Remo R. Schmidlin

Voice Recognition im Arbeitsverhältnis – eine datenschutzrechtliche Analyse

Im Arbeitsverhältnis wird Voice Recognition als Arbeitsmittel, Leistungsmessung, Zugangskontrolle oder Gesundheitsindikator verwendet. Der Einsatz von Voice Recognition muss in datenschutzrechtlicher Hinsicht einen genügend hinreichenden Arbeitsplatzbezug aufweisen. Entscheidend ist in vielen Fällen die Verhältnismässigkeit der Bearbeitung und, insb. bei Cloud-Lösungen, die Wahrung der erforderlichen Datensicherheit. Ist eine Einwilligung des Arbeitnehmers vorausgesetzt, sind hohe Hürden an die Freiwilligkeit zu setzen. Zudem muss sie in den meisten Fällen ausdrücklich sein. Durch die Revision des Datenschutzgesetzes werden Regelungskonzepte wie das Profiling, die Datenschutz-Folgenabschätzung, automatisierte Einzelentscheidungen und technische Anforderungen von der europäischen DSGVO übernommen. Allerdings bringt die Schweizer Ausgestaltung keine in der Praxis relevanten Änderungen im Zusammenhang mit Voice Recognition mit sich.

Zitiervorschlag:
REMO R. SCHMIDLIN, Voice Recognition im Arbeitsverhältnis – eine datenschutzrechtliche Analyse, sui generis 2022, S. 25

Remo R. Schmidlin, M.A. HSG in Law & Economics.

URL: sui-generis.ch/201
DOI: https://doi.org/10.21257/sg.201

I. Einführung

1 Während die technologische Ausschöpfung unserer Stimme noch vor wenigen Jahren lediglich aus dem Genre Science-Fiction zu vernehmen war, so lässt sie sich heute ganz gezielt nutzen und einsetzen. Zwangsläufig erhält die unter dem Stichwort *Voice Recognition* geläufige Technologie auch Einzug in die Arbeitswelt 4.0.[1] Mittlerweile können Computer mittels Spracherkennung die Befehle von Arbeitnehmern genau verstehen und ausführen. Dabei sind die Einsatzbereiche von Voice Recognition äusserst vielfältig. Dokumentation und Transkription ordnen sich noch unter den eher simplen Arbeitsmitteln ein. Lernbasierte Sprachassistenten vermögen dahingegen den Arbeitnehmer nicht nur zu unterstützen, sondern analysieren die persönliche Arbeitsweise ihres Benutzers und errechnen individuelle Handlungsvorschläge.[2] Weiter greifen sog. *People-Analytics*-Programme auf Stimm- und Sprachdaten zurück, indem sie bspw. Verhaltenscharakteristiken von Bewerbern auswerten.[3] Die v.a. aus Call-Centern bekannte Methode des *Keyword Spotting* erkennt verkaufsfördernde und kritische Schlüsselwörter[4] oder analysiert zusätzlich die Stimmung des Agenten während des Gesprächs.[5] Über die Stimme lässt sich darüber hinaus eine Zugangskontrolle über kritische Informationen und Ressourcen etablieren.[6] Ferner ermöglicht die Stimmanalyse die frühzeitige *Erkennung von Krankheiten*[7] oder die Messung der Stressbelastung am Arbeitsplatz.[8]

Gleichzeitig gewährt die Stimme aber auch Einblick in 2
die Persönlichkeit einer Person. Durch sie lässt sich eine Person eindeutig identifizieren und sie verrät vieles über die Charaktereigenschaften, das Verhalten und die Gesundheit. Dadurch wird eine Fülle an Daten erhoben und bearbeitet, was eine Gefahr für das individuelle Recht auf informationelle Selbstbestimmung darstellt, welches wiederum als *raison d'être* des Datenschutzrechts gilt.[9] Nach einem langandauernden Revisionsprozess steht seit 25. September 2020 nun die definitive Fassung des revidierten Datenschutzgesetzes bereit, welches sich dem Schutzniveau der europäischen DSGVO[10] angleichen und hinsichtlich moderner automatisierter Datenbearbeitungen mehr Rechtssicherheit bieten soll. Die folgende Analyse der Voice Recognition nimmt sich den datenschutzrechtlichen Neuerungen sogleich an.

II. Grundlagen der Voice Recognition

1. Definition

Voice Recognition ist eine Sammelbezeichnung für Tech- 3
nologien, die einen Sprecher anhand stimmspezifischer Merkmale identifizieren *(Stimmerkennung),*[11] den linguistischen Inhalt aus natürlich gesprochener Sprache extrahieren *(Spracherkennung)*[12] oder aufgrund der Stimme Rückschlüsse auf den Charakter, emotionalen Zustand oder Wahrheitsgehalt ziehen *(Stimmanalyse).*[13]

Die Stimmerkennung unterteilt sich wiederum in die *Sprecherverifikation,* bei der nur eine binäre Entscheidung 4
getroffen wird (gesuchter Sprecher: ja – nein) und die *Sprecheridentifikation,* wobei eine Vielzahl an möglichen Ergebnissen vorliegt.[14]

1 GAYE KARACAY, Talent Development for Industry 4.0, in: Ustundag/Cevikcan (Hrsg.), Industry 4.0: Managing the Digital Transformation, Cham 2018, S. 125.

2 CHRISTIAN JAKSCH, Datenschutzrechtliche Fragen des IT-gestützten Arbeitsplatzes, Wiesbaden 2020, S. 151 ff.

3 So bspw. Vima Link SA, Recruitment oder HireIQ, vgl. KEVIN G. HEGEBARTH, Emotional Assessments, 2015, S. 4 f.; MARIA CRISTINA CALDAROLA / JOACHIM SCHREY, Big Data und Recht, München 2019, Rz. 307; TOMAS CHAMORRO-PREMUZIC / REECE AKHTAR / DAVID WINSBOROUGH / RYNE A. SHERMAN, The datafication of talent, Curr. Opin. Behav. Sci. 2017, S. 14; GABRIEL KASPER / ISABELLE WILDHABER, Big Data am Arbeitsplatz, in: Kieser/Pärli/Uttinger (Hrsg.), Datenschutztagung 2018, Zürich 2018, S. 205.

4 PETER GOLA, Handbuch Beschäftigtendatenschutz, 8. Aufl., Frechen 2019, Rz. 549, 1136 und 1357; EBERHARD KIESCHE / MATTHIAS WILKE, Neue Überwachungsformen in Call-Centern, Computer und Arbeit 2012/4, S. 6.

