Interview mit Marit Hansen

Datenschutz als Vorteil auf dem Weltmarkt

Marit Hansen ist Landesbeauftragte für Datenschutz Schleswig-Holstein. OBJEKTspektrum führte mit der Informatikerin ein virtuelles Interview unter anderem über die Datenschutz-Grundverordnung (DSGVO) und damit konforme Start-up-Ideen.

Johannes Mainusch: Marit, du bist seit drei Jahren Datenschutzbeauftragte des Landes Schleswig-Holstein. Dein Vorgänger war Thilo Weichert. In seiner Amtszeit erschien Schleswig-Holstein als das strengste Datenschutz-Bundesland in Deutschland. Bist du auch so streng?

Marit Hansen: War Thilo Weichert besonders streng? Wir machen es wie immer: Es gilt das Datenschutzrecht. Und das wenden wir an. In Schleswig-Holstein hatten wir allerdings ein ganz besonderes Instrument: die Zertifizierung. Datenschutzgerechte Lösungen konnten ein Gütesiegel erhalten. Wir haben nicht nur auf Sanktionen gesetzt, sondern auch auf das Fördern guter Lösungen. Dafür braucht es ein klares Bekenntnis – nicht nur schwammige Aussagen oder „Es kommt darauf an". Mit der DSGVO soll übrigens in ganz Europa verstärkt auf Zertifizierung gesetzt werden.

„Wir sind lösungsorientiert und begreifen neue Technik eher als willkommene Herausforderung"

Jedenfalls hat das ULD – das Unabhängige Landeszentrum für Datenschutz – dieses Image bekommen, nicht nur streng, sondern auch sehr kompetent zu sein ...

Ich bin selbst Informatikerin, und wir haben hier vergleichsweise viele, die im Technikbereich, also Informatik, Mathematik oder Wirtschaftsinformatik, ausgebildet sind. Daher führen wir viele Diskussionen nicht nur juristisch, sondern gleich interdisziplinär. Wir sind lösungsorientiert und begreifen neue Technik eher als willkommene Herausforderung denn als Bedrohung. Einerseits, um neue Risiken zu identifizieren, andererseits, um neue Lösungsmöglichkeiten kennenzulernen und diese dann auch bekannt zu machen,

Wie viele seid ihr denn beim ULD?

Im Augenblick haben wir 32 Stellen. Außerdem haben wir einen Bereich, der mit Drittmittelförderung finanziert ist, in Summe sind wir etwa 40 Kollegen.

Nicht jedes Bundesland hat so viele Mitarbeiter in der Aufsichtsbehörde für Datenschutz, oder?

In 2018 sind einige der anderen Aufsichtsbehörden ganz schön gewachsen. Wir allerdings nicht. Ich hoffe auf Zuwachs im Laufe des Jahres. Aber einige Aufsichtsbehörden sind auch ganz klein geblieben. Einige spezielle Aufgaben waren uns vom alten Landesdatenschutzgesetz aufgegeben, beispielsweise die Zertifizierung, Beratungen und Schulungen, unter anderem zum Selbstdatenschutz der Bürgerinnen und Bürger. Außerdem sind wir selbst für unsere Technik verantwortlich. Das bedeutet, dass wir unsere Aktenhaltung und unsere Internetanbindung selbst realisieren. Wir betreiben unsere IT also getrennt von der Landes-IT, unsere digitalen Daten sind von dort aus nicht zugreifbar. Das wäre in unserem Selbstverständnis der Unabhängigkeit ein No-Go.

„Für mich ist Cloud kein No-Go"

Spannend! … Aber dann könntet ihr doch auch in die Cloud gehen, so wie alle anderen Unternehmen das demnächst machen?

Wenn wir eine sichere, vertrauenswürdige, überprüfbare Cloud hätten, bei der kein Unbefugter auf unsere Daten zugreifen und uns beobachten kann – denn Informationen über unsere vertraulichen Prüfungen oder Strategien sollen nicht in falsche Hände gelangen. Wir haben uns in Multi-Cloud-Projekten mit verschiedenen Arten der Verschlüsselung, Datentrennung und Nachweisbarkeit der Zugriffsmöglichkeiten beschäftigt – sehr gute Ansätze! Für mich ist Cloud kein No-Go, allerdings sind kostenlose Public Clouds mit dubiosen Geschäftsmodellen tabu.

