appropriate in the circumstances."

A1 Datenschutzerklärung

Wir verwenden folgende Daten:

Allgemeine Daten – schließen Sie mit uns einen Vertrag ab, so verarbeiten wir folgende Daten:

- Ihre Stammdaten: Familien- und Vorname, akademischer Grad, Adresse, Teilnehmernummer und Kontakt-Informationen (z.B. E-Mail-Adresse, Telefonnummer), Informationen über Art und Inhalt unseres Vertragsverhältnisses und Ihre Bonität.
- Sonstige personenbezogene Daten, die Sie oder Dritte uns mit Ihrem Einverständnis oder sonst zulässigerweise bei der Vertragsanbahnung oder während des Vertragsverhältnisses zur Verfügung stellen, das sind: Geburtsdatum bzw. Alter, Familienstand, Geschlecht, Beruf, Ausweisdaten, Bankverbindung, Zeichnungs- oder Vertretungs-Befugnis, verwendetes Endgerät, Vertragsbindung, Vertragslaufzeit, Kündigungsfrist, Produkte von Tochtergesellschaften der A1 Telekom Austria AG oder weitere Informationen zu Ihrer Person, die Sie offensichtlich selbst öffentlich gemacht haben. Unter diesen Begriff fallen keine datenschutzrechtlich sensiblen Daten, das sind insbesondere rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische oder Gesundheitsdaten.

Telekommunikationsdaten – schließen Sie mit uns einen Vertrag über Telekommunikationsdienstleistungen ab, so verarbeiten wir entsprechend Ihrem Vertrag zusätzlich folgende Daten:

- Ihre Verkehrsdaten einschließlich Standortdaten: Daten, die wir zum Weiterleiten einer Nachricht an ein Kommunikationsnetz oder zum Verrechnen verarbeiten.
- WLAN Messdaten: Eigenschaften der verwendeten WLAN Frequenz (Übertragungsstärke, Überlagerung, Netzstärke), Dauer der Anbindung, Netzstärke und Art einzelner Endgeräte, sowie WLAN Wiederherstellung und Vernetzung von Mashup Systemen.

Ihre Inhaltsdaten werden grundsätzlich nicht gespeichert. Diese Daten werden nur dann kurzfristig gespeichert, wenn es technisch notwendig ist, oder wenn es die Serviceerbringung betrifft, z.B. SMS-, Mobilboxnachrichten.

Smart Home Daten – schließen Sie mit uns einen Vertrag über ein Smart Home Produkt ab, so verarbeiten wir zusätzlich folgende Daten:

- Messdaten: jene Daten, die von den an Ihr Smart Home System angebundenen Geräten bzw. Sensoren erzeugt oder ermittelt werden in Verbindung mit den Internetverbindungsdaten Ihres Smart Home Systems.

Datenverarbeitung im Auftrag

Auch wenn wir einen Auftragsverarbeiter beauftragen, bleiben wir für den Schutz Ihrer Daten verantwortlich. Auftragsverarbeiter außerhalb der Europäischen Union setzen wir nur dann ein, wenn für das betreffende Drittland ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt oder wenn wir geeignete Garantien oder verbindliche interne Datenschutzvorschriften mit dem Auftragsverarbeiter vereinbart haben.

Wir löschen:

- Ihre Stammdaten und sonstigen personenbezogenen Daten grundsätzlich nach Beendigung des Vertragsverhältnisses, spätestens jedoch nach Erlöschen aller gesetzlichen Aufbewahrungspflichten (beispielsweise jener nach § 212 UGB oder §§ 207f BAO in der geltenden Fassung).
- Ihre Verkehrsdaten innerhalb einer Frist von drei Monaten nach erfolgtem Bezahlvorgang, sofern Sie keinen schriftlichen Einspruch getätigt haben.
  Bitte beachten Sie, dass wir Ihre Daten während eines laufenden Verfahrens (Einspruch, offene Rechnungen, etc.) nicht löschen.
- Ihre Inhaltsdaten, sobald ihre Verarbeitung nicht mehr zur Erbringung unserer Kommunikationsdienste erforderlich ist.
- Ihre WLAN Messdaten spätestens drei Monate nach deren Erhebung.
- Ihre Teilnehmerdaten, sobald ein Teilnehmer entfernt wird bzw. mit Beendigung Ihres Smart Home Vertrages.
- Ihre Messdaten spätestens sechs Monate nach deren Erhebung
- Ihr Nutzerprofil mit Beendigung Ihres Smart Home Vertrages.

