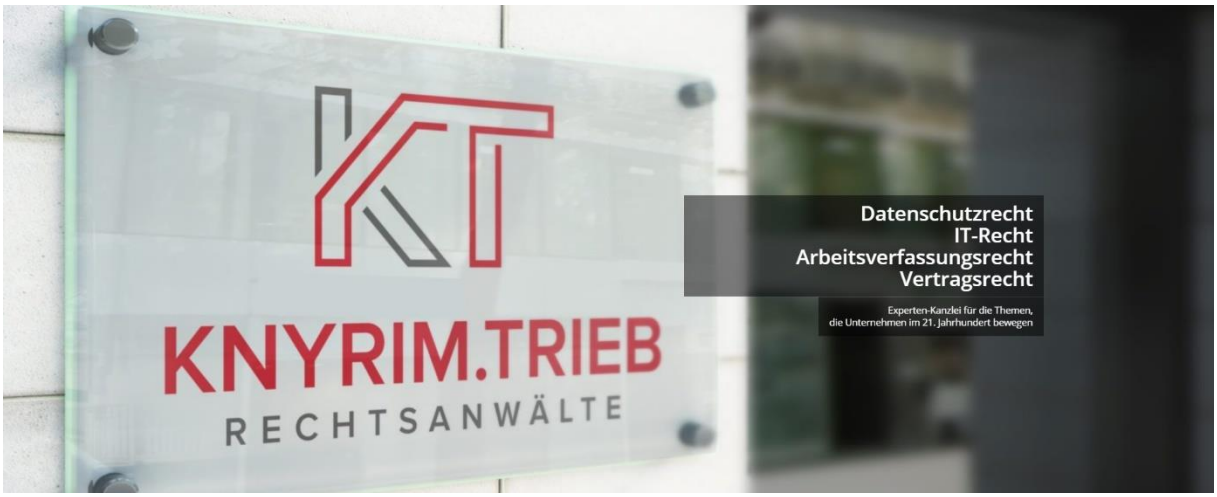

Newsletter Nov 2019
Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!
Liebe Datenschutzinteressierte!

Konferenz der Datenschutzbehörden in Tirana

Jedes Jahr treffen sich die Datenschutzbehörden aus aller Welt zu einer Jahreskonferenz, um aktuelle Themen zu besprechen und Resolutionen zu fassen. Die Konferenz findet jedes Jahr in einem anderen Land auf Einladung dieses Landes statt. Heuer fand die 41. International Conference of Data Protection and Privacy Commissioners Ende Oktober in Tirana, der Hauptstadt Albaniens statt.

Bild1: In der Eingangshalle des Kongresspalastes von Tirana

Bild 2: Der Premierminister von Albanien, Edi Rama eröffnet die Konferenz

Eröffnet wurde die Konferenz – und das zeigt die Bedeutung derselben für das Land – von Edi Rama, dem Premierminister von Albanien. Der sprach in seiner Rede auf witzige und sehr offene Art und Weise gleich an, was viele Konferenzteilnehmer sich vielleicht dachten, als sie zum ersten Mal im Leben in Albanien ankamen: Wird man beim Verlassen des Flughafens gleich überfallen? Oder erst beim Aussteigen aus dem Taxi vor dem Hotel? Ist Albanien vielleicht noch immer das „Nordkorea Europas“? Der Premierminister zerstreute die Ängste und versicherte, dass die Konferenzteilnehmer auch am Abend in Tirana alleine sicher ausgehen können, weil Gastfreundlichkeit bei den Albanern über Allem steht. Und nach und nach mussten ihm die Konferenzteilnehmer beipflichten, denn Tirana verfügt tatsächlich über ein sehr nettes Ausgehviertel, in dem man in stylischen Lokal bei guten Cocktails bis spät in die Nacht über Datenschutzrecht plaudern kann.

Aber zunächst zum Inhalt der Konferenz:

Bild 3: Brad Smith, Präsident von Microsoft, zeigt wie „die Cloud" tatsächlich aussieht.

Höhepunkt der Konferenz war der Auftritt von Brad Smith, dem Präsident und Chief Legal Officer von Microsoft. Er zeigte zunächst ein kurzes Video, in dem er mit einem ehemalige DDR-Bürger in einem früheren DDR-Gefängnis spricht, in dem dieser zweieinhalb Jahre eingesperrt war, weil er dabei erwischt wurde, wie er Flugzettel mit verpönten politischen Botschaften heimlich am Abend auf der Straße verteilt hatte. Brad Smith erklärte, dass er dieses Video Micrsosoft-Mitarbeitern auf der ganzen Welt zeige, damit diese verstehen, warum den Europäern Datenschutz so wichtig sei. Er verglich das Verteilen der Flugzettel mit dem Senden von Emails und meinte, dass es deshalb so wichtig sei, Daten zu schützen.