5 Vgl. Xdroid International, Operations of VoiceAnalytics; KIESCHE/WILKE (Fn. 4), S. 6; MICHAEL ZOEBISCH, Stimmungsanalyse durch Call-Center, DuD 2011, S. 394.

6 So bspw. Swisscom AG, Höchste Sicherheit an der Swisscom Hotline dank Stimmerkennung, oder PostFinance AG, Authentifizierung mit Stimmerkennung; vgl. JOHN J. FAY, Access Control: People, Vehicles, Materials, in: Fay (Hrsg.), Encyclopedia of Security Management, 2. Aufl., Burlington (MA) 2007, S. 255 f.; NANCY YUE LIU, Bio-Privacy, Abingdon 2012, S. 42.

7 EVA WOLFANGEL, Was die Stimme über uns verrät, Technology Review vom 23. Januar 2019; THOMAS JÜNGLING, Diese Stimmanalyse entlarvt all unsere Geheimnisse, Welt vom 6. März 2015; BJÖRN W. SCHULLER, Maschinelle Profilierung durch KI, digma 2017, S. 206 f.

8 GINNY ENGHOLM, 5 Ways AI Can Keep Employees Engaged, HT Leads Business vom 6. Juni 2019; DIRK MÜLLER, Interview mit Kirsten Seegmüller, HR Software Guide 2019, S. 10.

9 Art. 1 DSG (Bundesgesetz über den Datenschutz vom 19. Juni 1992 [DSG; SR 235.1]); ROMY DAEDELOW, Wenn Algorithmen (unfair) über Menschen entscheiden…, Jusletter vom 26. November 2018, Rz. 4.

10 EU-Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl 2016 L 119/1.

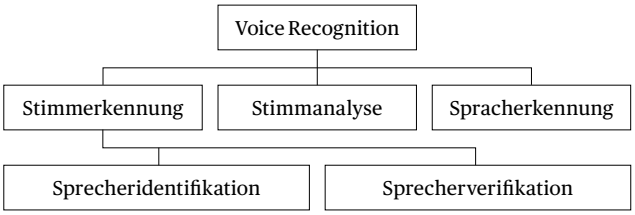
11 Vgl. ANIL K. JAIN / ARUN ROSS / SALIL PRABHAKAR, An Introduction to Biometric Recognition, IEEE TCSVT 2004, S. 10; DOMINIKA BLONSKI, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Bern 2015, S. 19.

12 VICTOR KEEGAN, Has voice recognition finally come of age?, The Guardian vom 13. Dezember 2007; DANIEL JURAFSKY / JAMES H. MARTIN, Speech and Language Processing, 2. Aufl., Upper Saddle River, New Jersey 2009, S. 319; BERND MÖBIUS / UDO HAIBER, Verarbeitung gesprochener Sprache, in: Carstensen et al. (Hrsg.), Computerlinguistik und Sprachtechnologie, 3. Aufl., Heidelberg 2010, S. 215.

13 AMIT KONAR / ANISHA HALDER / ARUNA CHAKRABORTY, Introduction to Emotion Recognition, in: Konar/Chakraborty (Hrsg.), Emotion Recognition. A Pattern Analysis Approach, Hoboken, New Jersey 2015, S. 7 ff.; SAVITA SONDHI / RITU VIJAY / MUNNA KHAN / ASHOK K. SALHAN, Voice Analysis for Detection of Deception, 11th International Conference KICSS 2016, S. 1 ff.

14 JURAFSKY/MARTIN (Fn. 12), S. 367.

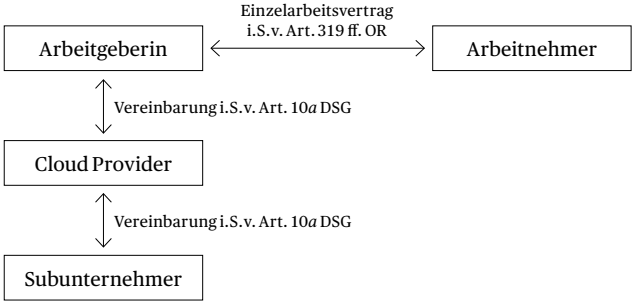
5 Im Zuge der Spracherkennung können gleichzeitig sprecherspezifische Eigenschaften, wie bspw. Wortwahl oder Sprechgeschwindigkeit identifiziert werden, die zur Spracheridentifikation bzw. -verifikation oder Stimmanalyse angewendet werden können.[15] Auch Kombinationen aus Stimm- und Spracherkennung sind denkbar, bspw. ein Mobiltelefon, das lediglich auf Sprachbefehle des Besitzers reagiert.[16] Letztlich ist der Stimmanalyse insofern eine Zwischenstellung zwischen der Stimm- und Spracherkennung beizumessen, als sie sowohl stimm- als auch sprachspezifische Merkmale analysiert, dabei aber einen eigenständigen Zweck verfolgt.[17]



Begriffliche Systematik der Voice Recognition

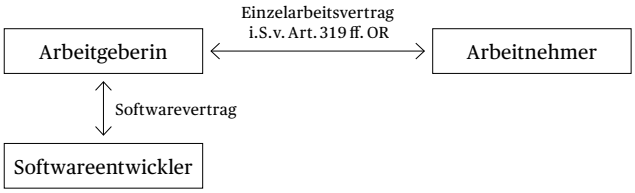
2. IT-Infrastruktur und Rechtsbeziehungen

6 Je nach Ausgestaltung der IT-Infrastruktur eines Voice Recognition Systems liegen verschiedene Rechtsbeziehungen vor. Bei *Cloud-Lösungen* wird die vertraglich vereinbarte Software über eine Applikation oder einen Browser unmittelbar in der Datenwolke ausgeführt *(Software as a Service)*.[18] Die Spracheingaben werden an einen Server übermittelt und analysiert, worauf die entsprechenden Befehle an das System retourniert werden.[19] Zwischen der Arbeitgeberin und dem Cloud-Provider muss eine Vereinbarung nach den Bestimmungen der Datenbearbeitung durch Dritte (Art. 10*a* DSG) bestehen.[20] Der Cloud-Provider kann zur Erbringung seiner Leistung auf die Infrastruktur, wie Netzwerk, Server oder Speicher, von Subunternehmern zurückgreifen.[21]



Vertragsbeziehungen Cloud Lösung

7 Bei reinen *Offline-Lösungen* findet die Bearbeitung stationär durch eine fest installierte Software statt. Offline-Lösungen sind v.a. in traditionell ausgestalteten Systemen vorherrschend oder wo hohe Anforderungen an die Datensicherheit gestellt werden.[22] Aufgrund der tieferen Leistungsfähigkeit und tendenziell höheren Kosten von Offline-Lösungen werden i.d.R. Cloud-Lösungen bevorzugt.[23] Je nach Ausgestaltung des konkreten Vertragsgegenstandes zwischen der Arbeitgeberin und dem Softwareentwickler kann ein Nominat- oder Innominatkontrakt vorliegen.[24] Entscheidend ist, dass aufgrund der lokalen Bearbeitung der Daten keine Datenbearbeitung Dritter vorliegt.



