Polizei unverordnet

Die EU-Datenschutzgrundverordnung, die Polizei und die Wahrheit

> Wer in den letzten Jahren über längere Zeit Kontakt zu Menschen hatte, die personenbezogene Daten verarbeiten und Computerpresse lesen, dürfte bei ihnen wachsende Unruhe bemerkt haben. Ursache: Die Datenschutzgrundverordnung der EU, formal Verordnung (EU) 2016/679 oder kurz DSGVO, die im Mai an die Stelle des alten Bundesdatenschutzgesetzes (BDSG) treten wird. Ihr Text ist ganz anders organisiert, Gesetzgeber ist die EU, und es steht was von Knast drin, wo Leute bisher allenfalls strenge Blicke der Landesbeauftragten für Datenschutz gewöhnt waren. Wirklich: Knast für die Datensammler vom Staatschutz?

Um es gleich zu sagen: Die viel diskutierte DSGVO gilt nicht für Friedenswächter (in Panem), imperiale Sturmtruppen (unter Darth Vader) sowie „die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ (im Geltungsbereich der DSGVO). Wo kämen wir auch hin, wenn sich die Säulen der Gesellschaft, die Grundfesten staatlicher Souveränität den gleichen Regeln unterwerfen müssten wie Krankenhäuser, Landratsämter, oder Ortsgruppen der Roten Hilfe?

Letzeres ist übrigens ernst gemeint – es ist durchaus vorstellbar, dass die Staatsgewalt irgendwann auch mal mit der DSGVO gegen RH-Strukturen vorgeht. In diesem Zusammenhang möchten wir kurz get connected in RHZ 2/12 erwähnen (Archiv-Link ist unten): wer sich unsere Mahnungen dort zu Herzen nimmt, sollte auf der sicheren Seite sein.

Den Friedenswächtern dagegen hat das EU-Parlament statt der DSGVO die Richtlinie (EU) 2016/680 gegeben -- im Folgenden kurz DSR. Eine Richtlinie unterscheidet sich in der EU von einer Verordnung dadurch, dass sie nicht direkt gilt, sondern nur in nationales Recht zu überführen ist. Ein erstes Umsetzungsgesetz zur DSR, dem vermutlich viele einschlägige Landesgesetze folgen werden, ist Teil 3 des neuen Bundesdatenschutzgesetzes. Es tritt ab 25.5.2018 an die Stelle seines Vorgängers, und weil außerhalb der Friedenswächterei jetzt viel direkt in der DSGVO geregelt wird, hat sich zumindest in Aufbau und Abfolge der Regelungen viel getan. Eine direkte Konsequenz: Wir brauchen

Hilfe!

In unserem Auskunftsgenerator auf datenschmutz.de zitieren wir nämlich die jeweiligen Rechtsgrundlagen, was spätestens dann keine schlechte Idee ist, wenn mensch eine Auskunft angreifen will. Und diese Zitate werden ab 25.5. jedenfalls teilweise ins Leere zeigen. Für die Bundesbehörden kriegen wir die Aktualisierungen schon noch gebacken. Aber für jedes Land rauspopeln, wie dort DSGVO und DSR jeweils in Datenschutz- und Polizeigesetze verdaut wurden (oder noch werden?), bei der Arbeit hätten wir wirklich gerne Hilfe. Von dir! Wenn du dir etwas Arbeit in der Richtung, etwa für dein Bundesland, vorstellen kannst, rühre dich doch bitte bei uns (Kontakt unten). Und nein, wenn du es nicht machst, macht es niemand anders – also: ran an die Tasten!

In der Sache ändert sich dabei gar nicht so furchtbar viel, auch wenn die Eröffnungsansage aus Artikel 1, Abs. 2 (b) DSR zunächst recht gruselig klingt. Demnach ist Ziel der Richtlinie, dass der „Austausch personenbezogener Daten [...] nicht aus Gründen, die mit dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verbunden sind, eingeschränkt oder verboten wird“. In Wahrheit ist das aber das alte „Prinzip der Verfügbarkeit”, das schon in den Nullerjahren im Stockholm-Programm (vgl. RHZ 2/2010) herumspukte. Die nationalen Polizeien haben schnell gelernt, sich dampfenden Sicherheitsbullshit (der weiterhin legitimer Grund bleibt, Datenflüsse

zu beschränken) aus dem Hintern zu ziehen, wenn sie ihren KollegInnen nichts abgeben wollten – und wenn sie Daten verschieben wollten, waren sie auch bisher schon unbesorgt um Gesetze und Menschenrechte.