In der Folge verdeutlichte er, dass es „die Cloud", in der heute immer mehr Korrespondenz und Daten gespeichert würden, nicht gibt, sondern diese einfach nur aus riesigen Rechenzentren bestünde, die es zu sichern gelte. Eine Aufgabe, die Microsoft – natürlich – sehr ernst nehme.

Sehr interessant waren die Zahlen, die Brad Smith dann zur DSGVO zeigte:

Bild 4: Brad Smith von Microsoft zeigt aus welchen Ländern wie viele Anfragen von Betroffenenrechten nach DSGVO an Microsoft gestellt wurden

Microsoft hat ausgewertet, wie oft ihnen gegenüber Betroffenenrechte nach der DSGVO geltend gemacht wurden und aus welchem Land die Betroffenen kamen, die diese gelten gemacht hatten. Spitzenreiter war wider Erwarten keineswegs ein EU-Land, sondern zunächst die USA mit 6,7 Mio Anfragen, dann Japan mit 1,4 Mio Anfragen und erst an dritter und vierter Stelle England und Frankreich, gefolgt von Kanada, Brasilien, Deutschland und China. Unter den 10 Ländern mit den meisten Anfragenden waren gerade einmal zwei aus der EU, obwohl eigentlich für diese die Betroffenenrechte von der EU geschaffen wurden.

Dies heißt aber nicht, dass seitens EU-Ländern keine Anfragen kamen, denn aus EU-Ländern dürften insgesamt rund 4 Mio Anfragen gestellt worden sein, dh fast jeder 50. EU-Bürger hat alleine gegenüber Microsoft hinsichtlich seiner Datenverarbeitungen DSGVO-Rechte geltend gemacht! Die Aufstellung zeigt aber auch, dass der Bedarf an Regelungen und Angeboten zu Betroffenenrechten auch auf allen anderen Kontinenten sehr hoch zu sein scheint und die DSGVO daher kein abstraktes und sinnentleertes Konstrukt ist, sondern tatsächlich den Wünschen der Bevölkerung entspricht, und zwar nicht nur in der EU, sondern weltweit und damit ein sehr einflussreiches „Vorzeigemodell" ist, dem wohl noch viele Staaten folgen werden. Nicht überraschend rief Brad Smith daher dazu auf, Zusammenzuarbeiten, um in der nahen Zukunft einen globalen „Datenschutzpakt" zu schaffen.

Weiterer Höhepunkt der Konferenz war eine von der Leiterin der österreichischen Datenschutzbehörde und Vorsitzenden des Europäischen Datenschutzausschusses geleitetet

Podiumsdiskussion mit den Leitern der Datenschutzbehörden von Frankreich und Kanada, der globalen Datenschutzbeauftragten von Mastercard sowie Vertretern zweier Datenschutz-NGOs zum Thema Verantwortlichkeit. Diskutiert wurde dabei, wie die Kluft zwischen der Erwartungshaltung der Datenschutzbehörden und den verantwortlichen Unternehmen überbrückt werden kann und ob und wie die Verantwortlichkeit skalierbar und flexibel gestaltet werden kann und dennoch hohe Standards auch bei KMUs und Start-ups gesichert werden können.

Bild 5: Dr. Andrea Jelinek (ganz rechts) moderiert die Podiumsdiskussion zum Thema Verantwortlichkeit

Besonders interessant waren dabei die Einblicke, die der Datenschutzkommissar von Kanada, Daniel Therrien in von seiner Behörde geführten Verfahren gab: So habe man nach einem Data Breach bei der Equifax mit 147 Millionen Betroffenen festgestellt, dass dort überhaupt kein Accountability Framework implementiert war. Auch Facebook habe man nach dem Cambridge Analytica – Vorfall untersucht und festgestellt, dass zwar Policies vorhanden waren, diese aber zum Teil widersprüchlich waren und im Detail nicht perfekt, dass aber das eigentliche Problem die fehlende interne Kontrolle gewesen sei.

