SCHWEIZERISCHE BANKRECHTSTAGUNG 2019

Institut für Bankrecht, Universität Bern

Profiling nach der DSGVO und dem E-DSG bei Banken

David Vasella

In: Susan Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019

ISBN 978-3-7190-4269-1

Inhaltsübersicht

Profiling nach der DSGVO und dem E-DSG bei Banken

David Vasella, Zürich*

* Rechtsanwalt, Dr. iur., CIPP/E, Partner bei Walder Wyss AG, Zürich.

I. Einleitende Bemerkungen

1. Worum geht es?

Der Ausdruck «Profiling» erinnert an «Racial Profiling», das Profiling von Serientätern im Fernsehen und die massenhafte Auswertung der Datenspuren unseres digitalen Lebens, also das Vordringen der Technologie in die tieferen Schichten der menschlichen Persönlichkeit und an datenbasierte Diskriminierungen. Ein Blick in die fast zwanzig Jahre alte Empfehlung des Europarats zum Profiling[1] zeigt die damaligen Befürchtungen: Durch Profiling ist es möglich, Personen unbemerkt und auf Basis grosser Datenmengen in Kategorien einzuordnen, was – je nach Anwendungsgebiet und Kontext – die Selbstbestimmung und sogar die Menschenwürde der Betroffenen gefährdet.

Gleichzeitig umfasst Profiling nach heutigen Definitionen auch harmlose Vorgänge und Vorgänge im Interesse der betroffenen Person, bspw. Datenanalysen zur Betrugsprävention. Dieser Gegensatz wird in der gesetzlichen Regelung sichtbar: Der Ausdruck «Profiling» wird in der Europäischen Datenschutz-Grundverordnung (DSGVO), aber auch im Entwurf des DSG (E-DSG) wiederholt bloss als dramaturgisches Mittel eingesetzt; eigenständiger Regelungsgegenstand ist das Profiling nur vereinzelt. Gleichzeitig beruht Art. 20 Abs. 2 lit. b E-DSG auf der Fiktion, Profiling sei prinzipiell hochriskant, weshalb jedes Profiling eine Datenschutz-Folgenabschätzung erfordert.

2. Profiling und Persönlichkeitsprofile: Revision des DSG

Das DSG wird derzeit bekanntlich revidiert, im Gefolge besonders der DSGVO und der Revision der Europaratskonvention 108. Schon der Vorentwurf des revidierten DSG vom 21. September 2016 (VE-DSG) sah dabei vor, den Begriff des Persönlichkeitsprofils fallenzulassen und stattdessen das Profiling zu regeln – ein naheliegender Vorschlag, zumal die Europäische Datenschutz-Grundverordnung nun wie erwähnt das «Profiling» regelt und der Begriff des Persönlichkeitsprofils ausländischen Datenschutzrechten soweit ersichtlich unbekannt ist.[2] Der VE-DSG stiess im Vernehmlassungsverfahren allerdings auf wenig Gegenliebe. Kritisiert wurden besonders die sogar über die Anforderungen der DSGVO hinausgehenden Eigenheiten, der sog. Swiss Finish,[3] aber auch zahlreiche weitere Punkte. Ein wesentlicher Kritikpunkt

1 Europarat, Empfehlung Profiling, S. 1 ff.

2 Botschaft rev. DSG, S. 6971.

3 Vgl. VASELLA/SIEVERS, digma 2017, S. 44 ff.

war die vorgeschlagene Regelung des Profiling. Der VE-DSG definierte das Profiling so weit, dass selbst jede Datenauswertung von Hand als Profiling in Betracht kam. Darüber hinaus galt nach dem Vorentwurf, dass jedes Profiling ohne ausdrückliche Einwilligung persönlichkeitsverletzend gewesen wäre. Selbst andere Rechtfertigungsgründe wären nicht in Frage gekommen (Art. 23 Abs. 2 lit. d VE-DSG). Faktisch wäre für viele Alltagsvorgänge ein Verbot mit sehr beschränkten Ausnahmen eingeführt worden.

Im derzeitigen Entwurf des DSG (E-DSG) schränkte der Bundesrat die Definition des Profiling ein und liess gleichzeitig das grundsätzliche Verbot fallen, was die vorgeschlagene Regelung erheblich entschärft hat. Derzeit ist davon auszugehen, dass der Nationalrat den Entwurf mit den von der SPK-N vorgeschlagenen Änderungen in der Herbstsession 2019 berät.[4] Man darf gespannt sein, was die weitere Beratung in den Räten ergibt.

II. Übersicht über die gesetzliche Regelung

Die DSGVO spricht häufig vom Profiling:

- Art. 4 Ziff. 4 (Legaldefinition);
- Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g (Informationspflicht);
- Art. 15 Abs. 1 lit. h (Auskunftspflicht);
- Art. 21 Abs. 1 und 2 (Widerspruchsrecht aufgrund einer besonderen Situation bzw. gegen Direktmarketing);
- Art. 22 Abs. 1 (automatisierte Einzelfallentscheidungen);
- Art. 35 Abs. 3 lit. a (Datenschutz-Folgenabschätzung);
- Art. 47 Abs. 2 lit. e (Binding Corporate Rules);
- Art. 70 Abs. 1 lit. f (Aufgaben des Europäischen Datenschutzausschusses); und
- in den Erwägungsgründen 60, 63, 71, 72 und 91.

Allerdings trügt diese Liste. Häufig wird das Profiling nur mitgenannt, um eine andere Aussage zu verstärken. Das trifft, zumindest nach hier vertretener Auffassung, zu auf die Informations- und Auskunftspflichten, das Widerspruchsrecht, die Beschränkung automatisierter Einzelfallentscheidungen und Datenschutz-Folgenabschätzungen. Eine eigenständige Bedeutung hat das Profiling nur in Art. 4 Nr. 4 (Legaldefinition), am Rande bei Art. 70 Abs. 1 lit. f DSGVO (Aufgaben des Ausschusses) und in den Erwägungsgründen 60

[4] Medienmitteilung der SPK-N vom 29. Mai 2019.

und 63 (eigenständige Informationspflicht bei Profiling) und 71 (Anforderungen an die Durchführung des Profiling).

Vergleichbares gilt nach dem Entwurf des DSG (E-DSG), doch ist der Regelungsgehalt hier weiter. Nur mitgenannt wird das Profiling in Art. 19 Abs. 1 (Informationspflicht). Eigenständige Bedeutung hat das Profiling dagegen in

- Art. 4 lit. f (Legaldefinition);
- Art. 5 Abs. 6 (Ausdrücklichkeit der Einwilligung);
- Art. 20 Abs. 2 lit. b (Pflicht zur Durchführung einer DSFA bei Profiling);
- Art. 27 Abs. 2 lit. c Ziff. 1 (keine Vermutung des überwiegenden Interesses an der Prüfung der Kreditwürdigkeit, wenn dabei ein Profiling erfolgt); und
- Art. 30 Abs. 2 lit. b (Erfordernis einer formellgesetzlichen Grundlage für das Profiling durch Bundesbehörden).

III. Zur Legaldefinition des Profiling

1. Art. 4 Nr. 4 DSGVO

a) Begriff und Beispiele

Die DSGVO definiert das Profiling in Art. 4 Nr. 4 als «jede Art der automatisierten Verarbeitung» von Personendaten, die darin besteht, dass diese Daten «verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten». Zu einer solchen Bewertung gehören insbesondere die «Analyse oder Vorhersage» von «Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche[n] Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel». Es geht also um

- eine Verarbeitung von Personendaten,[5]
- die automatisiert erfolgt, und zwar
- mit dem Ziel einer Bewertung persönlicher Aspekte.