Es besteht die Möglichkeit, dass anstatt einer Löschung eine Anonymisierung der Daten vorgenommen wird. In diesem Fall wird jeglicher Personenbezug unwiederbringlich entfernt, weshalb auch die datenschutzrechtlichen Löschungsverpflichtungen entfallen.

A1 Telekom Austria AG, Postfach 1001, 1011 Wien
Sitz: Wien, Firmenbuch-Nr. FN 280571f, Firmenbuchgericht: Handelsgericht Wien, DVR 0962635, UID ATU 62895905

Recht auf Einschränkung der Verarbeitung: Sie können von uns die Einschränkung der Verarbeitung Ihrer Daten verlangen, wenn

- Sie die Richtigkeit der Daten bestreiten, und zwar für eine Dauer, die es uns ermöglicht, die Richtigkeit der Daten zu überprüfen.
- die Verarbeitung der Daten unrechtmäßig ist, Sie aber eine Löschung ablehnen und stattdessen eine Einschränkung der Datennutzung verlangen,
- wir die Daten für den vorgesehenen Zweck nicht mehr benötigen, Sie diese Daten aber noch zur Geltendmachung oder Verteidigung von Rechtsansprüchen brauchen, oder
- Sie Widerspruch gegen die Verarbeitung der Daten eingelegt haben.

Dieses Recht können Sie ab dem 25.5.2018 in Anspruch nehmen.

Recht auf Datenübertragbarkeit: Sie können von uns verlangen, dass wir Ihnen Ihre Daten, die Sie uns zur Aufbewahrung anvertraut haben, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen, sofern

- wir diese Daten aufgrund einer von Ihnen erteilten und widerrufbaren Zustimmung oder zur Erfüllung eines Vertrages zwischen uns verarbeiten, und
- diese Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Dieses Recht können Sie ab dem 25.5.2018 in Anspruch nehmen.

Widerspruchsrecht: Verarbeiten wir Ihre Daten zur Wahrnehmung von im öffentlichen Interesse liegenden Aufgaben, zur Ausübung öffentlicher Gewalt oder berufen wir uns bei der Verarbeitung auf die Notwendigkeit zur Wahrung unseres berechtigten Interesses, so können Sie gegen diese Datenverarbeitung Widerspruch einlegen, sofern ein überwiegendes Schutzinteresse an Ihren Daten besteht. Der Zusendung von Werbung können Sie jederzeit ohne Angabe von Gründen widersprechen.

Beschwerderecht: Sind Sie der Meinung, dass wir bei der Verarbeitung Ihrer Daten gegen österreichisches oder europäisches Datenschutzrecht verstoßen, so ersuchen wir Sie, mit uns Kontakt aufzunehmen, um allfällige Fragen aufklären zu können. Sie haben selbstverständlich auch das Recht, sich bei der österreichischen Datenschutzbehörde, ab 25.5.2018 auch bei einer Aufsichtsbehörde innerhalb der EU, zu beschweren.

Sie können folgende Rechte im Hinblick auf die Verarbeitung Ihrer Daten geltend machen:

Auskunftsrecht: Sie können von uns eine Bestätigung darüber verlangen, ob und in welchem Ausmaß wir Ihre Daten verarbeiten.

Kontakt / Verantwortlicher:
A1 Telekom Austria AG
Datenschutz
Lassallestraße 9, 1020 Wien
datenschutz@a1telekom.at

Recht auf Berichtigung: Verarbeiten wir Ihre personenbezogene Daten, die unvollständig oder unrichtig sind, so können Sie jederzeit deren Berichtigung bzw. deren Vervollständigung von uns verlangen.

Recht auf Löschung: Sie können von uns die Löschung der Ihre personenbezogenen Daten verlangen, sofern wir diese unrechtmäßig verarbeiten oder die Verarbeitung unverhältnismäßig in Ihre berechtigten Schutzinteressen eingreift. Bitte beachten Sie, dass es Gründe geben kann, die einer sofortigen Löschung entgegenstehen, z.B. im Fall von gesetzlich geregelten Aufbewahrungspflichten.