Vertragsbeziehungen Offline-Lösung

III. Voice Recognition im Geltungsbereich des Datenschutzrechts

1. Qualifikation von Stimm- und Sprachdaten

8 Eine fundamentale Unterscheidung beim Einsatz von Voice Recognition ist, ob das System *Stimm-* oder *Sprach*daten bearbeitet. Die *Stimme* ist ein biometrisches Merkmal[25] und weist als solches in jedem Fall einen Personenbezug auf. Während biometrische Daten unter dem

15 JERRY KAPLAN, Künstliche Intelligenz, Frechen 2017, S. 74.

16 GEORGE FREWAT et al., Android voice recognition application with multi speaker feature, 18th MELECON 2016, S. 1 ff.; FindBiometrics, Voice and Speech Recognition.

17 GOLA (Fn. 4), Rz. 1359; KONAR/HALDER/CHAKRABORTY (Fn. 13), S. 7 ff.; JOHANNES WAGNER / FLORIAN LINGENFELSER / ELISABETH ANDRÉ, Building a Robust System for Multimodal Emotion Recognition, in: Konar/Chakraborty (Hrsg.), Emotion Recognition. A Pattern Analysis Approach, Hoboken, New Jersey 2015, S. 387 f.; ZOEBISCH (Fn. 5), S. 6.

18 KIRSTIN BRENNSCHEIDT, Cloud Computing und Datenschutz, Baden-Baden 2013, S. 35 f.; THORSTEN HENNRICH, Cloud Computing, Berlin 2016, S. 69 f.

19 EDÖB, Schlussbericht im Zusammenhang mit der Datenbearbeitung der Microsoft Corporation im Rahmen von Windows 10, Bern 2016, S. 26 f.

20 BRENNSCHEIDT (Fn. 18), S. 59 f.; EDÖB, Erläuterungen zu Cloud Computing; BRUNO BAERISWYL, in: Baeriswyl/Pärli (Hrsg.), Stämpflis Handkommentar Datenschutzgesetz (DSG), Bern 2015, Art. 10a N 1 (zit. SHK DSG-BEARBEITERIN).

21 BRENNSCHEIDT (Fn. 18), S. 59; HENNRICH (Fn. 18), S. 70.

22 Fortune Business Insights, Speech and Voice Recognition Market; MILICA MATIĆ / IGOR STEFANOVIĆ / UNA RADOSAVAC / MILAN VIDAKOVIĆ, Challenges of Integrating Smart Home Automation with Cloud Based Voice Recognition Systems, 7th ICCE, Berlin 2017, S. 248 f.

23 GODSON MICHAEL D'SILVA / VINAYAK BHARADI / SHRIDHAR KAMBLE, Biometric Authentication using Software as a Service (SaaS) Architecture with Real-time Insights, ICCUBEA 2016, S. 2; MATIĆ/STEFANOVIĆ/RADOSAVAC/VIDAKOVIĆ (Fn. 22), S. 248.

24 Vgl. zur ausführlichen Qualifikation GIANNI FRÖHLICH-BLEULER, Rechtsprechung zum Software-Vertragsrecht, Jusletter vom 24. Januar 2011; DERS., Softwareverträge, Bern 2014, Rz. 14 ff.

25 BLONSKI (Fn. 11), S. 18; ZOEBISCH (Fn. 5), S. 395.

gegenwärtigen DSG grundsätzlich als «gewöhnliche» Personendaten zu qualifizieren sind,[26] gelten sie unter dem revidierten Datenschutzgesetz[27] als besonders schützenswerte Personendaten, wenn sie eine Person eindeutig identifizieren.[28] Diese Formulierung dürfte schon aufgrund der technischen Unmöglichkeit nicht so zu verstehen sein, dass das angewandte Verfahren eine hundertprozentige Sicherheit der Identifikation bewerkstelligt. Vielmehr bemisst sich der Erfolg des technischen Verfahrens anhand eines vordefinierten Schwellenwertes *(threshold)*.[29] So sind Aufnahmen der Stimme als biometrische Daten zu qualifizieren, wenn das Verfahren dem Zwecke der Identifikation dient.[30]

9 Lassen Stimmdaten Rückschlüsse auf die Gesundheit oder Rassenzugehörigkeit zu, so können bereits unter geltendem Recht besonders schützenswerte Daten vorliegen.[31] Entscheidend sind die Geeignetheit der Daten und der Bearbeitungszweck. Werden Anzeichen einer Depression diagnostiziert, liegen Gesundheitsdaten vor, hingegen genügen temporäre Gemütszustände oder der Wahrheitsgehalt einer Aussage nicht.[32] Zudem können Unterschiede in Aussprache, Wortwahl, Dialekt und syntaktischen Strukturen mit geografischen und sozialen Faktoren und letztlich der Rasse i.S.v. Ethnizität in Verbindung gebracht werden.[33]

10 Die *Sprache* – im Gegensatz zur Stimme – ist primär ein Medium, das dem Informationstransfer dient.[34] Diese Informationen sind als (besonders schützenswerte) Personendaten zu qualifizieren, wenn sie die gesetzlichen Anforderungen erfüllen.[35] Zu beachten ist jedoch, dass die Natur der Daten nicht im Voraus erkennbar und dementsprechend keine separate Bearbeitung realisierbar ist, womit konsequenterweise für sämtliche Sprachdaten der strengere Massstab der besonders schützenswerten Personendaten angelegt werden muss.[36] Fraglich ist allerdings, ob die Sprache an sich ein Personendatenwert sein kann. In der Regel werden Sprachdaten durch ein auf den Arbeitnehmer zurückzuführendes Endgerät bearbeitet. Folglich lassen sich die Daten regelmässig einer bestimmten Person zuordnen, wodurch ein Personenbezug anzunehmen ist. Dies gilt umso mehr für internetfähige Endgeräte, welche eine einmalige IP-Adresse besitzen.[37]

Ausserdem ist im Kontext von *Big Data* und *People Analytics* für einen weiten Anwendungsbereich des DSG zu plädieren. Moderne technische Möglichkeiten erlauben selbst bei eigentlich anonymisierten Daten eine Re-Identifizierung.[38] Insofern ist es schwer denkbar, dass man sich in der Bearbeitung von Stimm- und Sprachdaten ausserhalb des Geltungsbereiches des DSG bewegt. 11