Die Legaldefinition ist klärungsbedürftig. Zunächst fragt sich, wann eine Verarbeitung von Personendaten i.S.v. Art. 4 Nr. 1 und 2 DSGVO «automatisiert» erfolgt. Dieser Ausdruck findet sich in der DSGVO wiederholt, besonders in Art. 2 Abs. 1 zum sachlichen Anwendungsbereich, wird aber nicht definiert

[5] Die DSGVO verwendet den Begriff der «personenbezogenen Daten»; der Lesbarkeit zuliebe spricht dieser Beitrag dennoch von «Personendaten»; gleichzeitig aber von «Bearbeitung», wenn es um schweizerisches Datenschutzrecht, und von «Verarbeitung», wenn es um Europäisches Datenschutzrecht geht.

und auch in den Erwägungsgründen nicht geklärt. Aus Art. 4 Nr. 2 und Art. 20 Abs. 1 lit. b DSGVO ist aber zu schliessen, dass es um eine Verarbeitung «mit Hilfe automatisierter Verfahren» geht, und die Artikel-29-Datenschutzgruppe[6] stellt diese den Datensammlungen aus Papier gegenüber.[7] Eine Verarbeitung erfolgt demnach immer dann automatisiert, wenn die Daten in elektronischer Form verarbeitet werden.[8] Für das Profiling soll es dabei genügen, wenn die Verarbeitung nur teilweise automatisiert erfolgt.[9] Eine Verarbeitung kann also auch dann ein Profiling darstellen, wenn ein Teil der Verarbeitung von Hand bzw. analog erfolgt.

Im Ergebnis wird das Tatbestandselement der Automatisierung selten einschränkend wirken. Eine Einschränkung kann auch nicht sinnvoll über quantitative Elemente erfolgen. Es ist bspw. nicht notwendig, dass eine umfangreiche Datenbasis verwendet wird, sobald schon wenige Daten geeignet sind, eine Bewertung persönlicher Aspekte zu ermöglichen; ohnehin wäre es unmöglich, eine genaue Grenze festzulegen. Wenn also etwa aufgrund eines Wohnortwechsels in ein bestimmtes Quartier auf die Bonität einer Person geschlossen wird (vgl. S. 198), dürfte dieser Vorgang als Profiling gelten.[10] Ob die Verlässlichkeit der Bewertung gut oder schlecht ist, spielt für den Begriff des Profiling dabei keine Rolle; diese Frage ist bei den inhaltlichen Anforderungen an das Profiling zu prüfen.

Wichtiger, aber schwieriger zu beantworten ist die Frage, wann eine solche Verarbeitung das Ziel verfolgt, «persönliche Aspekte» zu «bewerten». Eine «Bewertung» verlangt jedenfalls eine inhaltliche Auseinandersetzung. Dies entspricht dem Wortsinn, wird aber auch durch die Beispiele der Analyse oder Prognose persönlicher Eigenschaften oder Verhaltensweisen in Art. 4 Nr. 4 DSGVO verdeutlicht. Erforderlich ist deshalb eine Auseinandersetzung mit der Datenbasis, die zu einer zusätzlichen Aussage führt, die man als «informatiellen Mehrwert» bezeichnen könnte. Es geht mit anderen Worten darum, das Erkenntnispotential von Datenbeständen zu erschliessen.[11]

---

6 Die Art.-29-Datenschutzgruppe ist der frühere Name des Ausschusses der Datenschutz-Aufsichtsbehörden der Mitgliedstaaten und des Europäischen Datenschutzbeauftragten. Mit dem Wirksamwerden der DSGVO wurde sie durch den «Europäischen Datenschutzausschuss» abgelöst (Art. 68 ff. DSGVO).

7 Art.-29-Gruppe, Leitlinien Datenportabilität, S. 7.

8 So auch ROSSNAGEL, Art. 2 DSGVO N 14.

9 Art.-29-Gruppe, Leitlinien Profiling, S. 7; so auch SCHOLZ, Art. 4 Nr. 4 DSGVO N 4.

10 Vgl. SCHOLZ, Art. 4 Nr. 4 DSGVO N 5.

11 So SCHOLZ, Art. 4 Nr. 4 DSGVO N 6.

Eine Bewertung fehlt also, wenn Personen lediglich nach feststehenden Kriterien klassifiziert werden. Wer seine Kunden lediglich in Alterskohorten einteilt, profiliert sie deshalb nicht.[12] Anders verhält es sich, wenn Kunden Affinitäten zugewiesen werden, d.h. ein statistisch bestimmtes Interesse an einer Produktkategorie: Eine solche Klassifizierung ist ein Profiling, denn hier wird ein Kunde dadurch bewertet, dass eine Verhaltensprognose erstellt wird.

Damit stellen etwa folgende Tätigkeiten ein Profiling i.S.d. DSGVO dar, soweit sie in den räumlichen Anwendungsbereich der DSGVO[13] fallen:

- Die Bestimmung der Bonität, also der Wahrscheinlichkeit eines Zahlungsausfalls;
- die Kreditfähigkeitsprüfung i.S.v. des KKG;[14]
- das Tracking des Aufenthaltsorts einer Person in einer App mit dem Ziel, ortsbasierte Aktionen anzuzeigen, z.B. in einer App zur Verwaltung von Kreditkarten;
- die Prüfung von Kreditkartentransaktionen auf auffällige Muster, die auf einen Betrugsversuch hindeuten können;
- das Screening von E-Mails zur Aufdeckung und Verhinderung von Insiderhandel oder anderen Verstössen;[15]
- die Personalisierung von Beratungsleistungen und von Angeboten auf individuelle Kunden;[16]
- im HR-Bereich die Vorauswahl von Bewerbungen,[17] Laufbahnprognosen, Potenzialanalysen,[18] Background-Prüfungen,[19] die Auswertung von Stimmprofilen.[20]

---

12 So auch Art.-29-Gruppe, Leitlinien Profiling, S. 7.

13 Dazu Art. 3 DSGVO und Art. 129 IPRG.

14 Art. 28 Abs. 2 und Art. 29 Abs. 2 KKG; vgl. auch Art. 30 Abs. 1 KKG betr. summarische Kreditfähigkeitsprüfung; vgl. auch OGer BE, ZK 16 148 vom 23. September 2016, E. 20.7.1 („prognostische Beurteilung").

15 Vgl. FINMA RS 2013/8, Rz. 53 f. (Massnahmen zur Überwachung der Mitarbeitergeschäfte); SBVg, Data Leakage Protection, S. 23.

16 Dies erwähnt bspw. die ZKB in ihrer Datenschutzerklärung, abrufbar unter <http://bit.ly/2KNyV2f>; vgl. dazu auch Art. 10 ff. FIDLEG (Inkrafttreten am 1. Januar 2020); WEBER/BAISCH, AJP 2016, S. 1071.

17 Dazu WILDHABER, AJP 2017, S. 214.

18 SCHOLZ, Art. 22 DSGVO N 24.

19 Vgl. dazu etwa SBVg, Data Leakage Protection, S. 46.

20 Dazu BETZ, *passim*.

b) Automatisierte Entscheidung im Einzelfall

Abzugrenzen ist das Profiling von der «automatisierten Entscheidung im Einzelfall» (im Folgenden «AEE»), die etwa Art. 13 Abs. 2 lit. f DSGVO in einem Atemzug nennt. Eine AEE ist nach Art. 22 Abs. 1 DSGVO

- eine «Entscheidung»,
- die der betroffenen Person gegenüber eine rechtliche Wirkung entfaltet
- oder sie «in ähnlicher Weise erheblich beeinträchtigt».