A1 Telekom Austria AG, Postfach 1001, 1011 Wien
Sitz: Wien, Firmenbuch-Nr. FN 280571f, Firmenbuchgericht: Handelsgericht Wien, DVR 0962635, UID ATU 62895905

Beispiel Bank Austria – Kontaktdaten DSB

Vertrauen ist wichtig, besonders wenn es um Ihre Daten geht. Deshalb sehen wir es als unsere Verpflichtung, Ihre Daten mit höchster Sorgfalt zu verwalten und alles zu tun, um Ihre Informationen vor Missbrauch zu schützen.

Die UniCredit Bank Austria AG hält sich strikt an die datenschutzrechtlichen Vorschriften bei der Erhebung und Verarbeitung Ihrer Daten. Die folgenden Informationen erklären im Detail, welche Daten während Ihres Besuches auf unserer Website erfasst werden und wie wir diese nutzen.

Diese Datenschutzerklärung gilt für die Website http://www.bankaustria.at der UniCredit Bank Austria AG. Einzelne Seiten können Links auf andere Anbieterinnen und Anbieter innerhalb und außerhalb der UniCredit Group enthalten, auf die sich die Datenschutzerklärung nicht erstreckt, d. h., für diese Inhalte können wir keinerlei Haftung übernehmen.

1. Wer ist für die Datenverarbeitung verantwortlich, und an wen können Sie sich wenden?

Für die Datenverarbeitung verantwortlich:
UniCredit Bank Austria AG
Schottengasse 6-8
1010 Wien
E-Mail: info@unicreditgroup.at

Datenschutzbeauftragter der UniCredit Bank Austria AG:
Richard Jarolim
Lassallestraße 5
1020 Wien
Telefon: 05 05 05-32836
E-Mail: datenschutz@unicreditgroup.at

DATENSCHUTZINFORMATION

"Gewinnspiele und Marketingmaßnahmen"

der Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG

1)	**Verarbeitungstätigkeit**	**Veranstaltung von Gewinnspielen und Durchführung von Marketingmaßnahmen für Kunden**[1]	
2)	**Verantwortlicher**	**Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG („Verlag")** Sitz: Muthgasse 2, A-1190 Wien Niederlassung: Richard-Strauss-Straße 16, 1232 Wien Tel: 05 1727-0 E-Mail: kundenservice@mediaprint.at	
3)	**Kontaktdaten des Datenschutzbeauftragten**	Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG c/o Datenschutzbeauftragter Richard-Strauss-Straße 16, 1232 Wien E-Mail: datenschutz@mediaprint.at	
4)	**Zwecke der Datenverarbeitung**	a)	Neu- und Rückgewinnung von Kunden für den Vertrieb von Verlagsprodukten („Produkte"), insbesondere Tageszeitungen und Zeitschriften (Print und

15)	**Externe Empfänger von Daten**	**Konzernunternehmen**	**Auftragsverarbeiter**
		Redaktionen:	**Kategorien externe wirtschaftliche Dienstleister:**
		KRONE - Verlag Gesellschaft m.b.H. & Co. KG, Muthgasse 2, 1190 Wien	Steuerberater/Wirtschaftsprüfer
		KRONE Multi Media Gesellschaft m.b.H., Muthgasse 2, 1190 Wien	Rechtsanwälte
		KURIER Zeitungsverlag und Druckerei Gesellschaft m.b.H, Leopold-Ungar-Platz 1, 1190 Wien	Beauftragte Dienstleister: Zustell- und Kooperationspartner
		KURIER RedaktionsgmbH & Co. KG Leopold-Ungar-Platz 1, 1190 Wien	Beauftrage Dienstleister: Werbe-Kooperationspartner
		Telekurier Online Medien GmbH & Co KG 1190 Wien, Leopold-Ungar-Platz 1	Beauftragte Dienstleister: Externe Call-Center
		KRONE - Verlag Gesellschaft m.b.H. & Co. KG, Muthgasse 2, 1190 Wien	
		Vertrieb:	
		MediaCalling Callcenter GmbH	E-Mail-Kampagnenversand: eyepin GmbH, Billrothstraße 52, 1190 Wien
			SMS-Kampagnenversand: A1 Telekom Austria AG, Lassallestraße 9, 1020 Wien