Eine weitere Podiumsdiskussion wurde von Trevor Hughes, dem Gründer der International Association of Privacy Professionals (IAPP) zu den künftigen Herausforderungen der Datenschutzbehörden und Datenschutzbeauftragten geführt, die hier nachgelesen werden kann: **Full Story**

Der erste Teil der Konferenz ist traditionell nicht der allgemeinen Öffentlichkeit zugänglich, dort werden aber immer Resolutionen von den Datenschutzbehörden verabschiedet, die dann öffentlich abrufbar sind. Die Resolutionen der heurigen Konferenz, die ua grenzüberschreitende Kooperation zwischen den Behörden bei der Exekution des Datenschutzrechts, aber auch die Rolle des menschlichen Fehlers bei Data Breaches und Gegenmaßnahmen gegen dieses Problem betrafen, sind hier abrufbar: https://privacyconference2019.info/closed-session-documents/.

Nach Abschluss der Konferenz bot sich noch die Gelegenheit, für ein paar Stunden Tirana zu erkunden. Abgesehen vom eingangs erwähnten Ausgehviertel bietet die Stadt eine geradezu einzigartige Mischung einerseits aus immer noch aktiv genutzten Gebäuden aus der Isolationszeit unter Diktator Enver Hoxha, die aus den achtziger Jahren stammen, aber eher an die 50er bis 70er-Jahre erinnern, wie etwas der Kongresspalast selbst, in dem die Konferenz stattfand, oder dem Nationalmuseum mit seinem heute bizarr anmutenden Mosaik über dem Eingang, oder dem Kulturpalast, der heute die Oper beherbergt. Anderseits gibt es (wenige) übrig gebliebenen Gebäuden aus dem 19. Jahrhundert im Stadtzentrum und einige ganz neue Bürohäuser und Hotels. Attraktion sind auch die Bunker, von denen der Diktator fast 200.000 im ganze Land aus Angst vor ausländischen Angriffen bauen ließ, zum Teil direkt im Stadtzentrum. Auch der ehemalige Regierungsbunker mit 180 Räumen auf mehreren Etagen in einem Berg am Stadtrand ist zugänglich und enthält nicht nur das originale Bunker-Arbeits- und Schlafzimmer von Enver Hoxha, sondern auch ein unterirdisches Parlament, das auch als Theater- oder Kinosaal benutzt werden kann, zu dem sich der Diktator bei einem Besuch in Nordkorea inspirieren ließ.

Die Konferenzteilnehmer waren jedenfalls von der Stadt Tirana sehr positiv überrascht und freuten sich über die Gastfreundlichkeit insbes. der Behördenmitarbeiter, die die beschränkten finanziellen Mittel durch ihren monatelangen persönlichen Einsatz für die Planung und Durchführung der Konferenz bestmöglich kompensierten. Ich persönlich kann nur empfehlen, sich diese Stadt und dieses

Land anzusehen, denn es erscheint einem zwar mental sehr fern, ist aber in weniger als 90 Flugminuten zu erreichen.

Hier noch ein paar Eindrücke aus der Stadt:








PriSec – das Jahresforum für Privacy und Security am 12. und 13. November in Rust

Das Privacy & Security Jahresforum von BusinessCircle findet heuer wieder in Rust am Neusiedlersee statt.

Highlights heuer sind ua zur Eröffnung ein Gespräch zwischen mir und dem Roboter „Pepper“ zum Thema Datenschutz und im Anschluss daran ein Vortrag von Clemens Wasner von Enlite AI zur Frage,

was die Verschmelzung von Mensch und Maschine für Privacy und Cyber Seucrity bedeutet, eine Keynote von Herrn Univ.-Prof. Nikolaus Forgo zu Datenschutz. Dateneigentum. Datensouveränität. und eine weitere Keynote von mir zum Thema „18 Monate DSGVO - Highlights und Trends“.

Ein Impulsvortrag von Mag. Manfred Spanner MSc, Head of Department Group Data Protection Office OMV AG wird gefolgt von einem Talk mit ihm, Michael Mrak, Leiter der Abteilung Compliance der Casinos Austria, sowie Sergey Obolensky, Executive Director Corporate Sales, Risk Management Partners bei Munich Re über Organisationsstruktur bis Finanzierung von Security und Datenschutz im Unternehmen.

Am Nachmittag des 1. Tages gibt es mehrere parallele Sessions ua zu Tools im Datenschutzrecht, Whistleblowing & Datenschutz, E-Mail-Handhabung unter der DSGVO im Unternehmen gefolgt von einer Q&A-Session zum Thema „Cyber Attacks and Data Breaches – Lessons Learned“.