Eine AEE stellt keine Datenbearbeitung dar, sondern eine auf einer automatisiert bearbeiteten Datengrundlage beruhende Entscheidung. Die zugrundeliegende Bearbeitung kann ein Profiling sein, aber zwingend ist dies an sich nicht.[21] Ebenso lässt sich aus der Wendung «automatisierte[n] Entscheidungsfindung einschließlich Profiling» (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h, Art. 22 Abs. 1 DSGVO) jeweils nicht schliessen, Profiling stelle stets eine AEE dar; hier geht es nur darum, die besondere Bedeutung des Profiling illustrativ hervorzuheben (darauf ist zurückzukommen). Allerdings wird eine AEE in den meisten Fällen ein Profiling umfassen. Das liegt am Begriff der «Entscheidung»: Eine Entscheidung setzt voraus, dass der Verantwortliche aus mehreren Möglichkeiten auswählt, also eine gewisse Wahlfreiheit hat. An einer Entscheidung fehlt es, wenn ein Verantwortlicher nur einer gegenseitig vereinbarten Logik folgt, bspw. eine Auszahlung am Geldautomaten verweigert, weil ein vertraglich definiertes Limit erreicht ist. Hier hat der Verantwortliche keine Wahl, weshalb er keine Entscheidung trifft.[22] Dasselbe gilt bei anderen Automatismen, bspw. der automatisierten Prüfung, ob das Kontoguthaben eine Überweisung erlaubt oder der Kreditkartensaldo den Karteneinsatz.[23] Darüber hinaus wäre der Betroffene einer Entscheidung in solchen Fällen nicht «unterworfen», wie es die DSGVO verlangt, weil er an ihr – durch den Vertragsschluss zu den entsprechenden Bedingungen – ja gerade mitgewirkt hat.[24] Infolgedessen wird eine Entscheidung in den meisten Fällen auf einer «Bewertung» des Betroffenen beruhen, also einer Form des

---

21 Art.-29-Gruppe, Leitlinien Profiling, S. 8.

22 Man mag einwenden, der Verantwortliche könne auch hier entscheiden, nämlich aus Kulanz; tut er dies nicht, fehlt es aber schon an einer rechtlichen oder vergleichbaren Wirkung auf den Betroffenen.

23 Vgl. SCHOLZ, Art. 22 DSGVO N 18; GOLA, Art. 22 DSGVO N 20 (der dasselbe Ergebnis mit einer teleologischen Reduktion begründet).

24 So auch SCHOLZ, Art. 22 DSGVO N 18; SCHULZ, Art. 22 DSGVO N 19; a.A. ARNING, S. 230.

Profiling. Im Ergebnis erscheint die AEE weitgehend als qualifizierte Form des Profiling.

Eine AEE liegt allerdings nur dann vor, wenn die Entscheidung ausschliesslich automatisiert erfolgt. Anders als beim Profiling führt echte menschliche Beteiligung an der Entscheidung aus dem Anwendungsbereich heraus, d.h. eine Beteiligung, die nicht nur formal ist.[25] Ein Beispiel ist eine inhaltliche Überprüfung der Maschinenentscheidung durch einen Menschen mit der Kompetenz und faktischen Möglichkeit, die Entscheidung umzustossen. Im Fall einer Kreditentscheidung setzt dies voraus, dass der zuständige Sachbearbeiter einen gewissen Entscheidungsspielraum hat, die Entscheidung also nicht ausschliesslich oder stark überwiegend durch einen Scorewert vorgegeben ist. Eine Ablehnung eines Kreditantrags ausschliesslich aufgrund eines zu schlechten Scorewerts («Cut-off-Score») kann daher eine AEE darstellen.[26]

Zudem ist eine Entscheidung nur erfasst, wenn sie zu einer Rechtsfolge führt, z.B. zur Beendigung einer Vertragsbeziehung, oder zu einer ähnlichen Beeinträchtigung. Eine «Beeinträchtigung» ist klarerweise negativ; positive Folgen sind daher nicht erfasst. Strittig ist aber, ob auch die Rechtsfolge negativ sein muss, um den Tatbestand zu erfüllen. Nach hier vertretener Auffassung trifft dies zu, so dass eine vollautomatisierte Gutheissung eines Kreditgesuchs keine AEE darstellt, denn hier rechtfertigen sich die besonderen Einschränkungen der AEE nicht.

2. Art. 4 lit. f E-DSG

a) Begriff

Die Revision des DSG bezweckt die Anpassung der Definition des «Profiling» an das europäische Recht.[27] Ganz geglückt ist das nicht. Unter Profiling versteht Art. 4 lit. f E-DSG «die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten […]». Der Botschaft zufolge genügt dabei nur ein doppelt automatisierter Vorgang:[28]

– Personendaten müssen automatisiert ausgewertet werden, und

[25] Art.-29-Gruppe, Leitlinien Profiling, S. 21.
[26] Näher SCHOLZ, Art. 22 N 25 ff.
[27] Botschaft E-DSG, 6978.
[28] Botschaft E-DSG, 7022.

– auf dieser Basis muss auch die Bewertung der Person automatisiert erfolgen.

Anders als nach der DSGVO lässt die Botschaft dabei nur einen vollständig automatisierten Vorgang genügen.[29] Dies lässt einige Fragen offen. Mit der «vollständigen Automatisierung» ist wohl nur gemeint, dass beide Stufen, sowohl die Auswertung der Daten als auch die Bewertung der Person, automatisiert sein müssen. Die Trennung dieser beiden Stufen ist zwar fragwürdig. Da die Botschaft diese Unterscheidung aber vornimmt, ist die Forderung nach voller Automatisierung wohl dahingehend zu deuten, dass beide Stufen automatisiert sein müssen. Das bedeutet aber nicht, dass beide Stufen für sich genommen keine relevante menschliche Tätigkeit ertragen. Ein Profiling wird deshalb auch dann vorliegen, wenn ein Mensch beteiligt ist, solange die Bewertung im Wesentlichen automatisiert erfolgt, etwa bei einem Kreditscoring, bei dem ein Mensch eingreift. Ein engeres Verständnis fände im Wortlaut des Gesetzes keine Stütze, und auch der Normzweck spricht gegen das enge Verständnis. Ferner beabsichtigt der Entwurf des DSG der Botschaft zufolge eine «inhaltliche» Anpassung an die europäische Terminologie.[30] Das ist zwar in sich widersprüchlich, deutet aber gleichwohl darauf hin, dass die Regelung der DSGVO übernommen werden sollte. Ohnehin wird die Praxis bei der DSGVO entlehnten Konzepten wie dem Profiling ohne viel Federlesens das Verständnis der DSGVO zugrunde legen, zumal die datenschutzrechtliche Diskussion noch für längere Zeit von der DSGVO geprägt bleiben dürfte.[31] Im Ergebnis ist also davon auszugehen, dass auch teilautomatisierte Bewertungen ein Profiling i.S.v. Art. 4 lit. f E-DSG darstellen können.

b) Automatisierte Einzelentscheidung (AEE)

Auch der E-DSG kennt die Figur der automatisierten Entscheidung im Einzelfall, die hier «automatisierte Einzelentscheidung» heisst (Art. 19 E-DSG). Hier lehnt sich der Wortlaut an Art. 22 Abs. 1 DSGVO an, und auch inhaltlich deckt sich der Begriff mit dem Verständnis der DSGVO.[32] Keine AEE liegt da-

---

29 Botschaft E-DSG, 7022.

30 Botschaft E-DSG, 7021.

31 Der EDÖB hat ebenfalls schon anklingen lassen, dass er eine freiwillige Anwendung der DSGVO in der Schweiz erwartet, vgl. dazu den Beitrag von VASELLA auf datenrecht.ch vom 20. Mai 2019, abrufbar unter <http://bit.ly/2KMmBiB>.