2. Persönlichkeitsprofile / Profiling

Unter der Revision des DSG ersetzt das Profiling das bisherige Persönlichkeitsprofil.[39] Profiling setzt eine automatisierte Bearbeitung voraus, auf deren Basis persönliche Aspekte der betroffenen Person vorhergesagt oder beurteilt werden. 12

Das rDSG folgt einem risikobasierten Ansatz, sodass nur an Profiling mit hohem Risiko strengere Rechtsfolgen zu knüpfen sind. Ein solches liegt vor, wenn es mit einem hohen Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person verbunden ist. Dies ist wiederum nichts anderes als das Persönlichkeitsprofil unter geltendem Datenschutzrecht.[40] 13

Die Bearbeitung von Sprach- und Stimmdaten erfolgt bei Voice Recognition naturgemäss automatisiert. Sprach- 14

26 SUSAN EMMENEGGER / MARTINA REBER, Biometrische Daten im Bankkundenverkehr am Beispiel der Stimmauthentifizierung, in: Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019, S. 167; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, Bern 2009, S. 17; Blonski (Fn. 11), S. 79; PHILIPPE MEIER, Protection des données, Bern 2011, Rz. 2253 f.; teilweise wird vertreten, dass biometrische Daten Gesundheitsdaten *ergo* besonders schützenswerte Daten darstellen (Art. 3 lit. c Ziff. 2 DSG), vgl. FRANZISKA SPRECHER, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 2018, S. 494.

27 Revidiertes Bundesgesetz über den Datenschutz vom 25. September 2020 (rDSG, BBl 2020 7639), nicht in Kraft.

28 Art. 5 lit. c Ziff. 4 rDSG.

29 BLONSKI (Fn. 11), S. 14 f.; LIU (Fn. 6), S. 33.

30 DAVID ROSENTHAL, Der Entwurf für ein neues Datenschutzgesetz, Jusletter vom 27. November 2017, Rz. 8.

31 Art. 3 lit. c Ziff. 2 DSG.

32 ROLAND MATHYS, Was bedeutet Big Data für die Qualifikation als besonders schützenswerte Personendaten?, Jusletter IT vom 21. Mai 2015, Rz. 22 f.; DAVID VASELLA, Der EDÖB in 10vor10 zur Stimmerkennung bei Postfinance, *in fine*; a.M. wohl EMMENEGGER/REBER (Fn. 26), S. 167 f., wonach unabhängig vom Bearbeitungsvorgang besonders schützenswerte Daten vorliegen, wenn es objektiv möglich ist, aus den vorhandenen Daten Informationen über den Gesundheitszustand zu gewinnen.

33 SU LIN BLODGET / BRENDAN O'CONNOR, Racial Disparity in Natural Language Processing, S. 1 ff.; EDÖB (Fn. 26), S. 17.

34 Vgl. ZOEBISCH (Fn. 5), S. 395.

35 Hinzuweisen ist auf die Drei-Sphären-Theorie, vgl. BGE 97 II 97 E. 3; BGE 118 IV 41 E. 4; BGE 119 II 222 E. 2b; ferner GABOR P. BLECHTA, in: Maurer-Lambrou/Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz & Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, Art. 3 N 35 f. (zit. BSK DSG-BEARBEITERIN); MICHAEL SILVESTRO / JOHN BLACK, «Who Am I Talking To?», Business Law Today 2016/4, S. 4.

36 EDÖB (Fn. 19), S. 16.

37 Vgl. BGE 136 II 508 E. 3.2 und 3.5; ausführlich BARBARA WIDMER, Bei IP-Adressen kommt es darauf an…, digma 2017, S. 77.

38 KASPER/WILDHABER (Fn. 3), S. 212.

39 Art. 5 lit. f rDSG; zu den Unterschiedenen der Begrifflichkeiten vgl. Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 6941), S. 7022.

40 DAVID ROSENTHAL, Das neue Datenschutzgesetz, Jusletter vom 16. November 2020, Rz. 27; DAVID VASELLA, Überlegungen zum Profiling mit hohem Risiko, datenrecht vom 23. November 2020.

erkennende Systeme betreiben Profiling, wenn persönliche Aspekte des Nutzers bewertet werden. *Sprachassistenten* können den Arbeitnehmer mitunter bezüglich Interessen, beruflichen Schwerpunkten und persönlichen Präferenzen analysieren und ggf. darauf basierend selbständige Handlungen vornehmen.[41] Profiling im *Rekrutierungsprozess* liegt vor, wenn Charakterzüge, der emotionale Zustand oder die Arbeitsweise des Bewerbers analysiert werden.[42] Stimmanalysierende Zutrittskontrollen betreiben nur Profiling, wenn die Anzahl der Zutrittskontrollen griffige Rückschlüsse auf den Bewegungsablauf, das Verhalten oder den Aufenthaltsort eines Arbeitnehmers ermöglichen.[43]

15 Offen bleibt, ob durch das Profiling Persönlichkeitsprofile entstehen, die zu einem hohen Risiko für die betroffene Person führen. Dies hängt wiederum von den im konkreten Fall getroffenen Schutzmassnahmen ab.[44]

IV. Ausgewählte datenschutzrechtliche Problemfelder

1. Bearbeitung innerhalb des arbeitsrelevanten Bereichs

16 Der Datenschutz ist in seiner Natur vordergründig Persönlichkeitsschutz.[45] Gemäss Art. 328*b* OR[46] liegt im Arbeitsverhältnis eine persönlichkeitsverletzende Datenbearbeitung vor, wenn sie über den für das konkrete Arbeitsverhältnis relevanten Bereich hinaus geht.[47]

17 Der wohl herrschende Teil der Lehre betrachtet die Norm als Verbotsnorm, was ein Durchbruch zum Prinzip der grundsätzlichen Erlaubnis mit Verbotsvorbehalt aufzufassen ist.[48] Die Berufung auf einen Rechtfertigungsgrund i.S.v. Art. 13 DSG[49] wäre folglich nicht möglich.[50] Nach einer liberaleren und hier vertretenen Ansicht ist Art. 328*b* OR als ein auf das Arbeitsverhältnis beschränkter Bearbeitungsgrundsatz zu verstehen,[51] der den Grundsatz der Verhältnismässigkeit konkretisiert.[52] In diesem Sinne ist eine Verletzung von Art. 328*b* OR ebenso durch einen Rechtfertigungsgrund heilbar.[53]