Ein paar Neuigkeiten sind aber schon zu finden. Wenig überraschend vielleicht, dass „der Gefährder" (ihr kennt ihn aus dem neuen BKA-Gesetz, RHZ 4/17) auch hier einzieht, und zwar in der Kategorisierung von Speicheropfern (§72 BDSG-neu). Demnach ist die Eingriffstiefe von Speicherungen zu staffeln gemäß der behördlichen Einstufung als VerdächtigeR einer Straftat, VerurteilteR, Opfer, sonstige Person – das können MitbewohnerInnen, ÄrztInnen, Beratende der zuständigen RH-Aktivengrupppe oder die Bäckereifachverkäuferin vor Ort sein – oder eben GefährderInnen. Letztere sind, präzise, Menschen gegen die ein „begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden".

Von solchem Schwurbel aufgeworfene erkenntnistheoretische Probleme mal beiseite: Immerhin ist das ein gewisser Fortschritt gegenüber der DSR, die in Artikel 6 noch „Gefährder" und Verdächtige einer wirklich geschehenen Straftat in einen Topf wirft. Aber bemerkenswert an der Aufzählung der Kategorien von Speicheropfern ist sowieso weniger, dass für die Gruppen verschiedene Daten gespeichert werden sollen – das macht die Polizei schon selbst so, wenn sie ihre Daten benutzbar halten will –, sondern dass die durchaus umstrittene Praxis, staatlicherseits als unschuldig eingeschätzte Menschen in Polizeidatenbanken zu speichern, ein weiteres Siegel legislativer Billigung schon im grundlegenden Text erhält -- statt wie bisher erst in ohnehin beliebig grundrechtsfernen Texten wie dem „Anti-Terror"-GDG (vgl. RHZ 1/07).

Ohne Unterschrift gültig

Neu in DSGVO und DSR sind Regeln zu Profiling. Nach den Normen ist das die automatische Berechnung „bestimmte[r] persönliche[r] Aspekte" aus Daten, die nun, zusätzlich und unverbunden neben den Regeln zu Scoring (die es schon früher gab) ein paar eigene Paragraphen bekommen hat. Verwandt mit dem Profiling und gleich daneben geregelt sind „automatische Entscheidungen".

Für Friedenswächter gilt da zunächst §54 BDSG-neu. Gedacht ist vermutlich an Strafzettel, die von Verkehrskameras ausgestellt werden, längerfristig vielleicht auch wirklich an Robocop auf seinem Motorrad. Beides ist nicht etwa verboten, braucht aber eine Rechtsvorschrift. Jedenfalls, wenn Robocops Handeln „eine nachteilige Rechtsfolge für die betroffene Person hat". Jetzt nehmt an, ihr wolltet Leute, die euer Computer als GefährderIn einschätzt, an der Zugtür filzen. Ein einfacher Trick, um die Sache mit den negativen Rechtsfolgen zu umgehen, ist folgende Regelung: „Alle werden gefilzt, nur ein paar werden vom Computer als sicher klassifiziert, die dürfen einfach so durch." So hat niemand „nachteilige Rechtsfolgen" durch den Justiz-o-maten, und niemand muss lästige Gesetze machen.

Das, was in den USA „Racial Profiling" heißt, wird im BDSG-Neu zur Verarbeitung „besonderer Kategorien", zu denen nach §46 (14) „rassische oder ethnische Herkunft" (whatever), Geschlecht, politische, sexuelle oder religiöse Orientierung, DNA- und Gesundheitsdaten gehören. Das ist, tatsächlich, ohne Qualifikation verboten. Was das in der Praxis bedeutet, bleibt abzuwarten, denn sonstige Roboterjustiz („Einzelfallentscheidungen") auf der Basis dieser „besonderen" Daten lässt §54 durchaus zu – unter Wahrung der „berechtigten Interessen der betroffenen Personen". Doof, dass der Staat unsere Interessen fast durchweg für unberechtigt hält...

License to Lie

Im Auskunftsrecht (§57) scheint sich auf den ersten Blick nicht viel zu tun gegenüber dem alten §19. In der DSGVO hingegen steht etwas von „stellt eine Kopie der personenbezogenen Daten [...] zur Verfügung", zumal „in einem gängigen elektronischen Format". Das wäre im Friedenswächter-Bereich eine großartige Neuerung, denn bisher kommen die Auskünfte gerne sehr wolkig umschrieben, und die Polizeien haben sich in aller Regel strikt geweigert, wirkliche Abzüge der Datenbank-Zeilen zu liefern, wahlweise unter Verweis auf Geschäftsgeheimnisse oder die Staatssicherheit. Bei der Umwölkung gehen regelmäßig viele Details verloren, die durchaus relevant wären für eine bürgerrechtliche Bewertung. Aber wurst: Friedenswächter sind auch von dieser DSGVO-Regel ausgenommen.