32 Nach Ansicht von ROSENTHAL stellt ein Profiling i.S.v. Art. 4 lit. f E-DSG immer auch eine AEE dar (ROSENTHAL, Jusletter 27. November 2017, Rz. 102). Nach hier vertretener

her bspw. dann vor, wenn ein Mensch auf Basis eines Scoring einen Kreditentscheid fällt. Im Übrigen soll der Bundesrat den Begriff laut Botschaft erforderlichenfalls konkretisieren.[33]

IV. Rechtmässigkeit des Profiling

1. Rechtmässigkeit nach der DSGVO

Als Form der Datenbearbeitung untersteht das Profiling den allgemeinen datenschutzrechtlichen Grundsätzen und Anforderungen (für die DSGVO vgl. Erwägungsgrund 72). Dazu gehört im Anwendungsbereich der DSGVO zunächst der Grundsatz der Rechtmässigkeit, d. h. das Erfordernis einer Verarbeitungsgrundlage (Art. 5 Abs. 1 lit. a und Art. 6 ff. DSGVO). In Frage kommen für das Profiling alle Rechtsgrundlagen in Art. 6 und 9 f. DSGVO.

Ohne hier auf Einzelheiten einzugehen, lässt sich festhalten, dass viele Profiling-Vorgänge für den Abschluss oder die Durchführung eines Vertrags erforderlich sind (Art. 6 Abs. 1 lit. b DSGVO), etwa bei Verträgen, die grundsätzlich ein kreditorisches Risiko beinhalten. Solche Verträge «rechtfertigen die Durchführung eines Profilings sowohl im vorvertraglichen Stadium als auch während ihrer Durchführung»,[34] soweit das Profiling zur Beurteilung des Kreditrisikos geeignet ist; dies gilt sowohl für die Beschaffung eines externen Scorings als auch die eigene Durchführung eines entsprechenden Profiling. Aber auch bei anderen Verträgen kann Profiling erforderlich sein, z.B. für die Prüfung von Betrugsrisiken bei Kreditkartentransaktionen[35] oder im HR-Bereich.[36] Demgegenüber werden Aufsichtsbehörden Profiling zu Werbezwecken kaum als vertragsnotwendig gelten lassen, und zwar auch dann nicht, wenn das Profiling in den AGB des Anbieters erwähnt wird.[37]

Die Skepsis der Aufsichtsbehörden gegenüber dem Profiling zu Werbezwecken ist generell hoch. Hier sollte zwar an sich das berechtigte Interesse i.S.v. Art. 6 Abs. 1 lit. f DSGVO weit tragen, berücksichtigt man die Tatsache,

---

Auffassung ist das nicht zutreffend; die Wendung «automatisierten Bearbeitung, einschliesslich Profiling» lässt diesen Schluss nicht zu; «Profiling» wird hier vielmehr, wie bei den analogen Bestimmungen der DSGVO, lediglich illustrativ verwendet.

33 Botschaft E-DSG, S. 7056.

34 45. Tätigkeitsbericht Hessen, Ziff. 4.2.1.3; so auch BUCHNER/PETRI, Art. 6 DSGVO N 47 f.

35 Zu eng Art.-29-Gruppe, Arbeitspapier Rechtsgrundlage Vertrag, S. 9, wonach Profiling für Zwecke der Betrugsbekämpfung kaum notwendig sein soll.

36 Hier ist gestützt auf die Öffnungsklausel in Art. 88 DSGVO auch das Recht der Mitgliedstaaten zu beachten, z.B. § 26 des deutschen BDSG.

37 Vgl. Art.-29-Gruppe, Arbeitspapier Rechtsgrundlage Vertrag, S. 9 und 13.

dass der Schutz der betroffenen Person durch das Widerspruchsrecht von Art. 21 Abs. 1 und 2 DSGVO gewährleistet wird; zumindest dann, wenn der Verantwortliche diesen Schutz durch geeignete Garantien flankiert.[38] Die Entwicklung in Deutschland geht aber in eine andere Richtung. Zuletzt hat die Datenschutzkonferenz in ihrer Orientierungshilfe zwar nicht ausgeschlossen, dass sich ein personenbezogenes Tracking im Internet – das unter den Begriff des Profiling fallen kann – auf ein berechtigtes Interesse stützt, dass dies aber eine aufwendige, einzelfallbezogene Interessenabwägung verlangt.[39]

Ebenfalls in Frage kommt ein Profiling im Rahmen gesetzlicher Pflichten, z.B. zur Bekämpfung der Geldwäscherei. Hier verweist die Art.-29-Datenschutzgruppe auf die Rechtsgrundlage der Rechtspflicht, nicht der Vertragsnotwendigkeit.[40] Das ist solange überzeugend, als sich die Rechtspflicht aus EU-Recht bzw. dem Recht der Mitgliedstaaten ergibt (Art. 6 Abs. 3 DSGVO). Führt eine schweizerische Bank demgegenüber mit Bezug auf einen Kunden im EWR-Gebiet, aber gestützt auf schweizerisches Recht Profiling durch,[41] stellt sich spätestens dann die Frage der Rechtsgrundlage, wenn der betreffende Kunde gegenüber der Bank nach Art. 139 IPRG die DSGVO anruft. Hier kann die Bank wahlweise auf Art. 6 Abs. 1 lit. b und/oder lit. f DSGVO verweisen, denn das Profiling ist objektiv vertragsnotwendig und entspricht gleichzeitig dem berechtigten Interesse der Bank, schweizerisches Recht einzuhalten. Dass mehrere Rechtsgrundlagen nebeneinander anwendbar sein können, ergibt sich sodann aus dem Wortlaut von Art. 6 Abs. 1 DSGVO («rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist»).[42]

Kommt eine AEE hinzu, stellt sich die Frage der Rechtmässigkeit besonders. Art. 22 DSGVO erlaubt AEE nur eingeschränkt,[43] nämlich nur dann, wenn eine AEE für einen Vertrag zwischen der betroffenen Person und dem

---

38 «Geeignete Garantien» sind sämtliche Massnahmen zum Schutz der Betroffenen, bspw. erhöhte Transparenz, interne technische und organisatorische Massnahmen, besonders leicht auszuübende oder weitreichende Widerspruchsrechte, die freiwillige Durchführung einer Datenschutz-Folgenabschätzung usw. Alle diese Faktoren sind bei der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO zu berücksichtigen.

39 DSK, Orientierungshilfe, S. 11 ff.

40 Art.-29-Gruppe, Arbeitspapier Rechtsgrundlage Vertrag, S. 12.

41 Vgl. bspw. Art. 13 GwV-FINMA.

42 So auch BUCHNER/PETRI, Art. 6 DSGVO N 22.

43 Man kann sich fragen, ob Art. 22 DSGVO ein Verbot vorsieht oder der betroffenen Person lediglich einen Abwehranspruch verleiht. Es dürfte aber wohl von einem Verbot auszugehen sein. Das ist jedenfalls das Verständnis der Art.-29-Datenschutzgruppe.

Verantwortlichen erforderlich (Art. 22 Abs. 1 lit. a DSGVO)[44] oder gesetzlich erlaubt ist, wobei wiederum nur europäisches Recht beachtlich ist (lit. b), oder mit ausdrücklicher Einwilligung der betroffenen Person (lit. c).