Also dass zum Beispiel jetzt unser Interview in einem google.doc landet auf einem google drive ...

Kein Problem, unser Interview soll ja öffentlich werden. Allerdings würde ich über solche fremdbetriebenen Dienste keinen vertraulichen Projektantrag vorbereiten, natürlich keine personenbezogenen Daten über Kunden oder Bürger hochladen und schon gar keine Unternehmens-

oder Behördenstrategie besprechen. Für solche Angebote wären wir auch sicher kein Referenzkunde.

Ja, für einen Cloud-Provider wäret ihr eine super Referenz.

Richtig. Als ULD haben wir Verständnis für eine Cloud-Nutzung für öffentliche Daten. Allerdings haben die Beschwerden von Petentinnen und Petenten, denen wir nachgehen, und auch die Argumente der Unternehmen, die geprüft oder angehört werden, in der Öffentlichkeit oder auch bei der Konkurrenz nichts zu suchen. Daher nutzen wir derzeit keine Cloud.

„Wir vermeiden generell solche Dienstleister, auf deren Daten die Behörden aus anderen Staaten zugreifen“

Beschwerden, die etwa gegen Amazon bei euch vorliegen, die wolltet ihr dann nicht bei AWS speichern ...

Genau. Es ist klar, dass wir generell solche Dienstleister vermeiden, auf deren Daten die Behörden aus anderen Staaten zugreifen. Ich habe ein großes Interesse an guten und sicheren Cloud-Diensten in unserer nationalen oder auch in europäischer Souveränität. Bislang ist das nicht richtig auf die Füße gekommen. Ich hatte gehofft, die Datenschutz-Grundverordnung gibt da einen schnellen Push, weil sich dann ja alle an dasselbe Recht halten müssen. Aber es befolgen trotzdem noch lange nicht alle dieselben Regeln. Also noch kein “level playing field”, da müssen wir jetzt noch ran.

Was meinst du mit Datenschutz-Grundverordnung und “level playing field”?

Der 25. Mai 2018 bedeutet für alle, die in Europa Geschäfte machen wollen, dass sie sich an das Recht der EU und die Europäische Datenschutz-Grundverordnung halten müssen. Ich hatte gehofft, dass bis zum 25. Mai dann auch die Geschäftsmodelle der Unternehmen dem Datenschutz angepasst wurden, dass die Rechtsgrundlagen korrekt sind, dass unzulässige Zugriffe vermieden und am besten technisch ganz ausgeschlossen werden. Die Datenschutz-Grundverordnung enthält ja wichtige Vorgaben zur Technikgestaltung: Artikel 32 zur Sicherheit und Artikel 25 zu Datenschutz by Design & by Default. Das müssen alle umsetzen.
Außerdem habe ich erwartet, dass Anwender, also Unternehmen, Behörden oder auch Privatpersonen, die notwendigen Informationen bekommen, um erkennen zu können, wie ihre Daten verarbeitet werden, wo die Risiken liegen und wie sie diese Risiken in den Griff bekommen.

„Meine Hoffnung hat sich bisher nicht erfüllt, dass die Produkte schon gleich datenschutzkonform gebaut sind“

Stattdessen haben die großen Unternehmen gemacht, was sie immer machen: behaupten, dass alles datenschutzmäßig im grünen Bereich ist. Und dann abwarten, ob sich jemand beschwert oder vor Gericht geht – das dauert Jahre, so mag mancher Global Player auf Zeit spielen. Die KMUs hingegen haben einfach nur große Angst bekommen, was ihnen nun von Aufsichtsbehörden oder Abmahnanwälten droht.
Meine Hoffnung hat sich also bisher nicht erfüllt, dass die Produkte schon gleich datenschutzkonform gebaut sind, sodass alle Anwender sie ganz einfach einsetzen können. Zum Beispiel Betriebssysteme, Datenbanken, Kundenverwaltung, Kommunikationssysteme, Apps, Clients für Mail und sonst was, einfache Produkte, bei denen auch gleich einfach klar ist: „Dieses Produkt ist datenschutzkonform.”