Der zweite Tag wird mit einer Keynote von Max Schrems zu „Utopie Privatsphäre“ eröffnet, der darauf mit Anna Pouliou von Chanel und Marco Ratzmann von OneTrust über „Surveillance, Social Profiling, Citzen Scoring - im Visier von Big Tech und Geheimdiensten?“ diskutiert.

Ein weiteres Highlight am zweiten Vormittag wird ein Vortrag von und Interview mit dem stellvertretenden Leiter der Datenschutzbehörde, Dr. Matthias Schmidl über die Prüfpraxis und Sanktionen der Datenschutzbehörde sein. Es ist anzunehmen, dass dabei die im Oktober von der Datenschutzbehörde verhängte Strafe von EUR 18 Mio gegen die österreichische Post AG angesprochen wird.

Den Rest des Tages gibt es weiter parallele Sessions ua zum Management von Lieferantenrisiken, der Verwendung von WhatsApp im Unternehmenskontext, eine Case Studies zu Whistleblowing und risikobasiertes Datenschutzmanagement und Konzepte und Tools für Awarenessbildung und Schulung im Unternehmen sowie OT Security – Datenschutz und Geheimnisschutz in der Industrie.

Abschluss der Konferenz bildet eine Keynote zu Cyberangriffen, Industriespionage & dem fahrlässigen Umgang mit Daten von Walter Unger, dem Leiter des Cyber-Verteidigungszentrum des Österreichischen Bundesheers.

Beliebt ist die PriSec bei den wieder über hundert Teilnehmern nicht nur wegen der inhaltlichen Vorträge, sondern auch wegen der Möglichkeit, am Abend des 1. Tages während des Abendessens und danach an der Bar interessante neue Kontakte im Datenschutzrecht zu knüpfen und bei Wein und Musik über Datenschutzrecht in der Praxis zu plaudern, bis der letzte Bus zurück ins Hotel fährt.

WICHTIGER HINWEIS

Ich konnte mit BusinessCircle aushandeln, dass **Leser dieses Newsletters** sich mit einem Last-Minute-Preis zur PriSec anmelden können: Geben Sie bei der Online Buchung (https://businesscircle.at/datenschutz/konferenz/prisec-privacy-security/anmeldung/) die Referenz „KNY“ an und Sie erhalten EUR 200,-- Rabatt auf den Konferenzpreis, die somit für Praktiker statt EUR 990,-- nur 790,-- kostet.

Das volle Programm der PriSec finden Sie hier:
https://businesscircle.at/datenschutz/konferenz/prisec-privacy-security/#programm

Ein Rückblick zur letzten Konferenz findet sich unter:
https://businesscircle.at/datenschutz/konferenz/prisec-privacy-security/#rückblick

Österreichische Datenschutzbehörde verhängt EUR 18 Millionen Strafe gegen Österreichische Post AG

Die Datenschutzbehörde hat in einer Presseaussendung am 29.10.2019 bekannt gegeben, dass sie gegen die Österreichische Post AG eine Verwaltungsstrafe von EUR 18 Mio verhängt hat. Grund war laut dieser Presseaussendung, dass die Post durch die Verarbeitung von personenbezogenen Daten über die vermeintliche politische Affinität von Betroffenen gegen die DSGVO verstoßen hat. Weiters wurde u.a. eine Rechtsverletzung wegen der Weiterverarbeitung von Daten über die Paketfrequenz und die Häufigkeit von Umzügen zum Zweck des Direktmarketings festgestellt, weil dies keine Deckung in der DSGVO fände, so die Datenschutzbehörde. Die Presseaussendung kann hier eingesehen werden: https://www.ots.at/presseaussendung/OTS_20191029_OTS0095/strafverfahren-gegen-oesterreichische-post-ag

Die Strafe ist eine der höchsten in der EU und in absoluten Zahlen hoch, tatsächlich liegt sie aber „nur" knapp unter 1% des Konzernumsatzes von 1,96 Mrd EUR der Post. Betrachtet man allerdings den Gewinn der Post von EUR 165 Mio im Jahr 2018, so würde diese Strafe mehr als 10% des Gewinns „fressen". Der Gewinn spielt allerdings in der Strafzumessung nach der DSGVO keine Rolle, nur der Umsatz. Da die DSGVO einen Strafrahmen von bis zu 4% vorsieht, hätte die Strafe bis zu EUR 78 Mio betragen können. Dass die Strafe hoch sein wird, hat sich in der bisherigen Judikatur der Datenschutzbehörde zur DSGVO bereits abgezeichnet, denn auch die bisherigen Strafen gegen Einzelpersonen oder kleine Unternehmen waren im Verhältnis zum Einkommen oder Umsatz immer ziemlich streng.