2. Rechtmässigkeit nach dem E-DSG

Das schweizerische Datenschutzrecht beruht bekanntlich, anders als das Europäische Datenschutzrecht, auf dem Grundsatz der Erlaubnis mit Verbotsbehalt. Die Bearbeitung von Personendaten ist grundsätzlich zulässig. Die Frage lautet hier daher nicht, auf welche Rechtsgrundlage sich eine Bearbeitung stützt, sondern ob im konkreten Fall Rechtfertigungsbedarf besteht (Art. 26 E-DSG) und, falls ja, ob ein Rechtfertigungsgrund vorliegt (Art. 27 E-DSG). Dies gilt für alle Bearbeitungen durch Private, auch die Bearbeitung besonders schützenswerter Personendaten und Profiling.[45]

In Frage kommen alle Rechtfertigungsgründe (Art. 27 Abs. 1 E-DSG), wobei die Einwilligung ggf. – sofern sie aufgrund des E-DSG konkret erforderlich ist – ausdrücklich erfolgen muss (Art. 5 Abs. 6 E-DSG). Was «ausdrücklich» heisst, ist dabei weiterhin unklar.[46]

Fragen ergeben sich auch im Zusammenhang mit den Regelbeispielen eines überwiegenden privaten Interesses in Art. 27 Abs. 2 E-DSG. Ein Kunstfehler ist dem Bundesrat bei der Formulierung von Art. 27 Abs. 2 lit. c E-DSG unterlaufen, der Bearbeitung von Personendaten für die Prüfung der Kreditwürdigkeit. Das Interesse an dieser Datenbearbeitung soll nach Art. 27 Abs. 2 lit. c Ziff. 1 E-DSG dann nicht überwiegen, wenn ein Profiling stattfindet. Aber selbstverständlich kann das Interesse des Verantwortlichen und/oder eines Dritten an Profiling die gegenläufigen Interessen des Betroffenen überwiegen, und vor allem lässt der Vorschlag des Bundesrats ausser Acht, dass die Prüfung der Kreditwürdigkeit geradezu ein Schulbeispiel für Profiling ist. Eine Berufung auf ein überwiegendes Interesse hier nicht zuzulassen, ist widersprüchlich; dann könnte Art. 27 Abs. 2 lit. c insgesamt gestrichen werden.

---

44 Dieser praktisch bedeutsame Rechtfertigungsgrund ist hier allerdings enger als bei Art. 6 Abs. 1 lit. b DSGVO. Dort genügt es, dass eine Verarbeitung für einen Vertrag erforderlich ist, dessen Partei der Betroffene ist; dass dieser Vertrag mit dem Verantwortlichen besteht, ist anders als bei Art. 22 Abs. 1 lit. b DSGVO nicht vorausgesetzt.

45 Anders im öffentlichen Bereich; hier gilt das Erfordernis einer gesetzlichen Grundlage (Art. 30 E-DSG). Der E-DSG sieht daher bspw. vor, Art. 23 FINMAG dahingehend zu ändern, dass die FINMA zum Profiling befugt ist.

46 Vgl. ROSENTHAL, Jusletter 27. November 2017, Rz. 39; VASELLA, Jusletter 16. November 2015, Rz. 22 ff.

Zwar ist die Aufzählung in Abs. 2 nicht abschliessend, so dass Profiling zur Prüfung der Kreditwürdigkeit auch ohne Anpassung des Gesetzestextes durch überwiegende Interessen gerechtfertigt werden kann. Es ist dennoch zu hoffen, dass das Parlament diesen Fehler korrigiert und das Profiling bei Art. 27 Abs. 2 lit. c E-DSG streicht (und bei dieser Gelegenheit auch die nicht sachgerechte Beschränkung auf fünf Jahre in lit. c Ziff. 3 streicht oder anpasst).

V. Informations- und Auskunftspflichten im Zusammenhang mit Profiling

1. Informations- und Auskunftspflicht bei blossem Profiling?

Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. h DSGVO verlangen, dass die betroffene Person über «das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling» zu informieren ist; und entsprechendes sieht Art. 15 Abs. 1 lit. h DSGVO für das Auskunftsrecht vor. Aus diesem Wortlaut geht hervor, dass sich die Informations- und Auskunftspflichten nur auf Profiling beziehen, das Teil einer AEE ist («einschliesslich» Profiling). Blosses Profiling, das keine AEE ist, löst keine solchen Pflichten aus. Diesem Schluss ist zunächst allerdings entgegenzuhalten, dass

– die Erwähnung des Profiling nicht notwendig wäre, wenn sich keine Rechtsfolgen daran knüpfen, und dass
– es keinen Grund gäbe, AEE in Art. 13 und 14 zu erwähnen, wenn es an diesen Stellen nur um die Information über AEE – und nicht auch für Profiling – ginge; denn für AEE ergibt sich eine Informationspflicht schon aus Art. 22 Abs. 3 DSGVO.

Grosses Gewicht haben diese Argumente allerdings nicht, zumal die DSGVO diverse Unschärfen aufweist und die Erwähnung des Profiling auch als blosses Stilmittel verstanden werden kann. Im Gegenteil drängt sich der Schluss auf, dass Art. 13-15 das Profiling ohne AEE nicht erfassen. Diese Bestimmungen verweisen ausdrücklich auf AEE «gemäss Artikel 22 Absätze 1 und 4». Art. 22 Abs. 1 DSGVO greift dann zwar die Formulierung in Art. 13, 14 und 15 DSGVO auf («einschließlich Profiling»), regelt aber klarerweise nicht das Profiling als solches. Denn wäre Profiling ohne AEE hier erfasst, hätte dies zur Folge, dass das Profiling der eingeschränkten Zulässigkeit nach Art. 22 DSGVO unterläge. Es wäre wie AEE nur zulässig, wenn es für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem

Verantwortlichen (Abs. 2 lit. a) oder aufgrund rechtlicher Vorschriften erforderlich ist (Abs. 2 lit. b) oder mit ausdrücklicher Einwilligung der betroffenen Person (Abs. 2 lit. c). Eine Rechtfertigung durch berechtigtes Interesse oder eine nicht ausdrückliche Einwilligung entfiele. Eine so weitreichende Folge müsste sich im Gesetzestext aber eindeutig wiederfinden.[47] Wenn die zitierte Formulierung bei Art. 22 Abs. 1 DSGVO das Profiling nun aber nur in symbolhafter Weise und nicht als eigenständigen Regelungsgegenstand erwähnt, kann für die entsprechende Formulierung in Art. 13 ff. nichts anderes gelten. Schon deshalb ist eine auf Art. 13 oder 14 DSGVO gestützte Informationspflicht und eine Auskunftspflicht nach Art. 15 DSGVO abzulehnen. In der Literatur ist dieser Schluss freilich umstritten.[48]

Art. 5 Abs. 1 lit. a DSGVO gibt allerdings parallel zu Art. 13 und 14 DSGVO vor, dass die Verarbeitung von Personendaten transparent erfolgen muss. Es handelt sich um eine programmatische Generalklausel, die sich aber – anders als die Vorgängernorm in der Datenschutz-Richtlinie – nicht an die Mitgliedstaaten, sondern an den Verantwortlichen[49] richtet und direkt anwendbar ist; und ihre Verletzung ist mit Busse bedroht (Art. 83 Abs. 5 lit. a DSGVO).[50] Es ist nicht auszuschliessen, dass sich daraus eine über Art. 13 f. hinausgehende Informationspflicht über Profiling ableiten lässt. So verlangt auch Erwägungsgrund 60, dass die betroffene Person darauf hingewiesen wird, dass ein Profiling stattfindet und welche Folgen dies hat.[51] Erwägungsgründe sind aber nicht Teil des «verfügenden», d.h. verbindlichen Teils der DSGVO; sie dienen nur zu dessen Begründung und dürfen «keine Bestimmungen mit normativem Gehalt» enthalten.[52] Eine Informationspflicht über

---

47 Vgl. auch SCHOLZ, Art. 22 DSGVO N 5: Art. 22 DSGVO schränkt die Zulässigkeit des Profiling nicht ein.

48 Wie hier PAAL/HENNEMANN, Art. 13 DSGVO N 26; KAMLAH, Art. 13 N 27; ARNING, S. 152; wohl auch VEIL, Art. 13 und 14 DSGVO N 114; a.A. (Informationspflicht auch bei blossem Profiling) FRANCK, Art. 13 DSGVO N 27; BÄCKER, Art. 13 DSGVO N 54; MESTER, Art. 13 DSGVO N 27.