§ 13 DSG neu - Bildverarbeitung

- Betrifft sowohl **Foto**, als auch **Videoaufnahme**

- **Kennzeichnungspflicht: Name des Verantwortlichen!**


Knyrim (Hrsg)
Der DaKomm
Zeitnah zum Inkrafttreten der DSGVO
Der DaKomm
Praxiskommentar zum Datenschutzrecht
DSGVO und DSG
Kommentar
MANZ
Faszikelwerk in 1 Mappe
erscheint im Sommer 2018.
Komplett ca 1.000 Seiten.
Ca. EUR 198,–
ISBN 978-3-214-17236-7
Im Abonnement zur Fortsetzung
vorgemerkt.
Warten lohnt sich!
Der neue Praxiskommentar beantwortet Ihre Fragen zum neuen Datenschutzrecht umfassend und zeitnah zum Inkrafttreten der Datenschutzgrundverordnung.
Die DSGVO und das österreichische DSG werden inhaltlich sinnvoll verschränkt dargestellt und tiefgehend kommentiert. Die wesentlichen Auslegungsschritte, wichtige Literatur und Judikatur – auch zu bisher geltendem Recht – finden Sie hier!
Anhänge mit Checklisten, Guidelines und Beschlüssen des Datenschutzausschusses, wichtigen Bestimmungen aus Nebennormen, wie zB der RL über Polizei und Strafjustiz, runden den Praxiskommentar ab.
Erarbeitet wird diese fundierte Rechtsinformation von einem 33-köpfigen Autorenteam.
Der Herausgeber:
Dr. Rainer Knyrim, Partner bei Knyrim Trieb Rechtsanwälte in Wien.
Die Redaktion:
Mag. Viktoria Haidinger, LL.M., Stv. Leiterin der Stabsabteilung Statistik in der WKÖ.
DI Michael Löffler, Data Protection Officer im AIT Austrian Institute of Technology.
Kommerzialrat Prof. Hans-Jürgen Pollirer, Gerichtssachverständiger und Geschäftsführer der SECUR-DATA GmbH.
Dr. Gerald Trieb, LL.M., Partner bei Knyrim Trieb Rechtsanwälte in Wien
MANZ

Auf dem Weg zum höchsten Berg Europas

- Informationspflicht nach Art 13
- **Einwilligung**
- Datenschutz-Folgenabschätzung

Der Berg ruft…

- DSG § 69 Abs 9: Bereits eingeholte Zustimmungserklärung ist **auch künftig weiter gültig**, wenn schon bisher **Anforderungen der DSGVO** entsprochen hat

- „Hellseher“-Bestimmung?!

Berg ja, Twin Peaks nein…

- **Achtung auf Kopplungsverbot Art 7 Abs 4 DSGVO: Vertragsgegenstand und Werbezustimmung sind zu trennen!**

- **Waren Sie Hellseher? Oder haben Sie sich an die OGH-Judikatur gehalten?**

Altbestand: Den Abhang hinunter?

Art 29-Gruppe, Guidelines on Consent, WP 259, letzte Seite:

"For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed."

Auf dem Weg zum höchsten Berg Europas

- Informationspflicht nach Art 13
- Einwilligung
- **Datenschutz-Folgenabschätzung**

DATENSCHUTZGRUPPE NACH ARTIKEL 29

17/DE

WP 248 Rev. 01

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"