Ist das nicht ein Problem der doppelt mangelnden Kompetenz? Zum einen verstehen Unternehmen Datenschutz gar nicht und zum anderen sind sie doch häufig gar nicht in der Lage, ihre IT wirklich substanziell zu ändern. Und dann kann man mit Datenschutzkonformität auch kein Geld verdienen ...

Es müssen sich alle gleichermaßen an die DSGVO halten. Derjenige, der sich nicht daran hält, müsste einen Nachteil haben. Wenn DSGVO-Compliance ein Kriterium bei der Auswahl von Produkten und Dienstleistung ist, haben die Unternehmen mit DSGVO-konformen Angeboten einen Vorteil im Wettbewerb. Ihre Lösungen sollten für Kunden einfach in die Unternehmens-IT integrierbar sein, Sicherheit und Datenschutz wären eingebaut, Risiken wären transparent, die notwendige Dokumentation wäre gleich mit dabei. Die Kunden erhalten maximale Unterstützung, keiner muss das Rad ständig neu erfinden.

Zum Beispiel wäre ein Subdienstleister in der Auftragsdatenverarbeitung im Vorteil, wenn er mir die Prüfung alle zwei Jahre so erleichtern wurde ...

Also von zwei Jahren steht konkret nichts in der DSGVO, aber es stimmt, man muss sich regelmäßig vergewissern, dass Subdienstleister mit Auftragsdatenverarbeitung DSGVO-konform agieren. Zwei Jahre ist bestimmt keine schlechte Zeit. Aber was macht man denn normalerweise? Man überlegt, was möchte man, und dann überlegt man die verschiedenen Qualitäten, die auf dem Markt vorhanden sind.
Im öffentlichen Dienst müssen wir bei IT-Projekten genau wie Firmen bei großen Vorhaben eine Ausschreibung starten. In Sachen DSGVO müssten jetzt alle, die hier anbieten wollen, bestimmte Qualitäten in Funktionalität, Absicherung und Dokumentation schon standardmäßig mitbringen. Die Unternehmen und Behörden als Verantwortliche müssen ihre Arbeit ordentlich machen und diese Verantwortung bewusst übernehmen, denn letztlich sind sie für die personenbezogenen Daten und die Verarbeitung verantwortlich und sollten sich bei ihren Subunternehmern vergewissern, dass die alles ordentlich machen. Jeder Verarbeiter muss halt wissen, was mit den Daten passiert.
Aber das ist doch normal: Auch wenn ich irgendwo Papier lagere, muss ich wissen, wer Zugriff darauf hat. Wenn ich Aufbe-

Marit Hansen

noch keine 50 Jahre alt

Aufgabe: Landesbeauftragte für Datenschutz Schleswig-Holstein

Lieblingsstrategie: Gemeinsam ist man stärker – im interdisziplinären Austausch

Superkraft: Begeisterung für Lösungen mit eingebautem Datenschutz

Größtes Lernfeld: mit 24 Stunden am Tag auskommen und Life-Work-Balance

Überzeugung: Das Bessere ist der Feind des Guten

Was ich noch sagen wollte: Datenschutz ist wie Passivraucher-Schutz, denn wenn die Person neben mir Daten von sich preisgibt, kann es mich auch betreffen

wahrungsfristen einhalten muss und es kommt der Steuerprüfer, hilft es wenig, wenn man sagt: „Das ist mir jetzt zu komplex gewesen, ich hab das einfach nicht gemacht."

„Die DSGVO hat die durchaus problematische Eigenschaft, dass sie recht abstrakt gehalten ist"

Also wäre deine Hoffnung bei der DSGVO, dass die Erfüllung dieser Qualität für Lieferanten von Unternehmen dann auch so etwas wie ein positives Differenzierungsmerkmal wird?