49 Inwieweit sich aus Art. 5 DSGVO auch für den Auftragsverarbeiter Pflichten ergeben, ist nicht geklärt.

50 Rechtsstaatlich ist eine so unbestimmte Strafbestimmung falsch. Der Entwurf des DSG tut aber dasselbe, indem die Informationspflicht nach Art. 17 Abs. 2 E-DSG ebenfalls mit einer Generalklausel operiert, deren Verletzung nach Art. 54 Abs. 1 lit. a E-DSG aber mit Busse bedroht ist.

51 Das Wort «sollte» («should») in Erwägungsgrund 60 erlaubt dabei nicht den Schluss, es gehe lediglich um eine Empfehlung; das ist eine in Erwägungsgründen auch anderswo häufig verwendete Formulierung.

52 Leitfaden Rechtstexte, Ziff. 10.

Profilingmassnahmen kann sich daher nicht allein auf Erwägungsgrund 60 stützen. Erwägungsgrund 60 kann aber natürlich bei der Auslegung von Art. 5 Abs. 1 lit. a DSGVO berücksichtigt werden. Eine Informationspflicht für blosses Profiling sieht denn auch die Art.-29-Datenschutzgruppe. Der Leitfaden zum Profiling lässt sich zwar so lesen, dass es nur «good practice» ist, über Profiling zu informieren, solange keine AEE vorliegt. Dem steht aber gegenüber, dass derselbe Leitfaden an gleicher Stelle auf Erwägungsgrund 60 verweist;[53] und der Leitfaden zur Transparenz geht recht deutlich von einer Informationspflicht zu Profiling aus.[54]

Die Gerichte werden klären müssen, ob, wann und in welcher Form blosses Profiling separat informationspflichtig ist. Nach hier vertretener Auffassung verlangt die Generalklausel von Art. 5 Abs. 1 lit. DSGVO jedenfalls eine Abwägung im Einzelfall. Der Verantwortliche hat dabei Ermessensspielraum.

In der Praxis informieren Banken vielfach freiwillig über Profilingmassnahmen, so etwa die UBS,[55] die Credit Suisse[56] und die ZKB[57] und im Ausland bspw. die Deutsche Bank,[58] während z.B. die Julius Bär soweit ersichtlich darauf verzichtet. Die Informationen sind dabei jeweils knapp gehalten, was zumindest dem Anliegen der Verständlichkeit (Art. 12 Abs. 1 DSGVO) entspricht.

Im Rahmen des E-DSG besteht ebenfalls eine Informationspflicht für AEE. Art. 19 Abs. 1 E-DSG verwendet die gleiche Wendung wie die DSGVO: Die Informationspflicht bezieht sich auf AEE «einschliesslich Profiling». Insofern stellen sich ähnliche Auslegungsfragen wie soeben bei der DSGVO. Auch das Ergebnis ist dasselbe: Eine Informationspflicht entsteht nicht durch blosses Profiling. Auch die Botschaft hält dies ausdrücklich fest.[59]

---

53 Art.-29-Gruppe, Leitlinien Profiling, S. 25.

54 Art.-29-Gruppe, Leitlinien Transparenz, S. 22.

55 Data Privacy Notice, abrufbar unter <http://bit.ly/2IUoBmz>.

56 Informationspflichten im Rahmen der Erhebung von personenbezogenen Daten bei der betroffenen Person nach Artikel 13 Absätze 1, 2 und 4 sowie Artikel 21 Absatz 3 der EU-Datenschutz-Grundverordnung (DSGVO), abrufbar unter <http://bit.ly/2wUio4i>.

57 Datenschutzerklärung, abrufbar unter <http://bit.ly/2RlrmRC>.

58 Data protection information under the Swiss Federal Act on Data Protection and EU General Data Protection Regulation, abrufbar unter <http://bit.ly/2wRZkDF>.

59 Botschaft E-DSG, S. 7057.

2. Information und Auskunft bei AEE

Kommt zum Profiling eine AEE hinzu, greifen dagegen die Informationspflichten nach Art. 13 und 14 und die Auskunftspflicht nach Art. 15 DSGVO. Darüber hinaus gelten die besonderen Anforderungen bzw. Betroffenenrechte nach Art. 22 Abs. 3 DSGVO, sofern die AEE nicht auf gesetzlicher Grundlage beruht (sondern durch Vertragsnotwendigkeit oder ausdrückliche Einwilligung gerechtfertigt ist), und die eingeschränkte Zulässigkeit nach Art. 22 Abs. 1 und 2 DSGVO, die angesprochen wurde, hier aber nicht vertieft wird.

Die Informationspflicht in Art. 13, 14 und 15 DSGVO betrifft jeweils folgende Punkte:

- dass eine AEE stattfinden soll;
- ihre «Logik» und
- ihre Tragweite und die angestrebten Auswirkungen auf die Betroffenen.

Die involvierte Logik meint die Kriterien, die das Ergebnis der AEE beeinflussen, und die Art und Weise, wie sie auf die AEE einwirken. Dies verlangt weder eine detaillierte Erklärung technischer Abläufe noch eine Offenlegung der Entscheidformel, die ein Geschäftsgeheimnis darstellt,[60] aber eine verständliche Erläuterung des zugrundeliegenden Prinzips,[61] so dass der Betroffene in der Lage ist, die AEE nachzuvollziehen. Die Mitgliedstaaten können gestützt auf Art. 23 DSGVO Einschränkungen der Informations- und Auskunftspflicht vorsehen.

Art. 19 Abs. 1 E-DSG verlangt ebenfalls, dass die betroffene Person über die AEE informiert wird. Aus Art. 19 Absatz 2 E-DSG ergibt sich ferner das Recht der betroffenen Person, ihren Standpunkt darzulegen. Dies setzt voraus, dass die betroffene Person über diejenigen Informationen verfügt, die erforderlich sind, um die AEE in ihren Grundzügen zu verstehen. Offen bleibt, ob es am Verantwortlichen liegt, der betroffenen Person diese Informationen von sich aus zur Verfügung zu stellen, oder ob es genügt, erst auf Nachfrage zu informieren. Die Botschaft geht von letzterem aus. Es genügt, wenn die betroffene Person Gelegenheit hat, «ihre Ansicht zum Ergebnis der

---

60 Vgl. Erwägungsgrund 63 *(«Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen»)*; SCHOLZ, Art. 22 DSGVO N 17; vgl. auch das Urteil des deutschen Bundesgerichtshofs (BGH) vom 28. Januar 2014 i.S. Schufa, VI ZR 156/13.

61 So, Art. 13 DSGVO N 19.

Entscheidung zu äussern» und gegebenenfalls «nachzufragen, wie die Entscheidung zustande gekommen ist».[62] Aus Praktikabilitätsüberlegungen ist diese Sicht zu begrüssen, zumal der Schutz der betroffenen Person auch so sichergestellt sein dürfte. Demnach hat der Verantwortliche von sich aus nur über das Vorliegen der AEE und ihr Ergebnis zu informieren, z.B. in einem Schreiben, in der über die Ablehnung eines Online-Kreditantrags informiert wird. Aus Art. 19 E-DSG folgt weiter nur, dass die betroffene Person das Recht hat, weitere Informationen zu verlangen, sodass sie ihren Standpunkt darlegen kann (abgesehen vom Recht, eine Entscheidung durch eine natürliche Person zu verlangen; ebenfalls Art. 19 Abs. 2 E-DSG).