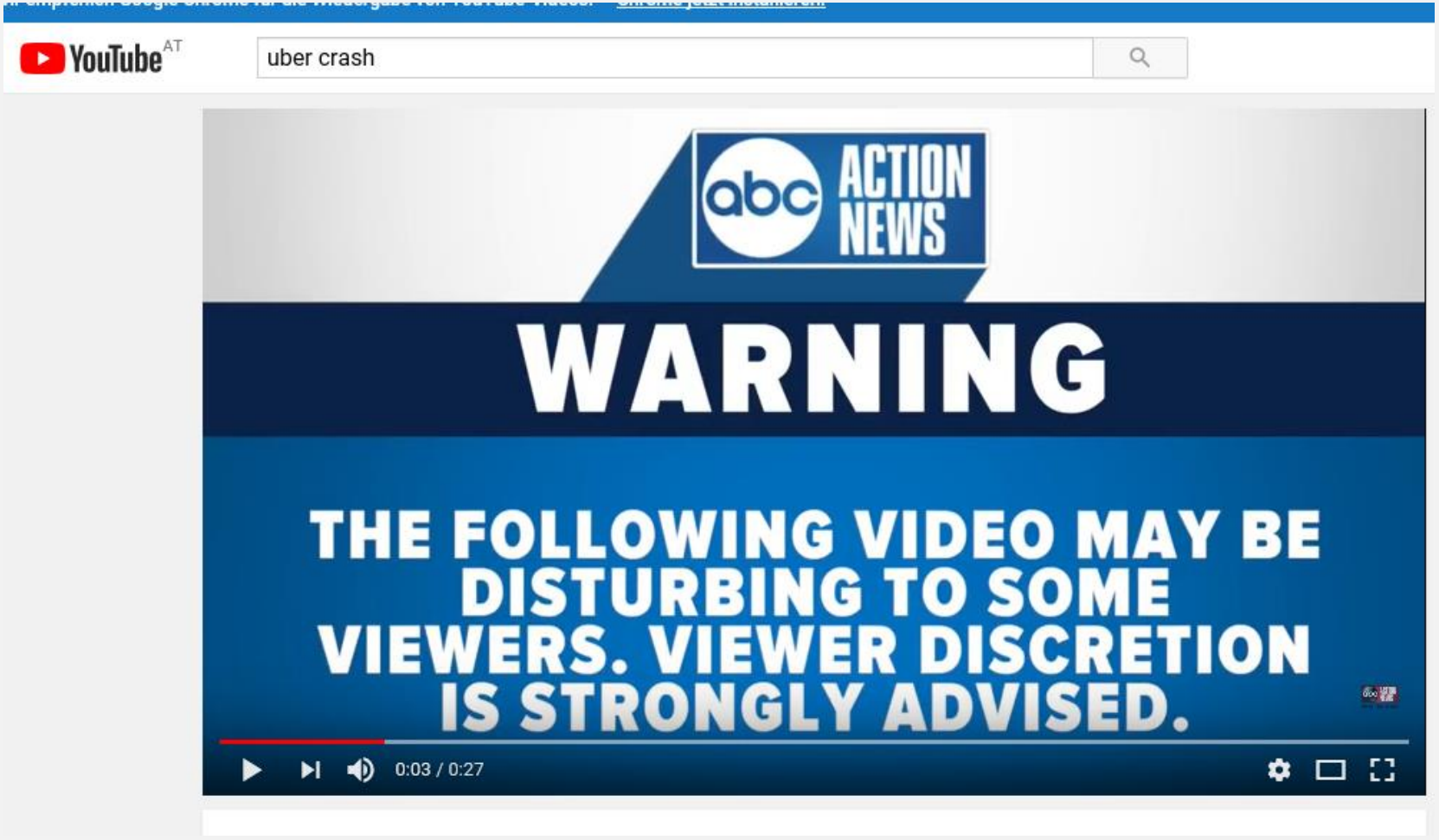
Um unter Berücksichtigung der in Artikel 35 Absatz 1 und Artikel 35 Absatz 3 Buchstaben a bis c genannten Elemente, der gemäß Artikel 35 Absatz 4 und den Erwägungsgründen 71, 75 und 91 auf einzelstaatlicher Ebene festzulegenden Liste sowie anderer Bezugnahmen in der DSGVO auf Verarbeitungsvorgänge, die „*wahrscheinlich ein hohes Risiko mit sich bringen*“[14], eine konkretere Menge von Verarbeitungsvorgängen zu ermitteln, für die aufgrund ihres hohen Risikos eine DSFA erforderlich ist, müssen folgende neun Kriterien berücksichtigt werden:

4. Vertrauliche Daten oder höchst persönliche Daten: Hierzu zählen besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 (z. B. Informationen über die politischen Meinungen von Einzelpersonen) sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne von Artikel 10. Hierfür seien als Beispiele ein allgemeines Krankenhaus genannt, das die Krankenakten seiner Patienten archiviert, oder ein Privatdetektiv, der Akten zu Straftätern führt. Darüber hinaus gibt es weitere Datenkategorien, die zwar nicht in den DSGVO-Bestimmungen aufgeführt sind, jedoch die möglichen Risiken für die Rechte und Freiheiten von Personen erhöhen können. Diese personenbezogenen Daten gelten als vertraulich (im gängigen Sinne des Wortes), da sie mit häuslichen und privaten Aktivitäten verknüpft sind (wie etwa die elektronische Kommunikation, deren Vertraulichkeit geschützt werden muss), sich auf die Ausübung eines der Grundrechte auswirken (wie etwa Standortdaten, deren Erfassung die Freizügigkeit in Frage stellt) oder die Verletzung derselben mit ernsthaften Konsequenzen für den Alltag des Betroffenen einhergeht (wie etwa Finanzdaten, die für den Zahlungsbetrug missbraucht werden könnten). In diesem Zusammenhang kann es von Bedeutung sein, ob die Daten durch den Betroffenen oder durch Dritte bereits öffentlich zugänglich gemacht worden sind. Die öffentliche Zugänglichkeit personenbezogener Daten kann als bestimmender Faktor gelten, wenn beurteilt werden soll, ob eine weitere Nutzung der Daten für bestimmte Zwecke vorgesehen war. In dieses Kriterium können auch Daten wie persönliche Dokumente, E-Mails, Tagebücher, Notizen aus E-Readern mit Notizfunktion sowie über Lifelogging-Anwendungen erfasste, sehr persönliche Informationen fallen.

KNYRIM.TRIEB
RECHTSANWÄLTE

Privatsphäre und IT-Technologie am Abgrund

Autonomes Fahren – Privatsphäre und künstliche Intelligenz am Abgrund



KNYRIM.TRIEB
RECHTSANWÄLTE

Polizeistation stellt in laufender Untersuchung Video eines Unfalls zur Verfügung, an dem nur 2 Personen beteiligt sind

uber crash

Aus der Finsternis…

…taucht eine Fußgängerin auf und wird überfahren.

Die „Mörderin“, die auf ihr Handy schaute.

„Dazu wollen wir den Rechtsrahmen ausbilden und unsere Digitalen Testfelder fortführen."

Dorothee Bär verteidigt die Technik

Die Staatsministerin für Digitalisierung, Dorothee Bär, verteidigte die neue Technik nach dem tödlichen Unfall in den USA. „Wir messen jedem Unfall, der mit einem selbstfahrenden Fahrzeug geschieht, eine wesentliche höhere Beachtung bei als wenn das eben jetzt im Realverkehr mit Fahrern passiert", sagte die CSU-Politikerin im Inforadio des rbb.

Bisher warnten Kritiker selbstfahrender Autos vor allem vor Fällen, in denen Software entscheiden müsse, wen sie opfert, wenn ein Unfall unausweichlich sein sollte. Im Fall Tempe geht es zunächst einmal um die grundsätzliche Funktionstüchtigkeit der Technologie. Warum konnten die Sensoren die Frau im Schatten nicht besser erkennen als das menschliche Auge? Und warum war der Wagen mit leicht überhöhter Geschwindigkeit (38 Meilen pro Stunde statt der erlaubten 35, bzw. 61 km/h statt 56 km/h) unterwegs?

https://de.nachrichten.yahoo.com/polizei-veröffentlicht-aufnahmen-tödlichem-uber-unfall-104813957--finance.html

Nachrichten Sport Finanzen Stars Style Movies Flickr Mobile Mehr

Suche Suche

Drei Tage nach dem tödlichen Unfall mit einem selbstfahrenden Auto von Uber in Tempe im US-Bundesstaat Arizona hat die Polizei am Mittwoch Videoaufnahmen von den letzten Sekunden vor dem Zusammenstoß mit einer Fußgängerin veröffentlicht

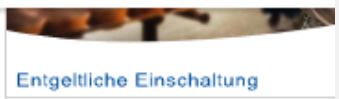
Drei Tage nach dem tödlichen Unfall mit einem selbstfahrenden Auto von Uber im US-Bundesstaat Arizona hat die Polizei Videoaufnahmen von den letzten Sekunden vor dem Zusammenstoß mit einer Fußgängerin veröffentlicht. In den am Mittwoch (Ortszeit) von der Polizei von Tempe veröffentlichten Aufnahmen ist zu sehen, wie die Insassin des Wagens kurz vor dem Aufprall sichtlich entsetzt den Mund aufreißt.