18 Ein Arbeitsplatzbezug ist insb. bei der Verwendung von Spracherkennung als Arbeitsmittel zu bejahen. Beim *Keyword Spotting* oder der Stimmanalyse ist ein solcher ebenfalls zu vermuten, sofern sich die Analyse der Leistung oder des Verhaltens betrieblich begründen lässt.[54] Dabei ist aber insb. zu berücksichtigen, wie flächendeckend solche Analysen durchgeführt werden, ob auch private Unterhaltungen ausgewertet werden und ob die Analyse dem Arbeitnehmer bekannt ist.[55]

19 Charaktereigenschaften wie Belastbarkeit, Teamfähigkeit oder Kommunikationsfähigkeit zählen zu den beruflichen Qualifikationen, weshalb bei Stimm- und Sprachanalysen *im Bewerbungsverfahren* ebenfalls ein Arbeitsplatzbezug zu vermuten ist.[56] Die Analyse weiterer Charaktereigenschaften, die der persönlichen Qualifikation zuzurechnen sind, kann sich im konkreten Fall ebenfalls aufdrängen, besonders wenn dies aufgrund von Haftungs- und Reputationsrisiken geboten ist.[57] Dieselben Überlegungen sind auch *während des Arbeitsverhältnisses* anzustellen. Anders ist die Rechtslage hingegen, wenn anhand von bestehenden Schlüsselmitarbeitern ein Wunschprofil als Referenz für Bewerbende erstellt wird. In diesem Fall erfolgt die Bearbeitung nicht im Zusammenhang mit dem persönlichen Arbeitsverhältnis.[58]

20 Biometrische Stimmdaten, die zur Identifikation oder Verifikation verwendet werden, weisen einen Arbeitsplatz-

41 JAKSCH (Fn. 2), S. 169.

42 GOLA (Fn. 4), Rz. 551 ff.; ebenso die Legaldefinition in Art. 5 lit. f rDSG.

43 GOLA (Fn. 4), Rz. 1226; FLORIAN HÖLD, Die Überwachung von Arbeitnehmern, Hamburg 2006, S. 57.

44 Vgl. ROSENTHAL (Fn. 40), Rz. 27.

45 Art. 1 DSG; BSK DSG-RAMPINI, Vor Art. 12-15 N 3.

46 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 20. März 1911 (OR; SR 220).

47 WOLFGANG PORTMANN / ROGER RUDOLPH, in: Lüchinger/Oser (Hrsg.) Basler Kommentar Obligationenrecht I, 7. Aufl., Basel 2019, Art. 328b N 7 (zit. BSK OR-BEARBEITERIN).

48 GABRIEL AUBERT, La protection des données dans les rapports de travail, in: Aubert (Hrsg.), Journée 1995 de droit du travail et de la sécurité social, Zürich 1999, S. 149 f.; ADRIAN STAEHELIN, Zürcher Kommentar zum Schweizerischen Zivilrecht, Bd. V/2/c, Der Arbeitsvertrag Art. 319-330a OR, 4. Aufl., Zürich 2006, Art. 328b N 1; ULLIN STREIFF / ADRIAN VON KAENEL / ROGER RUDOLPH, Praxiskommentar Arbeitsvertrag, 7. Aufl., Zürich 2012, Art. 328b N 3 (zit. STREIFF/VON KAENEL/RUDOLPH).

49 Vgl. Rz. 33 ff.

50 STREIFF/VON KAENEL/RUDOLPH, Art. 328b N 3.

51 MEIER (Fn. 26), Rz. 2037; ROBERTA PAPA / THOMAS PIETRUSZAK, Datenschutz im Personalwesen, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, Basel 2015, Rz. 17.8; BSK OR-PORTMANN/RUDOLPH, Art. 328b N 23 und 26; DAVID ROSENTHAL / YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich et al. 2008, Art. 328b OR N 5 ff. (zit. HK-ROSENTHAL/JÖHRI); KASPER/WILDHABER (Fn. 3), S. 197 f.

52 Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG) (BBl 1988 II 413), S. 488; gleichfalls dürfte in Art. 328b OR aber auch der Grundsatz der Zweckbindung verkörpert sein, vgl. PAPA/PIETRUSZAK (Fn. 51), Rz. 17.5.

53 HK-ROSENTHAL/JÖHRI, Art. 328b OR N 12; KASPER/WILDHABER (Fn. 3), S. 197 f.

54 Vgl. BSK OR-PORTMANN/RUDOLPH, Art. 328b N 41.

55 Vgl. BSK OR-PORTMANN/RUDOLPH, Art. 328b N 41.

56 KASPER/WILDHABER (Fn. 3), S. 201.

57 SHK DSG-PÄRLI, Art. 328b OR N 27; BSK OR-PORTMANN/RUDOLPH, Art. 328b N 37; HKROSENHTAL/JÖHRI, Art. 328b OR N 36; KASPER/WILDHABER (Fn. 3), S. 202.

58 KASPER/WILDHABER (Fn. 3), S. 195.

bezug auf, sofern sie für Sicherheitszwecke notwendig sind.[59] Werden anhand von Stimmdaten Krankheiten diagnostiziert, liegt i.d.R. kein Arbeitsplatzbezug vor.[60]

2. Arbeitnehmerüberwachung

21 Das Abhören und die Aufnahme fremder Gespräche ist gemäss Art. 179bis StGB[61] verboten. Die Norm dürfte allerdings im Zusammenhang mit Voice Recognition kaum einschlägig sein. Zunächst wäre im Einzelfall zu klären, ob die registrierte Sequenz überhaupt ein Gespräch i.S. eines Gedanken- und Informationsaustausches darstellt.[62] Die definitionsgemäss vorausgesetzte Einwilligung kann ausdrücklich oder stillschweigend erfolgen,[63] wodurch sie sich bereits konkludent durch die Aktivierung des entsprechenden Systems ergibt. Bei fortlaufend aktiven Systemen kann die Einwilligung auch in Form einer arbeitsvertraglichen Klausel vorliegen.[64] Zudem schränkt Art. 179^{quinquies} Abs. 1 StGB den Anwendungsbereich von Art. 179bis StGB zusätzlich ein.