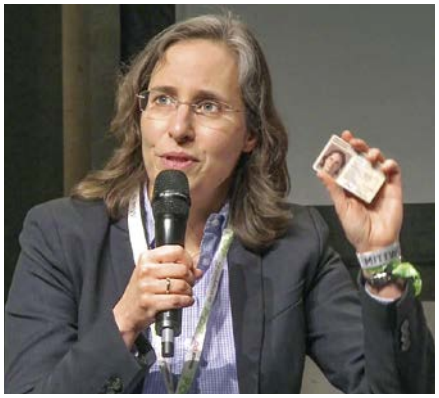
Genau! Wie eine rote Linie: Darunter geht es nicht – alle, die Datenverarbeitung anbieten, müssen DSGVO können. Und dann über die Zeit mit mehr technischem Fortschritt besser werden, den Stand der Technik weiterentwickeln.
Die Datenschutz-Grundverordnung hat aus Sicht der Engineers die durchaus problematische Eigenschaft, dass sie recht abstrakt gehalten ist. Man liest den Text und hat eine gewisse Idee, aber doch nicht ganz genau, wie man einen Prozess aufsetzen oder eine technische Komponente implementieren soll.
Das ist aber weniger ein Bug als ein Feature: Weil wir im IT-Bereich so schnelle Entwicklungszyklen haben und diese Grundverordnung für einige Jahrzehnte halten soll, muss die DSGVO eine gewisse Abstraktheit haben. Für die konkreten aktuellen Situationen muss man auf dieser Basis weiter spezifizieren. Etwa: Wo kann man sinnvoll Verschlüsselung oder Pseudonymisierung einbauen und welche Verfahren sind für den Anwendungsfall geeignet?
Resilienz ist eine neue Anforderung in der DSGVO: Wie lassen sich Systeme bauen, die unempfindlicher sind gegen unvorhergesehene Störungen und Angriffe und die für den Fall, dass doch so ein Ereignis eintritt, schnell wieder funktionieren? Das ist in einem Unternehmensnetz wahrscheinlich relativ einfach, betrifft aber auch beispielsweise autonome Fahrzeuge. Ganz allgemein gesagt: Wie bauen wir unsere zunehmend digitalisierte Welt, die verlässlich und vertrauenswürdig sein muss?

Diese Abstraktheit ist also wünschenswert, damit die Verordnung langlebig ist.

Genau. Auf Prinzipienebene ist die DSGVO gegenüber dem vorherigen deutschen Datenschutzrecht großenteils gleich geblieben, das betrifft auch die meisten Verpflichtungen. Geändert haben sich vor allem das Bewusstsein und die Einsicht, handeln zu müssen.

Und wahrgenommen sind meine Verbraucherrechte größer geworden?

Ja, ein wenig schon. Es muss mehr über die Datenverarbeitung informiert werden, und das muss verständlich geschehen. Die Betroffenenrechte, beispielsweise Auskunft zu den eigenen personenbezogenen Daten oder Ansprüche auf Berichtigung oder Löschung, gab es vorher auch schon, waren aber kaum bekannt.
Neu ist die Datenportabilität für Daten, die ich selbst bereitgestellt habe. Wenn ich von einem sozialen Netzwerk in ein anderes umziehen möchte oder von einer Cloud in die andere, habe ich das Recht, meine personenbezogenen Daten mitzunehmen.



CC BY-SA 3.0 de, re:publica 2018

„4 Prozent des Vorjahresumsatzes, das ist natürlich eine erhebliche Erweiterung des Bußgeldrahmens"

Ach cool! Und es gibt, glaube ich, drakonischere Strafen für Zuwiderhandlungen, weshalb jetzt alle Unternehmen ein bisschen aufgescheucht sind?

Genau, das war ganz zentral in der Berichterstattung. Geldbußen von 20 Millionen Euro oder 4 Prozent des Vorjahresumsatzes, das ist angesichts der vorherigen maximalen Buße von 300.000 € im Bundesdatenschutzgesetz natürlich eine erhebliche Erweiterung des Bußgeldrahmens.
Eigentlich richtet sich das aber an die ganz großen und ganz schweren Fälle. Beispielsweise wenn ein Datenverarbeiter, der absichtlich mit einem datenschutzwidrigen Geschäftsmodell Schindluder treibt, alle möglichen sensiblen Informationen über Menschen missbräuchlich nutzt, Zugriffe nicht im Griff hat oder sogar gezielt Unberechtigten ermöglicht und dann bei der Aufklärung durch die Aufsichtsbehörden nicht kooperiert und sein Verhalten verschleiert. In einem solchen schweren Fall hat ein Unternehmen alles vorsätzlich falsch gemacht, dann sollen die ganz hohen Bußgelder greifen.
Aber Bußgelder sind ja rückwärtsgewandt: Man hat etwas falsch gemacht und dann entrichtet man dafür das Bußgeld. Wie bei der Radarkontrolle.
Viel Interessanter finde ich die Sanktionen, die anders aufgebaut sind als ein Bußgeld. Die Aufsichtsbehörde kann beispielsweise mit Wirkung für die Zukunft anordnen, dass bestimmte Verarbeitungen geändert werden oder unterbleiben müssen.