Die Aufnahmen aus dem Inneren des Autos scheinen zu belegen, dass sich die Fahrerin auf die Automatikfunktion ihres Wagens verlassen hatte: Sekundenlang blickt sie nach unten, erst kurz vor dem Zusammenprall schaut sie auf und schnappt entsetzt nach Luft.

Aufnahmen einer Kamera auf dem Amaturenbrett zeigen gleichzeitig, wie die Fußgängerin ihr Fahrrad über die unbeleuchtete Straße schiebt: Scheinbar aus dem Nichts tauchen zuerst ihre Füße im Bild auf, anderthalb Sekunden später wird sie von dem Auto in voller Fahrt getroffen. Die 49-Jährige erlag im Krankenhaus ihren Verletzungen.

Der tödliche Unfall fachte die Debatte über die Sicherheit des autonomen Fahrens weiter an. Der US-Fahrdienstvermittler Uber äußerte sich am Montag tief betroffen und stoppte vorübergehend den Betrieb seiner selbstfahrenden Autos für Tests oder Kundenfahrten in Tempe, Pittsburgh, Toronto und San Francisco. Gleichzeitig kündigte das Unternehmen an, "vollständig mit den örtlichen Behörden" zu kooperieren, um den Unfall aufzuklären.

erst entstehen lassen, die heute von Menschen verursacht werden.



Aber natürlich, wenn irgendwann einmal viele selbstfahrende Autos auf der Straße sind, dann würden sich auch Unfälle mit Todesopfern nicht vermeiden lassen.

In der Realität kam es anders. Der erste Todesfall passierte noch lange bevor Robotertaxis zum Alltag in den Städten wurden. In der US-Stadt Tempe mit gerade einmal gut 180 000 Einwohnern erfasste ein autonomer Testwagen des Fahrdienst-Vermittlers Uber eine Fußgängerin, die die Straße überquerte. Die 49-Jährige starb im Krankenhaus. Der aus einem Volvo-SUV umgebaute Uber-Roboterwagen habe keine Anstalten gemacht, abzubremsen, teilte die Polizei mit.

Polizei hat Verständnis für den Roboter

Die Polizeichefin von Tempe zeigte Verständnis für den menschlichen Sicherheitsfahrer am Steuer: Es war um 22.00 Uhr dunkel, die Frau trat direkt aus dem Schatten auf die Fahrbahn, er habe sie erst gesehen, als es zu dem Aufprall kam. Die Kameras des Autos belegten dies.

Was wird beim Uber-Crash übersehen?

Warum brauchen wir statt mehr künstlicher Intelligenz wieder mehr natürliche Intelligenz?

Aus der Finsternis… tauchte die Frau auf…

Fahren auf Sicht!

OGH: § 20 Abs 1 Satz 1 StVO - Fahren auf Sicht (hier: bei Dunkelheit mit Abblendlicht auf Freilandstraße)

GZ 2 Ob 109/10h, 17.02.2011

OGH: Der aus § 20 Abs 1 Satz 1 StVO abgeleitete Grundsatz des Fahrens auf Sicht bedeutet, dass ein Fahrzeuglenker seine Fahrgeschwindigkeit so zu wählen hat, dass er sein Fahrzeug beim Auftauchen eines Hindernisses rechtzeitig zum Stehen bringen und zumindest das Hindernis umfahren kann. Jeder Kraftfahrer muss daher seine Fahrweise so gestalten, dass der Weg des abzubremsenden Fahrzeugs in der Zeit vom Erkennen eines Hindernisses auf der Fahrbahn bis zum vollen Stillstand des Fahrzeugs nie länger als die durch ihn eingesehene Strecke ist. **Diese Pflicht besteht auch auf Freilandstraßen.**

Fährt ein Kraftfahrer bei Dunkelheit mit Abblendlicht, dann hat er, soweit nicht besondere Umstände die Sicht über die vom Abblendlicht erleuchtete Strecke hinaus ermöglichen, grundsätzlich mit einer Geschwindigkeit zu fahren, die ihm das Anhalten seines Fahrzeugs innerhalb der Reichweite des Abblendlichts gestattet. Fährt er mit höherer Geschwindigkeit, dann hat er **Fernlicht** zu verwenden.