22 Relevanter dürfte Art. 26 ArGV 3[65] sein, der den Einsatz von Überwachungs- und Kontrollsystemen verbietet, sofern sie nicht aus anderen Gründen, wie namentlich zur Sicherheits- oder Leistungsüberwachung, erforderlich sind.[66] Solche Systeme dürfen die Gesundheit und Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigen.[67] Die Abgrenzung von zulässigen und unzulässigen Systemen ist bisweilen problematisch, zumal Leistung und Verhalten stark miteinander verknüpft sind.[68] Die Zulässigkeit ist letztlich von der *Verhältnismässigkeit* (Art. 4 Abs. 2 DSG)[69] der konkreten Einsatzweise abhängig und inwieweit die Arbeitgeberin berechtigte Betriebsinteressen geltend machen kann.[70] Liegen besonders schützenswerte Daten vor, ist grundsätzlich Zurückhaltung gefragt.[71] In jedem Fall ist die Datenbearbeitung auf den konkreten Informationsbedarf der Arbeitgeberin zu beschränken und die Arbeitnehmer vorgängig anzuhören (Art. 5 und 6 ArGV 3).[72]

Sprachgesteuerte Systeme sind regelmässig durch Produktivitätsgewinne rechtfertigbar. Hingegen sind sie unzumutbar, wenn sie gleichzeitig die Identität oder Gemütslage analysieren oder generell lückenlos aufzeichnen, was auch private Unterhaltungen beinhalten kann.[73] 23

Das *Verhalten* des Arbeitnehmers gegenüber Kunden oder Geschäftspartnern stellt grundsätzlich eine zulässige Leistungskontrolle dar. Erfolgt nun aber eine Stimmanalyse oder Keyword Spotting andauernd und lückenlos, liegt ein unzulässiges Überwachungssystem vor.[74] Es ist allerdings zu beachten, dass die Arbeitgeberin ein berechtigtes Interesse daran hat, die Leistung der Arbeitnehmer zu überwachen. Es ist deswegen erforderlich, die Zwecke der eingesetzten Systeme genau zu bestimmen und nicht erforderliche Datenbearbeitungen klar abzugrenzen.[75] M.a.W. kommt dem Grundsatz der *Zweckbindung* (Art. 4 Abs. 3 DSG) grosse Bedeutung zu. In der Bewerbungsphase gesammelte Stimm- und Sprachdaten dürfen nicht zur Persönlichkeitsdurchleuchtung oder für das anschliessende Arbeitsverhältnis verwendet werden, wenn dies nicht vom Bewerber akzeptierten Zweck gedeckt ist.[76] Allgemein dürfen Stimm- und Sprachdaten nicht über längere Zeit systematisch gesammelt und verwaltet werden (sog. *Data Warehousing*) oder ggf. mit anderen Daten kombiniert werden (sog. *Data Mining*). Entstehen dadurch neue sog. Sekundärdaten, werden diese i.d.R. nicht vom ursprünglich angegebenen Zweck erfasst, zumal dieser bei der Datenbeschaffung gar nicht ersichtlich sein konnte.[77] 24

Zugangskontrollen, die mittels Stimmerkennung Stimmdaten bearbeiten, sind so zu gestalten, dass keine Erstellung eines Verhaltensprofils des Arbeitnehmers möglich ist, d.h. keine detaillierten Bewegungsabläufe ersichtlich 25

59 HK-ROSENTHAL/JÖHRI, Art. 328b OR N 41; BLONSKI (Fn. 11), S. 274 f.

60 Vgl. EDÖB, 17. Tätigkeitsbericht 2009/2010 – Gesundheitscheck für die Mitarbeiter der Post, Bern 2009, S. 69 f.; EDÖB, 22. Tätigkeitsbericht 2014/2015 – Gesundheitsfragebogen bei Bewerbungsverfahren, Bern 2105, S. 55 f.

61 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

62 Vgl. EMMENEGGER/REBER (Fn. 26), S. 173 f. unter Bezugnahme auf Art. 179^{quinquies} StGB.

63 Botschaft vom 21. Februar 1986 über die Verstärkung des Schutzes des persönlichen Geheimbereichs (BBl 1968 I 585), S. 593.

64 EDÖB, Erläuterungen zur Telefonüberwachung am Arbeitsplatz, Bern 2014, S. 5.

65 Verordnung 3 zum Arbeitsgesetz vom 18. August 1993 (ArGV 3, Gesundheitsschutz; SR 822.113).

66 PAPA/PIETRUSZAK (Fn. 51), Rz. 17.22; SECO, Wegleitung zu den Verordnung 3 und 4 zum ArG, S. 326-1.

67 Art. 26 Abs. 2 ArGV 3.

68 SECO (Fn. 66), S. 326-1; SIMON WOLFER, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich 2008, Rz. 60; ebenso BGE 130 II 425 E. 4.3.

69 Die Interessensabwägung fällt mit der Verhältnismässigkeitsprüfung nach DSG zusammen, Urteil des Bundesgerichts 9C_785/2010 vom 10. Juni 2011 E. 6.6.

70 SECO (Fn. 66), S. 326-4.

71 Vgl. ISABELLE WILDHABER, Die Roboter kommen, ZSR 2016, S. 348.

72 ISABELLE WILDHABER, Robotik am Arbeitsplatz, AJP 2017, S. 219; SECO (Fn. 66), S. 326-7; PAPA/PIETRUSZAK (Fn. 51), Rz. 17.55.

73 Dadurch könnten gemäss der Drei-Sphären-Theorie des Bundesgerichts Informationen der Intimsphäre vorliegen, vgl. Fn. 35.

74 Siehe dazu Urteil des Bundesgerichts 6B_536/2009 vom 12. November 2009 E. 3.6.2; Urteil des Bundesgerichts 9C_785/2010 vom 10. Juni 2011 E. 6.3; KIESCHE/WILKE (Fn. 4), S. 8; PAPA/PIETRUSZAK (Fn. 51), Rz. 17.55; WOLFER (Fn. 68), Rz. 564.

75 WILDHABER (Fn. 72), S. 219

76 KASPER/WILDHABER (Fn. 3), S. 205.

77 ASTRID EPINEY, Allgemeine Grundsätze, in: Belser/Epiney/Waldmann (Hrsg.), Datenschutzrecht, Bern 2011, Rz. 34; STEFAN GERSCHWILER et al., Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, Basel 2015, Rz. 3.86.

sind.[78] Zugangskontrollen sind auf sensible Räumlichkeiten und Ressourcen zu beschränken. Weiter ist von einer zentralen Speicherung von biometrischen Daten abzusehen.[79] Denkbar ist die Hinterlegung des Stimmabdrucks auf einer Smartcard oder dem dienstlichen Mobiltelefon.[80] Überdies sind Systeme vorzuziehen, die keine abschliessende Identifikation vornehmen, sondern durch anonymisierte Daten abgleichen, ob der konkrete Mitarbeiter zum Kreis der berechtigten Personen gehört.[81]

3. Verlust von Arbeitnehmerdaten

26 Die Anwendung von Voice Recognition stellt die Datensicherheit in verschiedener Hinsicht vor Herausforderungen. Namentlich bei Sprachassistenten, die sich durch einen Schlüsselbegriff aktivieren und daher permanent aufzeichnen, besteht ein gewisses Abhör- und Manipulationsrisiko.[82]