Das heißt, das ist auch einer der Gründe, warum ihr mehr Experten in der ULD haben müsst, um solche Sachen dann auch behandeln zu können?

Richtig. Wir wollen uns die Verfahren genau anschauen und verstehen, welche Änderungen nötig sind, um sie datenschutzkonform zu machen. Zum Beispiel arbeiten wir im Bereich Videoüberwachung mit Screenshots der eingesetzten Webcams und zeigen den Betreibern genau in diesen Bildern, was eine Webcam aufzeichnen darf und was nicht. Was zum Beispiel nicht erlaubt ist, ist die Webcam am Strand, mit der man reinzoomen kann, wenn junge Damen sich umziehen. Auch kann man ganze Bereiche ausblenden oder automatisiert „blurren", die Winkel, Bewegungen oder Zeiten der Aufzeichnung geschickt datenschutzkonform konfigurieren.

Ah, okay. Jetzt möchte ich dich ganz kurz um Kommentare aus Sicht der Datenschutzbehörde für drei Start-up-Ideen bitten. Erstes Start-up: Ein Start-up fotografiert Klingelschilder ab und liest diese per Texterkennung aus, verknüpft sie mit den geografischen Daten und stellt das öffentlich im Netz dar. Wäre das Okay?

Klingelschilder zeigen Besuchern eines Hauses an, wer dort in welcher Wohnung wohnt. Um die Schilder lesen zu können, müssen die Besucher tatsächlich vor der Tür stehen. Die digitale Bereitstellung im Internet entspricht nicht den Erwartungen der Bewohner. Es fehlt die Rechtsgrundlage: Möglich wäre es, wenn das Start-up einen Vertrag mit den Bewohnern schließen oder eine Einwilligung einholen würde.
Man kann noch überlegen, ob es sich beim Online-Stellen der Daten um ein berechtigtes Interesse des Start-ups han-

delt, muss aber gleichzeitig prüfen, ob entgegenstehende Interessen oder Rechte der Bewohner überwiegen – davon kann man wohl in diesem Fall – faktisch ein weltweit zugreifbares Wohnungsregister – ausgehen.
Vielleicht noch eine einfache Prüffrage für ein Start-up, die so nicht im Datenschutzrecht steht, aber doch etwas über Interessen und Rechte von betroffenen Personen aussagt: Kann man einen Shitstorm erwarten?
Übrigens zeigt die Regelung in Artikel 25 (2) DSGVO, dass ein Zugänglich-Machen einer unbestimmten Zahl von natürlichen Personen nicht der Standard sein darf. Weil dies nämlich ein Risiko für die Betroffenen bedeutet, wenn jeder die Wohnadresse recherchieren kann und dann vielleicht ungebetene Besucher auf der Matte stehen.

Okay, kann ich nicht als Start-up-König trotzdem sagen, ich mach das einfach mal?

Wer es so ähnlich probiert hat, ist ja Google mit den Häuserfassaden und Adressinformationen. Viele Betroffene haben sich aufgeregt, und Google hat dann die Bilder verpixelt. Der Start-up-König kann aber loslegen für diejenigen, die er informiert hat und die dann einwilligen.

„Eine einfache Prüffrage für ein Start-up, die etwas über Interessen und Rechte von betroffenen Personen aussagt: Kann man einen Shitstorm erwarten?“

In meiner nächsten Start-up-Idee scanne ich Autoschilder mit einer App und stelle das öffentlich dar, das sind ja jetzt keine direkt personenbezogenen Daten.

