Vol. 21 – Juli 19

ip Competence

Themenjournal für geistiges Eigentum

GESCHÄFTSGEHEIMNIS

Geschäftsgeheimnis und Datenschutz – ein offener Widerspruch?

Günther Leissler

Geschäftsgeheimnis und Datenschutz – ein offener Widerspruch?

Günther Leissler

Sowohl der Datenschutz als auch Betriebs- und Geschäftsgeheimnisse dienen dem Schutz von Information. Zwei Rechtsbereiche, ein Ziel? Ein genauer Blick zeigt, dass dem nicht so ist. Vielmehr gilt es, komplexe Widersprüche zu überwinden.

I. Einleitendes

Stellt man den Gedanken des Betriebs- bzw Geschäftsgeheimnisses jenem des Datenschutzes gegenüber, so erscheint beides von der gleichen Zielsetzung geprägt – es geht um den Schutz von Informationen. So möchte das Geschäfts- und Betriebsgeheimnis den Schutz betriebsinterner Informationen verwirklicht wissen, die nicht zuletzt aufgrund ihres geheimen Charakters einen gewissen Wert besitzen. Betrachtet man aber den Schutzgedanken des Datenschutzrechts, so zeigt sich, dass dieser ein anderer ist. Er möchte den von einer Datenverarbeitung Betroffenen schützen. Dessen Daten sollen nur innerhalb der gesetzlich erlaubten Ausnahmen verarbeitet werden. Der primäre Kontrollfaktor hierbei ist der Betroffene selbst. Ihm stellt das Datenschutzrecht ein Portfolio an Rechten zur Verfügung. Durch Ausübung dieser Rechte soll der Betroffene seinen Datenschutz durchsetzen können.

Das Problem hierbei: Daten sieht man nicht. Um eine effektive Rechteausübung zu gewährleisten, verlangt das Datenschutzrecht daher nach Transparenz. Denn nur derjenige, dem die Verarbeitung seiner Daten erkennbar gemacht wird, kann effizient seine Rechte ausüben. Während also der Gedanke des Geschäfts- und Betriebsgeheimnisses das Ziel verfolgt, einem Unternehmen eine „Black Box“ einzuräumen, die vor Einsichtnahme und Zugriffen Dritter schützen soll, will das Datenschutzrecht das Gegenteil – Transparenz der Datenverarbeitung! Ein dem Geschäfts- und Betriebsgeheimnis vergleichbares Konzept einer „Datenverarbeitungs-Black Box“ ist dem Datenschutzrecht grundsätzlich fremd. Man kann daher mit gutem Grund von einem latentem Konflikt zwischen diesen Rechtsbereichen sprechen.

II. Der Transparenzgedanke im Datenschutzrecht

A. Kurzüberblick über die Rechtslage

Dieser Konflikt wurde sowohl bei der Schaffung der Datenschutz-Grundverordnung (DSGVO)[1] als auch vom österreichischen Gesetzgeber erkannt, als dieser in Ergänzung zur DSGVO das Datenschutzgesetz 2018 (DSG) implementierte. Dies zeigt sich anschaulich an der vermutlich wichtigsten Transparenzregelung der DSGVO, dem datenschutzrechtlichen Auskunftsrecht. In aller Kürze zusammengefasst, verpflichtet dieses einen Datenverarbeiter (datenschutzrechtliche Terminologie: Verantwortlicher) auf Begehren eines von der Datenverarbeitung Betroffenen, Auskunft darüber zu erteilen, welche seiner Daten verarbeitet werden, woher diese Daten stammen, mit wem sie geteilt werden und auf welcher Rechtsgrundlage die Datenverarbeitung erfolgt. Der geschuldete Umfang einer solchen Beauskunftung ist umfangreich, im Detail kann er durchaus die Grenzen des Geschäfts- oder Betriebsgeheimnisses berühren. In Anerkennung dessen ist in ErwGr 63 zur DSGVO festgehalten, dass die Beantwortung eines datenschutzrechtlichen Auskunftsbegehrens das Geschäftsgeheimnis des Datenverarbeiters nicht beeinträchtigen darf. Auch der österreichische Gesetzgeber hat in § 4 Abs 6 DSG festgehalten, dass das Recht auf Auskunft in der Regel nicht besteht, wenn hierdurch das Geschäfts- oder Betriebsgeheimnis des Datenverarbeiters gefährdet würde.