Tatsächlich neu ist aber ein Satz in Absatz 6 des §57. Dort steht jetzt, dass dem Speicheropfer die Verweigerung einer Auskunft nicht mitgeteilt werden muss, „wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 56 Absatz 2 [der übliche Odel von Staats- und öffentlicher Sicherheit und Rechtsgütern und sowas] mit sich bringen würde". Das

alte BDSG hatte an die Möglichkeit, dass Behörden lügen („wir haben nichts") noch nicht mal gedacht und nur eingeräumt, dass vielleicht die Mitteilung von *Gründen* unterbleiben könne, wenn die Staatssicherheit auf dem Spiel steht.

Wie das wirklich aussehen wird, wissen vermutlich auch die AutorInnen des Gesetzes nicht – soll die Polizei sagen „wir sagen nicht, ob wir was haben"? Wenn sie das aber nur in solchen Fällen tut, wäre das effektiv eben doch die Mitteilung, dass Auskunft verweigert wurde. Tut sie es immer, ist das ganze Auskunftsrecht wertlos. Es bleibt also nach dem Geist des Gesetzes eigentlich nur die offene Lüge.

Diese Lizenz zum Lügen hatte Europol schon bisher, und uns scheint, dass dort großzügig Gebrauch gemacht wurde davon (belegen können wir es natürlich nicht). Wenn das hier Schule macht, ist das, entschuldigt das Melodrama, das Ende des Datenschutzes bei der Polizei – die Auskünfte und ihre Folden haben viel dazu beigetragen, dass Reste rechtsstaatlicher Verfasstheit im Corps erhalten geblieben sind. Aber vielleicht, erhebet die Herzen, sind die Aufsichtsstrukturen ja stark genug und die Polizei macht von ihrem Lügerecht keinen Gebrauch. Wir würden hohe Quoten dagegen annehmen, wenn wer wetten wollte.

Überwachen und bestraft werden

Ein guter Teil der Aufregung um die DSGVO kam aus den etwas erweiterten Strafvorschriften. Schon bisher konnte für zwei Jahre einfahren, wer beispielsweise „gegen Entgelt" (§44 alt) unbefugt personenbezogene Daten verarbeitet – Berichte, dass auch nur eine der zahlreichen Horrorgeschichten, mit denen wir als Datenschutzgruppe in den letzten 15 Jahren zu tun hatten in auch nur einer Geldstrafe für die beteiligten Friedenswächter resultiert hätte, haben uns nie erreicht (ein Disziplinarverwahren gabs wohl mal).

Insofern wäre es sehr überraschend, wenn wir in der U-Haft wegen „bei ExtremistInnen gestanden" (Grüße an Fabio!) plötzlich ZellennachbarInnen hätten, die PHWs zusammenfantasiert, Demo-AnmelderInnen in Terrordateien gespeichert oder Löschfristen ins Unendliche gestreckt haben. Da wird auch der erweiterte Strafrahmen von bis zu drei Jahren nicht helfen. Schade eigentlich – selbst fundamentale KritikerInnen von Freiheitsentzug müssen wohl einräumen, dass in diesen speziellen Fällen eine glaubhafte Strafandrohung die Dinge zum Besseren wenden könnte.

Umgekehrt schmerzt im Hinblick auf praktische Straflosigkeiten bei Verstößen auch der weitere Abbau von Benachrichtigungspflichten nicht. §56 Abs. 1 des neuen BDSG sieht nämlich von vorneherein vor, dass Friedenswächter nur dann Speicheropfer von sich aus benachrichtigen müssen, wenn es dazu spezielle Rechtsvorschriften gibt. Die restlichen Absätze schränken das weiter ein. Vom „Datenbrief", einem jährlich automatisch zu versendenden Auszug der gespeicherten Daten, der dem Datenschutzgerippe wenigstens etwas Fleich auf die Rippen geben würde, entfernen uns DSGVO und noch mehr DSR weiter denn je.

Und so bleibt, wenigstens im Hinblick auf den Friedenswächter-Bereich, von der großen Reform an Haupt und Gliedern, als die Datenschutzgrundverordnung in der Öffentlichkeit verhandelt wurde, eigentlich nur: Die Polizei darf jetzt wahrscheinlich lügen, und niemand weiß, wie das aussehen wird. Ach so: Arbeit am Auskunftsgenerator bleibt natürlich auch (siehe oben), und wir wären wirklich glücklich, wenn sie nicht allein an uns hängen bleiben würde.

Datenschutzgruppe der RH Heidelberg/Mannheim

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: 4FD3 B3EE 7FCE 9FFD EC75 CAF9 4847 5F52 5C0C 5DB1