Doch, denn zumindest auf den Halter kommt man mit einer Halteranfrage, somit ist es wieder personenbezogen. Aber selbst ohne Halteranfrage handelt es sich um eindeutige Auto-Kennungen, die sich in vielen Fällen auf denselben Fahrer beziehen. Das heißt: Personenbezug liegt vor. Deswegen dürfen Nummernschilder übrigens auch von der Polizei oder von Ordnungsämtern nur unter definierten Umständen erfasst werden. Das Bundesverfassungsgericht hat für das polizeiliche Kennzeichen-Scanning im Jahr 2008 ziemlich strikte Regelungen definiert. Demnach besteht ein Eingriff in die informationelle Selbstbestimmung, wenn ein Abgleich mit einem Datenbestand nicht unverzüglich erfolgt und das Kennzeichen nicht ohne weitere Auswertung sofort und spurenlos gelöscht wird.

Das ist aus Informatiksicht eine spannende Formulierung. Flüchtige Daten, die ganz schnell, in der sogenannten logischen Sekunde, wieder weg sein müssen. Nur wenn es in der Datenbank einen Treffer gibt, dann darf die Polizei das aufbewahren und dem nachgehen. In Dänemark ist das anders, da gibt es gesetzliche Regelungen, wonach die Polizei die Nummernschild-Daten auch bei Nichttreffern bis zu 24 Stunden aufbewahren darf.

Also haben die Dänen eine längere logische Sekunde?

Hahaha. Genau. Eigentlich geht es natürlich schon darum, dass der Zeitraum klein ist – so klein, dass keiner unberechtigt zugreifen kann. Eine 24-Stunden-Speicherung hat mit flüchtiger Datenerhebung nichts mehr zu tun. Für bestimmte Zwecke kann aber erlaubt sein, dass Nummernschilder gespeichert werden, zum Beispiel auf Basis eines Vertrags oder einer Einwilligung.
Einige Parkhaus-Betreiber wollen solche Daten verwenden. Aber auch hier ist zu überlegen, ob es nicht datensparsamer funktioniert. Bei Dash-Cams, die als Unfallschreiber eingesetzt werden, wird gerade diskutiert, welche Bedingungen an

einen rechtskonformen Einsatz zu stellen sind, zum Beispiel wann und wodurch eine Aufzeichnung ausgelöst wird, was von der Aufzeichnung umfasst ist und wie die Daten gegen unberechtigte Zugriffe gesichert werden. Jedenfalls darf es keine Daueraufzeichnung des öffentlichen Raumes geben.

„Jedenfalls darf es keine Daueraufzeichnung des öffentlichen Raumes geben“

Wenn so eine Kamera im Auto Verkehrsschilder erkennt, wie ist das dann?

Verkehrsschilder sind keine personenbezogenen Daten, gar kein Problem.

Nun kommt die dritte Start-up-Idee. Ich habe gelernt, 10 Millionen Hunde in Deutschland sind ein riesen Business-Case. Mit meinem NFC-Scanner und einer App lese ich nun die Chips der Hunde in meiner Umgebung aus, und so weiß ich, wer meine Straßen verschmutzt … Aber es sind ja nur Hunde, die ich scanne …

Schon wieder der indirekte Personenbezug. Da hängt ja meistens ein Mensch an der Leine. Oder ist als Hundehalter registriert. Also sind auch das personenbezogene Daten. Für diesen Vorschlag gilt auch die DSGVO.

Also müsste ich ein soziales Hundenetzwerk gründen, in dem sich Hunde und Besitzer registrieren, die müssten dann der Erfassung zustimmen und dann ginge das.

Ja, das ginge. Und natürlich müssten die Hundehalter dann auch kündigen und ihre Daten wieder löschen können. Es geht ja dann vielleicht nicht nur um Verschmutzung von Gehwegen, sondern um das Auffinden von weggelaufenen Tieren oder um gemeinsames Gassi-Gehen. Die Datenverarbeitung muss dann schriftlich etwa in AGB und Datenschutzbestimmungen des Unternehmens dargelegt werden. Sodass das jeder nachvollziehen kann.

Was wäre, wenn es ein Portal gäbe, in dem alle Menschen die Daten öffentlich machen könnten, die sie öffentlich machen wollen. Also wenn man in die andere Richtung geht und sagte, dass hier alles soll öffentlich über mich bekannt sein.