1 VO (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr, ABl L 2016/119, 1.

„DATEN SIEHT MAN NICHT. UM EINE EFFEKTIVE RECHTEAUSÜBUNG ZU GEWÄHRLEISTEN, VERLANGT DAS DATENSCHUTZRECHT DAHER NACH TRANSPARENZ. DEM GEGENÜBER BEDEUTET DIE DURCH DAS GESCHÄFTS- UND BETRIEBSGEHEIMNIS GESCHAFFENE VERTRAULICHKEIT INTRANSPARENZ."

„STELLT MAN DEN DATENSCHUTZ DEM GESCHÄFTS- UND BETRIEBSGEHEIMNIS GEGENÜBER, SO ERGIBT SICH DAHER DIE NOTWENDIGKEIT, GRENZEN ZU ZIEHEN."

B. Grenzen der datenschutzrechtlichen Transparenz

1. Der „Doppelwert" einer Information

Dem Gedanken der Begrenzung datenschutzrechtlicher Transparenz durch das Geschäfts- und Betriebsgeheimnis sind zwei Aspekte gemeinsam: (i) die Frage, ob durch eine Auskunft das Geschäfts- und Betriebsgeheimnis verletzt würde, ist stets einzelfallbezogen zu beurteilen; und (ii) weder die DSGVO, noch das DSG definieren das Geschäfts- oder Betriebsgeheimnis im datenschutzrechtlichen Sinn. Die Folge dessen ist ein Auftrag zur Selbstbeurteilung, die jedes Unternehmen im Anlassfall vorzunehmen hat. Typische Anlassfälle sind beispielsweise Scoringwerte oder Ausfallswahrscheinlichkeiten. Solche Informationen können aus beiderlei Sicht betrachtet werden. Die Information: „*Mit einer x-%igen Wahrscheinlichkeit wird der Kunde den Kredit nicht bedienen können.*" kann als eine Aussage über den präsumtiven Kreditnehmer, und damit als ein ihn betreffendes personenbezogenes Datum verstanden werden. Dieselbe Aussage kann aber auch als eine Information gewertet werden, die das Unternehmen selbst generiert hat und die aufgrund ihrer geheimen Natur einen kommerziellen Wert für das Unternehmen hat. Kurz: Ein Geschäfts- und Betriebsgeheimnis.

2. Abgrenzungsversuch: Personenbezogenes Datum

Wie ist nun angesichts dieser beiderlei vertretbaren Wertung die geschuldete Einzelfallabwägung im Rahmen eines Auskunftsbegehrens vorzunehmen? Ein möglicher Lösungsansatz könnte in einer genaueren Betrachtung des Begriffs des „personenbezogenen Datums" liegen. Denn dieses ist der Schlüssel zum datenschutzrechtlichen Auskunftsbegehren. Liegt kein personenbezogenes Datum vor, so greifen die Rechte der DSGVO (und damit auch das Auskunftsrecht) schon dem Grunde nach nicht.

Ein Detailblick zeigt: Oft ist die Aussage nicht die, dass der konkrete Kreditnehmer den Kredit mit einer x-%igen Wahrscheinlichkeit nicht bedienen wird können. Vielmehr ist die Aussage oft die, dass die Auswertung einer großen Anzahl von Kreditnehmern von beispielsweise gleicher beruflicher Situierung, gleicher regionaler Zuordnung, oder etwa gleichen Alters ergeben hat, dass der Kredit mit einer statistisch errechneten x-%igen Wahrscheinlichkeit nicht bedient werden kann. Es ist also keine Aussage über diesen konkreten Kreditnehmer, sondern eine statistisch hochgerechnete Aussage, die aus einer gesamthaften Marktbetrachtung gewonnen und diesem Kreditnehmer zugeordnet wird. Fraglich ist nun, ob eine solche Zuordnung statistisch gewonnener Informationen zu einer individuellen Person als deren personenbezogenes Datum angesehen werden kann.