27 Der Datenschutz soll den Einsatz von Cloud-Lösungen nicht unnötig beschränken.[83] Regelmässig ist die Auslagerung gar wünschenswert, namentlich wenn der Cloud-Provider spezialisierte Ressourcen zur Erfüllung der datenschutzrechtlichen Anforderungen aufweist.[84] Es ist indes zu beachten, dass die Auslagerung in die Cloud einen Kontrollverlust über die Daten mit sich bringt.[85] Es obliegt somit der Verantwortung der Arbeitgeberin, den Cloud-Provider entsprechend auszuwählen, die richtigen Instruktionen zu erteilen und zu überwachen.[86] Die zu treffenden Massnahmen hängen im Einzelfall von der Arbeitgeberin, der Sensitivität der Daten sowie der Organisation der eingesetzten Cloud-Lösung ab.[87] Werden Daten verschiedener Nutzer in der Cloud ungenügend isoliert, steigt das Risiko für Konsolidierungsschäden, wie *Distributed Denial of Services* oder *Hacker*-Attacken.[88]

Der Cloud-Provider muss die Datenbearbeitungen verschiedener Cloud-Nutzer strikt voneinander getrennt ausführen und darum besorgt sein, dass es zu keiner Durchmischung der Daten kommt. Es empfiehlt sich deswegen, Datenschutz-Qualitätszeichen oder Zertifizierungen zu berücksichtigen[89] und im Rahmen der Auftragsdatenbearbeitung festzuhalten, dass der Cloud-Provider die angemessenen Massnahmen im Rahmen des Gesetzes kennt und erfüllt.[90] Tritt dennoch ein ungewollter Verlust oder eine Offenlegung von Daten ein, so lässt sich eine Informationspflicht aus dem Grundsatz von Treu und Glauben ableiten. [91]

Biometrische Daten bergen zudem die latente Gefahr des Identitätsdiebstahls.[92] Der Grundsatz der Datensicherheit muss auf allen Ebenen eines Erkennungssystems beachtet werden. Voice-Recognition-Systeme sollten lediglich die zum Identifikationsabgleich erforderlichen Merkmale extrahieren, die Rohdaten aber wieder vernichten. Im Weiteren sollten die Daten nur komprimiert und/oder verschlüsselt bearbeitet werden.[93] Zudem ist, wenn immer möglich, eine dezentrale Speicherung der Daten zu bevorzugen.[94] 28

4. Datenrichtigkeit

Die Arbeitgeberin ist gem. Art. 5 Abs. 1 DSG verpflichtet, die Richtigkeit der Daten sicherzustellen. Die digitale Verarbeitung der Sprache und Stimme ist ein komplexer Vorgang, bei dem an verschiedenen Stellen Fehler auftreten können, was konsequenterweise zu unrichtigen Daten führt. Zudem sind die der Voice Recognition zugrundeliegenden Algorithmen oft so komplex, dass ein allfälliger Fehler in der Bearbeitung im Nachhinein kaum rekonstruierbar ist *(Black-Box-Problematik)*.[95] Präventiv wirkende technische Massnahmen dürften daher vermehrt in den Vordergrund rücken.[96] 29

Sprachassistenten können Eingaben falsch verstehen und in der Folge falsche Präferenzen für den Arbeitnehmer 30

78 WOLFER (Fn. 68), Rz. 392 ff.; vgl. auch BGE 130 II 425 E. 5 zur Erfassung von GPS-Daten.

79 Urteil des Bundesverwaltungsgerichts A3908/2008 vom 4. August 2009 E. 3; EDÖB (Fn. 26), S. 8; BSK DSG-MAURER-LAMBROU/STEINER, Art. 4 N 22.

80 Vgl. PASTUKHOV OLEKSANDR / KINDT ELS, Voice Recognition: Risks To Our Privacy, Forbes vom 6. Oktober 2016; THOMAS PROBST, Biometrie aus datenschutzrechtlicher Sicht, in: Nolde/Leger (Hrsg.), Biometrische Verfahren, Köln 2002, S. 121.

81 EDÖB (Fn. 26), S. 7 und 22.

82 Bundesbeauftragte für den Datenschutz und Informationsfreiheit (BfDI), Datenschutz kompakt – Sprachassistenten, Bonn 2017, S. 1 f.; HEIRES KATHERINE, The Risks of Voice Technology, Risk Management Magazine vom 2. Oktober 2017.

83 Vgl. Botschaft zum Bundesgesetz über den Datenschutz (DSG) (Fn. 52), S. 463.

84 HK-ROSENTHAL/JÖHRI, Art. 10a DSG N 81 f.

85 EDÖB (Fn. 20).

86 Botschaft zum Bundesgesetz über den Datenschutz (DSG) (Fn. 52), S. 464.

87 EDÖB (Fn. 20).

88 BfDi (Fn. 82), S. 2; EDÖB (Fn. 20); SILVESTRO/BLACK (Fn. 35), S. 4.

89 BSK DSG-BÜHLER/RAMPINI, Art. 10a N 15a.

90 EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, Bern 2015, S. 19; BSK DSG-STAMMPFISTER, Art. 7 N 12; BSK DSG-BÜHLER/RAMPINI, Art. 10a N 22d.

91 SHK DSG-BAERISWYL, Art. 4 N 18; EPINEY (Fn. 77), Rz. 22; HK-ROSENTHAL/JÖHRI, Art. 4 DSG N 16.

92 MEIER (Fn. 26), Rz. 2248.

93 Vgl. SILVESTRO/BLACK (Fn. 35), S. 4.

94 Vgl. Rz. 25; ausführlich EDÖB, Schlussbericht vom 13. September 2010, Verwendung biometrischer Daten für das Reservationssystem des Tennisclub XX, S. 18; ebenso EDÖB (Fn. 26), S. 20 f.; MEIER (Fn. 26), Rz. 2286.

95 IFEOMA AJUNWA / KATE CRAWFORD / JASON SCHULTZ, Limitless worker surveillance, California Law Review 2017, S. 132; DANILO DONEDA / VIRGILIO A.F. ALMEIDA, What Is Algorithm Governance, IEEE Internet Computing 2016/4, S. 60 f.