Der Hintergrund des Post-Falles kann auf „addendum" nachgelesen werden: https://www.addendum.org/datenhandel/post-strafverfahren/, dort werden auch die hohen Verfahrenskosten genannt: Diese Betragen 10% der verhängten Strafe, somit 1,8 Millionen Euro. Da die Post angekündigt hat, den Instanzenzug zu beschreiten, bleibt abzuwarten, ob die Strafe grundsätzlich und wenn ja, in dieser Höhe und mit diesen Verfahrenskosten „halten" wird. Darüber, ob auch in Österreich die Datenschutzbehörde Millionenstrafen verhängen wird, gibt es jetzt aber Gewissheit: Ja, es hat nun auch bei uns geknallt. Diejenigen, die dachten, dass das Datenschutzrecht in Österreich nach dem ersten DSGVO-Hype schon wieder eingeschlafen sei, sind dadurch hoffentlich selbst wieder aufgewacht.

EUR 30.000 Strafe wegen nicht richtiger Cookie-Implementierung

Bereits im letzten Newsletter haben wir über die Gefahren nicht richtiger Cookie-Implementierung berichtet. Dass das diesbezügliche Risiko immer größer wird, zeigt nun die erste große Geldstrafe einer Aufsichtsbehörde gegen ein Unternehmen im Zusammenhang mit der Informationsverpflichtung beim Einsatz von Cookies auf der eigenen Webseite.

Eine spanisches **Unternehmen** betrieb eine **Webseite** und setzte auf dieser **Cookies diverser Drittanbieter** ein, etwa von Google Analytics, Google Doubleclick und Facebook, überdies Pixel und Beacons. Mit Aufrufen der Webseite wurde der Besucher mittels üblichem **Cookie-Banner** wie folgt informiert:

„Wir verwenden Cookies, um Ihre Präferenzen zu speichern, Nutzungsstatistiken zu erstellen und Werbeangebote basierend auf Ihren Browsing-Gewohnheiten an Sie zu senden. Wenn Sie weitersurfen,

nehmen wir an, dass Sie deren Verwendung akzeptieren. Weitere Informationen diesbezüglich erhalten Sie in unseren Cookie-Bestimmungen.“

Daneben befand sich eine Schaltfläche mit dem Text *„Akzeptieren und weitersurfen“.* Es wurde auch auf die eigenen Cookie-Bestimmungen verwiesen.

Dies hat die **spanische Aufsichtsbehörde** als unzureichend bemängelt, da die Webseitenbesucher keine Möglichkeit hatten, auf das Setzen oder Auslesen der Cookies einzuwirken. Die Behörde erließ gegen das Unternehmen in weiterer Folge einen **Strafbescheid in Höhe von 30.000 Euro**.

Die spanische Aufsichtsbehörde hielt den bloßen Verweis auf Browsereinstellungen oder „do-not-track“ Blocking-Tools zur Verhinderung des Setzens oder Auslesens von Cookies als nicht ausreichend, um eine entsprechende Verarbeitung durch den Webseitenbetreiber zu rechtfertigen. Dieses Vorgehen stelle zwar eine komplementäre, jedoch keinesfalls hinreichende Information des Webseitenbesuchers dar.

Die Behörde hielt weiters fest, dass **Verantwortliche** ein **Managementsystem** oder eine andere **Konfigurationsmöglichkeit zur Verwaltung** der von ihnen gesetzten Cookies implementieren müssen, welches dem Webseitenbesucher **das granulare und generelle Auswählen oder Abwählen beziehungsweise Löschen der Cookies ermöglicht.**

Erneut daher von uns der dringende Rat, sich mit der Cookie–Implementierung auf der Webseite auseinanderzusetzen und dafür zu sorgen, dass Cookies erst nach einer aktiven Handlung implementiert werden und es eine **Ein/Ausschaltmöglichkeit für Werbe- und Trackingcookies** gibt.

Mit freundlichen Grüßen

Rainer Knyrim

Erfahren Sie mehr zu aktuellen Veranstaltungen auf unserer Webseite: www.kt.at/veranstaltungen

---

Knyrim Trieb Rechtsanwälte OG

Mariahilfer Straße 89a, A-1060 Wien, T: +43 1 909 30 70, F: +43 1 909 36 39
FB: knyrimtrieb E: ky@kt.at, W: www.kt.at

FN 462250f, HG Wien