Anzumerken bleibt, dass weder eine Informationspflicht noch ein Anspruch auf Darlegung des Standpunkts und Überprüfung besteht, wenn eine Offerte automatisch angenommen wird (Art. 19 Abs. 3 lit. a E-DSG; wenn ein Online-Kreditantrag angenommen wird, um im Beispiel zu bleiben, muss die Bank dem Kreditnehmer also nicht mitteilen, dass die Überprüfung ihres Antrags automatisiert erfolgt ist) oder wenn die betroffene Person ausdrücklich eingewilligt hat, dass eine Einwilligung automatisiert erfolgen kann (lit. b).

VI. Zu den Anforderungen an die Durchführung des Profiling

1. Vermeidung von Diskriminierungen

Die DSGVO enthält im verfügenden Teil keine spezifischen Vorgaben an die Durchführung des Profiling. Es gelten wie erwähnt die allgemeinen Grundsätze, besonders der Grundsatz der Zweckbindung[63] und die Grundsätze des Datenschutzes durch Technikgestaltung (Privacy by design) und durch datenschutzfreundliche Voreinstellungen (Privacy by default; Art. 25 DSGVO und Art. 6 E-DSG). Erwägungsgrund 71 gibt aber vor, dass für das Profiling «geeignete mathematische oder statistische Verfahren» angewandt werden sollen und dass Fehlerquellen und Risiken unrichtiger Daten zu minimieren und Diskriminierungen zu verhindern sind. Diese Anforderungen ergeben

62 Botschaft E-DSG, S. 7058.

63 Hierzu nur soviel: Ein Profiling ist genauso wie eine AEE kein Verarbeitungszweck, sondern ein Mittel der Verarbeitung. Der Einsatz von Profilingmassnahmen und AEE stellt daher nur dann eine Zweckänderung dar, wenn das damit angestrebte Ziel nicht mehr mit den ursprünglichen Zwecken der dabei verarbeiteten Daten vereinbar ist.

sich im Anwendungsbereich der DSGVO bereits aus allgemeinen Grundsätzen (Art. 5 DSGVO) und im HR-Bereich aus arbeitsrechtlichen Vorschriften;[64] Erwägungsgrund 71 zeigt aber, dass Diskriminierungsrisiken im Zusammenhang mit Profiling als besonders gewichtig eingestuft werden. Deshalb hat der deutsche Gesetzgeber in § 31 des deutschen Bundesdatenschutzgesetzes weitere Beschränkungen vorgesehen. Dem Schutz vor Diskriminierung dient etwa § 31 Abs. 1 Ziff. 3 BDSG, wonach ein Scoring nicht nur auf Adressdaten beruhen darf. Eine Bank darf demnach die Kreditwürdigkeit nicht allein auf der Basis von Adressdaten beurteilen. Damit soll verhindert werden, dass bestimmte Gebiete durch Geoscoring pauschal schlechtergestellt werden («redlining»).

Die Bank ist nach der DSGVO infolgedessen verpflichtet, die «Logik» des Profiling (vgl. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO) so auszugestalten, dass das Verfahren geeignet ist, die angestrebten Aussagen ausreichend abzustützen, sachgerechte Kriterien zu verwenden, Unschärfen und Fehler angemessen zu minimieren und (direkte und indirekte) Diskriminierungen zu verhindern. Auf den Einbezog besonders schützenswerter Personendaten ist nach Möglichkeit zu verzichten.[65] Die entsprechenden Überlegungen sollten mit Blick auf die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DSGVO) dokumentiert werden, ggf. im Rahmen des Verarbeitungsverzeichnisses (Art. 30 Abs. 1 DSGVO; Art. 11 E-DSG).

Für das E-DSG lassen sich diese Grundsätze nicht unbesehen übernehmen. Die Bedeutung des Diskriminierungsrisikos ist eine andere, denn die Schweiz kennt i.d.R. keine direkte Horizontalwirkung von Grundrechten.[66] Allerdings muss das Profiling selbstverständlich die Bearbeitungsgrundsätze

64 Dazu WILDHABER, AJP 2017, S. 214 ff.

65 Dieser Verzicht erlaubt es dem Verantwortlichen, sich ggf. auf ein berechtigtes Interesse i.S.v. Art. 6 Abs. 1 lit. f DSGVO zu berufen und eine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) zu vermeiden. Wenn der Verantwortliche nämlich abstrakt gesehen besonders schützenswerte Personendaten bearbeitet (z.B. Angaben über Spenden an eine religiöse Vereinigung oder Ausgaben bei spezialisierten Ärzten oder in Etablissements, deren Besuch dem Intimbereich zuzurechnen ist), die besondere Aussagekraft dieser Daten in das Profiling aber nicht einbezieht (also bspw. Affinitäten bestimmt, aber keine Kategorien wie «gesundheitlich beeinträchtigt» oder «Sin Hobby» bildet), kann er vertreten, dass er für das Profiling keine besonders schützenswerten Personendaten bearbeitet und keine ausdrückliche Einwilligung erforderlich ist.

66 Vgl. SCHWEIZER, Art. 35 BV N 58 ff.

einhalten, z.B. den Grundsatz der Verhältnismässigkeit; und in diesem Rahmen können Anliegen von Erwägungsgrund 71 der DSGVO berücksichtigt werden.

2. Risikobeurteilung

Sowohl die DSGVO als auch das DSG verfolgen einen risikoorientierten (oder «risikobasierten») Ansatz. Die Pflichten des Verantwortlichen richten sich mit anderen Worten bis zu einem gewissen Grad – soweit das anwendbare Recht Pflichten nicht vollständig determiniert – nach dem Risiko, das sich aus einer Datenbearbeitung für die Betroffenen ergibt.[67] Dies verlangt generell eine Risikobeurteilung, wie sich etwa in Art. 32 Abs. 1 DSGVO oder Art. 7 Abs. 1 E-DSG zeigt.

In bestimmten Fällen schreibt das Gesetz aber eine besondere, strukturierte und dokumentierte Risikobeurteilung in Form einer Datenschutz-Folgenabschätzung vor («DSFA»; Art. 35 f. DSGVO; Art. 20 E-DSG). Das trifft dann zu, wenn eine Bearbeitung voraussichtlich ein «hohes Risiko» mit sich bringt (Art. 35 Abs. 1 DSGVO; Art. 20 Abs. 1 E-DSG). Es fragt sich daher jeweils, wann mit einem hohen Risiko zu rechnen ist; eine Risikoentscheidung, die dem Verantwortlichen überlassen ist. Die DSGVO und der E-DSG geben aber Hinweise in Form von Regelbeispielen (Art. 35 Abs. 3 DSGVO; Art. 20 Abs. 2 E-DSG). Dabei fällt auf, dass nach Art. 20 Abs. 2 lit. b E-DSG jedes Profiling als Hochrisikofall gilt. Die Botschaft begründet dies nicht. Dass Profiling als höchst suspekt empfunden wird, war aber schon im Vorentwurf überdeutlich, der Profiling generell nur mit ausdrücklicher Einwilligung zulassen wollte (Art. 23 Abs. 2 lit. d des Vorentwurfs). Für den Bundesrat ist eine Risikobeurteilung in Form einer DSFA – ggf. mit Einbezug des EDÖB nach Art. 20 21 E-DSG – offenbar der Preis dafür, das Profiling nicht zu verbieten. Abwegig ist das nicht, aber viel zu pauschal. Die These, Profiling sei stets hochriskant, ist falsch. In vielen Fällen ist Profiling harmlos und liegt noch dazu im Interesse der betroffenen Person;[68] und wenn Profiling im Einzelfall tatsächlich hochriskant sein sollte, ist eine DSFA über Art. 20 Abs. 1 E-DSG ohnehin verpflichtend.