Polizeichef, in laufenden Ermittlungen:

Polizei hat Verständnis für den Roboter

Die Polizeichefin von Tempe zeigte Verständnis für den menschlichen Sicherheitsfahrer am Steuer: Es war um 22.00 Uhr dunkel, die Frau trat direkt aus dem Schatten auf die Fahrbahn, er habe sie erst gesehen, als es zu dem Aufprall kam. Die Kameras des Autos belegten dies.

Heute, 12.4.2018

Studie über Jugend am Smartphone

Verlernt Phono Sapiens Denken?

Hochinteressante Studie zur Korrelation zwischen extrem hoher Handy-Nutzung und Hirnleistung bei Jugendlichen in England: Durch die Auslagerung von Teilen des Großhirns an Google können Schüler bis zu 14 Prozent schlechter abschneiden als solche, die das Smartphone selten nutzen. Geprüft wurden rund 100.000 britische Schüler

Foto: iStock

Foto: ORF

Tesla-Crash – mit umgekehrter Geschichte

Update 13.4.2018, 7.39 Uhr: Der NTSB hat bestätigt, die Kooperation mit Tesla von sich aus beendigt zu haben. Das Unternehmen habe sich nicht an die Vereinbarung gehalten, indem es Informationen zum Unfallhergang veröffentlicht hatte, bevor sie von der Behörde überprüft und bestätigt werden konnten. Unvollständige Informationen zu veröffentlichen führe oft zu Spekulationen und falschen Annahmen über die wahrscheinliche Ursache eines Unfalls. Damit werde den Untersuchungen und der Öffentlichkeit ein schlechter Dienst erwiesen, heißt es in einer Mitteilung.

Untersuchungen der NTSB dauerten normalerweise ein bis zwei Jahre, bis sie abgeschlossen werden, erläutert die Behörde. Transparenz sei gegeben durch offizielle Zwischenberichte, auch seien Vorstandstreffen öffentlich. Bei zwei anderen Unfällen, in denen Tesla beteiligt ist, bleibe das Unternehmen Kooperationspartner der Untersuchungen des NTSB.

Bild 1 von 25

heise.de

Tesla-Crash – mit umgekehrter Geschichte

Bei dem Unfall war ein Tesla Model X auf einer Autobahn im kalifornischen Silicon Valley gegen einen Beton-Poller gefahren. Die Ermittlungsbehörde NTSB hatte daraufhin die Untersuchung angekündigt, was den Aktienkurs von Tesla zeitweise kräftig unter Druck brachte. Mit dem "Autopilot" hatte es bereits zuvor Unfälle und Kontroversen gegeben. Laut Tesla ist die einzige Erklärung für den tödlichen Crash jedoch ein Versagen des Fahrers. Dieser habe mehrere visuelle und eine akustische Warnung bekommen – und etwa fünf Sekunden Zeit und 150 Meter Entfernung bis zum Aufprall gehabt. Seine Hände seien vor der Kollision sechs Sekunden lang nicht auf dem Lenkrad gewesen.

heise.de

Was für Technologie wird hier in den USA gebaut?

Wikipedia.at:

Totmannschaltungen dienen der Arbeitssicherheit an Einzelarbeitsplätzen oder an gefährlichen Maschinen und sind häufig gesetzlich, zumindest aber versicherungsrechtlich vorgeschrieben. Sie reagieren auf Bewegungslosigkeit, waagerechte Körperlage (Totmanneinrichtung) oder Schlaf oder sie lösen beim Loslassen aus…

Vielleicht sollte man Art 32 DSGV als generelle IT-Norm einführen?

Art. 32 DSGVO Sicherheit der Verarbeitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Vielen Dank für Ihre Aufmerksamkeit!

RA Dr. Rainer Knyrim

Knyrim Trieb Rechtsanwälte OG

1060 Wien, Mariahilfer Straße 89A

Tel. +43/1/9093070, Fax +43/1/9093639

Email ky@kt.at

www.kt.at