Kann man machen. Aber: Man muss aufpassen, dass nicht absichtlich oder versehentlich die Daten anderer preisgegeben werden, etwa die der Nachbarn oder wenn jemand seine DNA veröffentlicht und damit auch Informationen über seine Verwandten weitergibt. Hier sind noch nicht alle Grenzen ausdiskutiert – es ist vergleichbar mit dem Passivraucher-Schutz, denn wenn die Person neben mir Daten von sich preisgibt, kann es mich auch betreffen.
Das Datenschutzrecht hilft nicht wirklich weiter bei der Frage des Gruppendrucks: Wenn das fast alle machen, muss ich dann mitmachen? Wenn es doch informiert und freiwillig – wirklich? – passiert?

Gruppendruck ist ja ein Riesenthema, beispielsweise WhatsApp in der Schule mit bis zu 200 Nachrichten pro Stunde … Haben wir da nicht eine Asymmetrie zwischen DSGVO und Angebot?

Rechtlich ist es insoweit klar, dass WhatsApp der DSGVO unterliegt, denn es ist ein Angebot auf dem europäischen Markt, und es reicht schon aus, wenn damit das Nutzungsverhalten von Personen in Europa beobachtet werden kann. Komplizierter wird es deswegen, weil WhatsApp als Telekommunikationsdienst gilt. Damit gilt das Telekommunikationsrecht. Verstöße dagegen sind in Deutschland strafrechtlich verfolgbar. Hier kommt dann neben der Bundesbeauftragten für den Datenschutz auch noch die Bundesnetzagentur ins Spiel.
Außerdem gehört WhatsApp mittlerweile zu Facebook, und für den Datenaustausch zwischen diesen Diensten ist dann die irische Datenschutzbehörde zuständig, da Facebook mit seiner Niederlassung für Europa dort seinen Sitz hat.

Die Zyniker haben gesagt, Facebook sei nach Irland gegangen, weil die drei damals vorhandenen Datenschützer einfach zu wenige sind, um überhaupt etwas zu behandeln ...

Das könnte erklären, warum die Ableger der großen amerikanischen Firmen sich auf wenige Staaten konzentrieren. Dass diese Geschäftsmodelle nicht fair sind, wird immer mehr zum Thema, auch bei der Vermittlung von Medienkompetenz gegenüber Schülerinnen und Schülern. Zum Beispiel das „Bezahlen” mit den personenbezogenen Daten in Netzwerken, die anscheinend ihre detaillierten Informationen über die User nicht nur dazu nutzen, gezielt für Produkte zu werben, sondern dass Manipulationen der Menschen beim Brexit oder den amerikanischen Präsidentschaftswahlen möglich waren.

Da wurde etwas geschaffen, was mit einem fairen Geld-Ware-Austausch und ohne Tracking personenbezogener Daten gar nicht möglich wäre.

„Datenschutz soll für Fairness sorgen und dafür, dass man als Individuum einen Einfluss auf die Verwendung der eigenen Daten nehmen kann“

Ist Datenschutz nun etwas, was in Zukunft wichtiger wird, oder wird es in Zukunft ein Feigenblatt sein, das im Herbststurm der Datensammlung weggeblasen wird?

Es geht beim Datenschutz um die Wahrung der Persönlichkeitsrechte, um einen Ausgleich zwischen individueller Privatheit und der Übermacht von datenverarbeitenden Konzernen oder Staaten. Datenschutz soll für Fairness sorgen und dafür, dass man als Individuum einen Einfluss auf die Verwendung der eigenen Daten nehmen kann und nicht ein Staat oder große Firmen auf Basis massenhaft auswertbarer und verknüpfbarer Daten übermäßigen Einfluss bekommen.
Es geht auch darum, wie zukünftig unser Zusammenleben aussehen wird. Das heißt, aus meiner Sicht wird Datenschutz auch noch Jahrhunderte in der Zukunft wichtig sein. Genau wie Werte wie Fairness, Transparenz, Freiheit, Sicherheit und unsere demokratische Gesellschaft. Und diese Zukunft wollen wir mitgestalten.

Marit, vielen Dank für das Gespräch.

Fotocredits:
Markus Hansen

Das Interview führte ...

Dr. Johannes Mainusch
(johannes.mainusch@kommitment.biz)
Berater für Unternehmen, die Bedarf im Bereich IT, Architektur und agiles Management haben. Dr. Mainusch ist seit 2012 Mitglied der OBJEKTspektrum-Redaktion.