---

67 Dazu Erwägungsgründe 74 ff.

68 Etwa durch Personalisierung von Angeboten oder durch Betrugsprävention, z.B. beim Schutz vor dem Missbrauch von Kreditkartendaten; vgl. HLADJK, Art. 22 DSGVO N 4; im HR-Prozess durch Zeitersparnis oder gerade dadurch, dass ein Bewerber lieber von einer Maschine automatisiert als von einem vorurteilsbehafteten Menschen beurteilt

Dies bestätigt ein Blick in die Leitlinien der Art.-29-Datenschutzgruppe. Im Sinne einer Faustregel ist eine DSFA dann durchzuführen, wenn bei einer Verarbeitung mindestens zwei Risikofaktoren zusammentreffen; wobei «evaluation or scoring, including profiling and predicting» (in der deutschen Sprachfassung der Leitlinien: «Bewerten oder Einstufen») einen Risikofaktor darstellt[69]. Für sich genommen führt ein Profiling demnach nicht generell zur Pflicht, eine DSFA durchzuführen, sondern nur dann, wenn einer der folgenden Risikofaktoren dazukommt:

- es wird eine AEE durchgeführt;
- es findet eine systematische Überwachung statt;
- es werden besonders schützenswerte Personendaten oder sonst besonders heikle Personendaten verarbeitet, bspw. Kontoangaben, die betrugsanfällig sind;
- Personendaten werden in grossem Umfang verarbeitet;
- Datensätze werden abgeglichen oder zusammengeführt;
- es werden Personendaten schutzbedürftiger Personen verarbeitet;
- es werden neue Technologien verwendet, oder bekannte Technologien in neuartiger Weise;
- betroffenen Personen kann ein Recht, eine Dienstleistung oder ein Vertrag verweigert werden.

Aufschlussreich ist in diesem Zusammenhang ein Blick auf die schwarzen und weissen Listen der Aufsichtsbehörden, die nach Art. 35 Abs. 4 und 5 DSGVO zu erstellen sind. Die deutsche Datenschutzkonferenz etwa verlangt eine DSFA u.a. in den folgenden Fällen:[70]

- Betrieb eines Fraud-Prevention-Systems;
- Scoring durch Wirtschaftsauskunfteien, Banken oder Versicherungen;
- Einsatz eines Data-Loss-Prevention-Systems, das systematische Profile der Mitarbeiter erzeugt;
- Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden.

---

wird; dazu BETZ, S. 149; generell durch ggf. an den Kunden weitergegebene Kosteneinsparungen und Effizienzgewinne, z.B. bei niedrigeren Gebühren in algorithmengestützter Anlageberatung, und durch Qualitätssicherung; vgl. WEBER/BAISCH, AJP 2016, S. 1069 f.

69 Art.-29-Gruppe, Leitlinien DSFA, S. 9.

70 DSK, DSFA-Liste.

Diese Liste zeigt, dass für Profiling auch nach der Art.-29-Datenschutzgruppe häufig eine DSFA durchzuführen ist. Der Schutz der Betroffenen verlangt dagegen nicht, bei Profiling immer eine DSFA durchzuführen.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 14. Juni 2019.

ARNING MARIAN, in: Flemming Moos/Jens Schefzig/Marian Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, Berlin 2018.

BÄCKER MATTHIAS, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, 2. Aufl. München 2018.

BETZ CHRISTOPH, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, S. 148-152.

BUCHNER BENEDIKT/PETRI THOMAS, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, 2. Aufl. München 2018.

EHMANN EUGEN, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

FRANCK LORENZ, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl. München 2018.

GOLA PETER, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

HLADJK JÖRG, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

KAMLAH WULF, in: Kai-Uwe Plath (Hrsg.), DSGVO/BDSG, 3. Aufl. Köln 2018.

MESTER ALEXANDRA, in: Jürgen Taeger/Detlev Gabel (Hrsg.), DSGVO – BDSG, 3. Aufl. Frankfurt a.M. 2019.

PAAL BORIS P./HENNEMANN, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl. München 2018.

ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz, Jusletter 27. November 2017.

ROSSNAGEL ALEXANDER, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, 2. Aufl. München 2018.

SCHOLZ PHILIP, in: Spiros Simitis/Gerrit Hornung/Indra Spieker genannt Döhmann (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, Baden-Baden 2019.

SCHULZ SEBASTIAN, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

SCHWEIZER RAINER J., in: Bernhard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung – St. Galler Kommentar, 3. Aufl., St. Gallen 2014.

VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter 16. November 2015.

VASELLA DAVID/SIEVERS JACQUELINE, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, S. 44-48.

VEIL WINFRIED, in: Sibylle Gierschmann/Katharina Schlender/Rainer Stentzel/Winfried Veil (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2018.

WEBER ROLF H./BAISCH RAINER, Regulierung von Robo-Advice, AJP 2016, S. 1065-1078.

WILDHABER ISABELLE, Robotik am Arbeitsplatz: Robo-Kollegen und Robo-Bosse, AJP 2017, S. 213-224.

Materialien

Europäische Union, Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union mitwirken, Luxemburg 2015, abrufbar unter <http://bit.ly/2MMbp8d> (zit. Leitfaden Rechtstexte).

Artikel-29-Datenschutzgruppe, Guidelines on the right to data portability, Arbeitspapier 242rev.01 vom 5. April 2017, abrufbar unter <http://bit.ly/31nNork> (zit. Art.-29-Gruppe, Leitlinien Datenportabilität).

Artikel-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679 vom 4. Oktober 2017, abrufbar unter <http://bit.ly/2XDPpOf> (zit. Art.-29-Gruppe, Leitlinien DSFA).

Artikel-29-Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Arbeitspapier 251rev.01 vom 6. Februar 2018, abrufbar unter <http://bit.ly/2XDOYn5> (zit. Art.-29-Gruppe, Leitlinien Profiling).

Artikel-29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679, Arbeitspapier 260rev.01 vom 11. April 2018, abrufbar unter <http://bit.ly/2AZ9Aff> (zit. Art.-29-Gruppe, Leitlinien Transparenz).

Artikel-29-Datenschutzgruppe, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects vom 9. April 2019, abrufbar unter <http://bit.ly/2ZpcUuv> (zit. Art.-29-Gruppe, Leitlinien Rechtsgrundlage Vertrag).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September, BBl 2017 6971 ff. (zit. Botschaft rev. DSG).

Der hessische Beauftragte für Datenschutz und Informationsfreiheit, 45. Tätigkeitsbericht 2016, abrufbar unter <http://bit.ly/2KUDXdn> (zit. 45. Tätigkeitsbericht Hessen).

Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, S. 7193 ff., abrufbar unter <http://bit.ly/2MPJa8M> (zit. E-DSG).

Europarat, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum, 23. November 2010, abrufbar unter <http://bit.ly/31ADBOF> (zit. Europarat, Empfehlung Profiling).

FINMA, Rundschreiben 2013/8 Marktverhaltensregeln – Aufsichtsregeln zum Marktverhalten im Effektenhandel vom 29. August 2013 (zit. RS 2013/8).

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK), Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Stand 17. Oktober 2018, abrufbar unter <http://bit.ly/2MQghZW> (zit. DSK, DSFA-Liste).

Schweizerische Bankiervereinigung, Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association, Oktober 2012 (zit. SBVg, Data Leakage Protection).

Vorentwurf des Bundesgesetzes über den Datenschutz vom 21. Dezember 2016, abrufbar unter <http://bit.ly/2RiKzmU> (zit. VE DSG).