Diese Rechtsfrage ist grundsätzlich offen, es gibt jedoch Indizien einer Antwort. So hat der deutsche Bundesgerichtshof (BGH) zum personenbezogenen Datumsbegriff noch unter der DatenschutzRL[2] zum Ausdruck gebracht, dass Scorings nicht als personenbezogene Daten anzu-

2 RL 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr – aufgehoben durch die DSGVO (EU) 2016/679.

sehen sind.[3] Da sich der Begriff des personenbezogenen Datums von der DatenschutzRL zur DSGVO strukturell nicht gewandelt hat, kommt den seinerzeitigen Erwägungen des BGH wohl auch unter der DSGVO Relevanz zu. Auch ein Gegenschluss unter der DSGVO hat Indizwirkung. So sieht die DSGVO etwa auch das Recht auf Datenberichtigung vor. Dieses Recht greift jedoch nur hinsichtlich unrichtig verarbeiteter Daten. Statistisch hochgerechnete Informationen, die einer Person zugeordnet werden, sind aber nicht berichtigungsfähig. Mit anderen Worten: Berichtigt werden kann die Grundlage der Zuordnung der statistischen Information zu einer individuellen Person, etwa wenn dieser Person irrtümlicherweise ein falsches Alter oder eine unrichtige Wohngegend zugeordnet wurde und diese daher in eine falsche „Zuordnungsklasse" eingestuft wird. Die eigentliche Aussage aber („*x-%ige Wahrscheinlichkeit, dass der Kredit nicht bedient wird*") ist nicht berichtigungsfähig. Es würde nun aber systemwidrig erscheinen, wenn die DSGVO, obgleich eines ihrer Kernelemente in der Stärkung der Rechtsposition des Betroffenen und in der effizienten Rechteausübung liegt, ein Terrain an personenbezogenen Daten definieren will, welches zumindest Teilen der Rechteausübung des Betroffenen entzogen ist. Genau dies wäre aber die Folge, wenn man Aussagen wie die oben zitierte als ein personenbezogenes Datum wertet. Auch eine konzeptionelle Betrachtung der DSGVO indiziert daher, dass derartige Aussagen nicht als personenbezogene Daten zu werten sind.

„DABEI IST ES BESONDERS WICHTIG ZU KLÄREN, OB EINER INFORMATION DER CHARAKTER EINES PERSONENBEZOGENEN DATUMS ZUKOMMT. DENN NUR BEI PERSONENBEZOGENEN DATEN GREIFT DAS TRANSPARENZPRINZIP DES DATENSCHUTZES."

3. Geschäftsgeheimnis und Datenschutz: Auftrag zur Selbstbeurteilung

Stellt man den Datenschutz dem Geschäfts- und Betriebsgeheimnis gegenüber, so ergibt sich also, dass Grenzen zu ziehen sind. Denn dort, wo das Geschäfts- und Betriebsgeheimnis beginnt, endet etwa das datenschutzrechtliche Auskunftsrecht. Wo diese Grenze verläuft, ist schwer zu beurteilen. Sie orientiert sich am Einzelfall. Ein Schlüssel zur Vereinbarkeit dieser beiden rechtlichen Konzepte könnte aber in einer sorgfältigen Qualifikation der verarbeiteten Informationen liegen. Die aufgezeigten Erwägungen zeigen: Nicht alles, was sich auf eine Person bezieht, bildet notgedrungen ein personenbezogenes Datum. Gerade statistische Informationen, wenn auch individuellen Personen zugeordnet, kann es dem für die Anwendung der DSGVO erforderlichen Personenbezug ermangeln. Nicht zuletzt weil diese Grenzziehung oft diffizil ist, wird es für Unternehmen unabdingbar sein, deren Geschäfts- und Betriebsgeheimnisse immer dann mit genauem Blick auf die DSGVO zu definieren, wenn zumindest ein Teil der geschützten Information in der Verarbeitung von Daten besteht.

III. Schlussstrich

Der Schutz von Geschäfts- und Betriebsgeheimnissen und der Schutz von Daten verfolgen Unterschiedliches. Beides in Einklang zu bringen, verlangt mitunter nach komplexen Überlegungen. Insb der Frage, ob einer Information der Charakter eines personenbezogenen Datums zuzusprechen ist, kann für die Abgrenzung zwischen dem Schutz betriebsinterner Informationen und dem datenschutzrechtlichen Transparenzgebot von essentieller Bedeutung sein.

3 BGH 28.1.2014, VI ZR 156/13 zum „Schufa"-Scoring.