96 Vgl. Rz. 43 f.

ableiten. Ein Assistent sollte demnach so gestaltet sein, dass falsche Eingaben unkompliziert bspw. im Nutzerprofil abgeändert oder gelöscht werden können.[97]

31 Obschon ein tendenziell konstantes biometrisches Merkmal,[98] kann sich die *Stimme* im Laufe der Zeit verändern.[99] Es ist deswegen eine angemessene Akzeptanzschwelle *(threshold)* zu definieren[100] und der Stimmabdruck in regelmässigen Abständen zu aktualisieren. In diesem Zusammenhang bieten Cloud-Lösungen den Vorteil einer fortlaufenden Echtzeitanalyse *(continuous real-time analysis),* wodurch die Stimmdaten in einem dynamischen Prozess aktualisiert werden.[101]

32 Der Einsatz von Cloud-Lösungen entbindet die Arbeitgeberin nicht von der Gewährleistung der Datenrichtigkeit.[102] Es scheint aber angebracht, den Cloud-Betreiber, der regelmässig über sämtliche Daten verfügt, im Rahmen der Auftragsdatenbearbeitung entsprechend zu beauftragen.[103]

5. Rechtfertigungsgründe

33 Im Allgemeinen ist bei der Anwendung von Rechtfertigungsgründen Zurückhaltung zu üben.[104] Im Kontext eines Arbeitsverhältnisses ist umstritten, ob die Rechtfertigungsgründe nach Art. 13 DSG überhaupt aufgerufen werden können. Nach der hier vertretenen Auffassung ist dieser Umstand zu bejahen.[105]

34 In der Arbeitswelt dürfte die Einwilligung in der Praxis der bedeutsamste Rechtfertigungsgrund darstellen. Private Interessen könnten zwar in Form von wirtschaftlichen Interessen angeführt werden, eignen sich jedoch kaum zur Rechtfertigung einer Persönlichkeitsverletzung.[106] Das rDSG anerkennt, in Anlehnung an Art. 6 Abs. 1 lit. b DSGVO, ein überwiegendes privates Interesse, wenn die Bearbeitung in unmittelbarem Zusammenhang mit einem Vertragsverhältnis steht, somit bspw. wenn sie zwecks Abklärung der Eignung eines Arbeitnehmers für eine konkrete Stelle erfolgt.[107] Aber auch dieser Aspekt dürfte im spezifischen Anwendungsgebiet des Arbeitsvertrages aufgrund der Anforderungen von Art. 328*b* OR in den Hintergrund treten.[108] Öffentliche Interessen sind in privatrechtlichen Verhältnissen ohnehin von nebensächlicher Bedeutung.[109] Sodann ist keine Gesetzesbestimmung ersichtlich, welche als Rechtfertigungsgrund herangezogen werden könnte.

35 Bei der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen, resp. beim Profiling mit hohem Risiko unter revidiertem Recht, muss die Einwilligung ausdrücklich erfolgen (Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 7 rDSG).

36 Die Arbeitgeberin hat den Arbeitnehmer bezüglich allfälliger Risiken der Datenbearbeitung in der Cloud aufzuklären.[110] Bei Stimmanalysen genügt die Information, dass Gespräche zu Trainingszwecken analysiert werden können, nicht. Die Arbeitgeberin muss darüber aufklären, was mit den Daten geschieht und in welchem Umfang sie verwendet werden, damit der Arbeitnehmer die Tragweite der Einwilligung einschätzen kann.[111] Überdies muss die Arbeitgeberin bei der Verwendung eines Stimmabdruckes ausdrücklich über die Risiken aufklären, die mit der Nutzung des biometrischen Datenwerts einhergehen und welche Massnahmen sie dagegen ergreift.[112]

37 An die *Freiwilligkeit* sind im Arbeitsverhältnis hohe Anforderungen zu stellen.[113] Bei *Bewerbern,* die in Datenbearbeitungen einwilligen, um ihre Chancen in weiteren Runden für die Stelle überhaupt aufrecht erhalten zu können, fehlt es wohl an der Freiwilligkeit.[114] Indessen ist zu berücksichtigen, dass die Einwilligung ohnehin obsolet wird, wenn die Bearbeitung für die Eignung des Arbeitsverhältnisses erforderlich ist.[115] Stehen für biometrische Eintrittskontrollen keine Alternativen bereit, ist die Freiwilligkeit der Einwilligung des Arbeitnehmers fraglich.[116] Es kann indessen nicht erwartet werden, dass die Arbeitgeberin in jedem Fall eine Alternative zur Stimmerkennung zur Verfügung stellen muss. Ob alternative Zugangsmechanismen eingerichtet werden müssen, hängt insb. von der Sensitivität der zu schützenden Ressourcen oder Räumlichkeiten ab.[117]

97 JAKSCH (Fn. 2), S. 197.
98 BLONSKI (Fn. 11), S. 18.
99 LISA MYERS, An Exploration of Voice Biometrics, S. 5.
100 EDÖB (Fn. 26), S. 8.
101 D'SILVA/BHARADI/KAMBLE (Fn. 23), S. 2.
102 BSK DSG-MAURER-LAMBROU/SCHÖNBÄCHLER, Art. 5 N 11.
103 BARBARA WIDMER, Auftragsdatenbearbeitung – zum Vierten, digma 2014, S. 173.
104 BGE 136 II 508 E. 5.2.4.
105 Eingehend Rz. 16 ff.
106 Vgl. BGE 138 II 346 E. 10.4 und 10.6; ebenso ANDREAS MEILI, in: Geiser/Fountoulakis (Hrsg.) Basler Kommentar Zivilgesetzbuch I, 6. Aufl., Basel 2018, Art. 28 N 49; EMMENEGGER/REBER (Fn. 26), S. 181 f.
107 Art. 31 Abs. 2 lit. a rDSG.
108 Vgl. Rz. 16 ff.
109 BSK DSG-RAMPINI, Art. 13 N 47; HK-ROSENTHAL/JÖHRI, Art. 13 DSG N 20.
110 SHK DSG-BAERISWYL, Art. 4 N 61; vgl. Rz. 27.
111 KIESCHE/WILKE (Fn. 4), S. 9.
112 Vgl. EMMENEGGER/REBER (Fn. 26), S. 177.
113 BSK DSG-RAMPINI, Art. 13 N 6; EPINEY (Fn. 77), Rz. 18.
114 KASPER/WILDHABER (Fn. 3), S. 225.
115 Vgl. Rz. 34.
116 Vgl. Urteil des Bundesverwaltungsgerichts A3908/2008 vom 4. August 2009 E. 4.5; EDÖB (Fn. 26), S. 15.
117 MEIER (Fn. 26), Rz. 859 und 2289 ff.

V. Neue Instrumente unter dem revidierten Datenschutzgesetz

1. Automatisierte Einzelentscheidung

38 Mit Art. 21 rDSG enthält das Konzept der automatisierten Einzelentscheidung Einzug in das Datenschutzrecht. Im Gegensatz zum europäischen (als Recht formuliertes) Verbot von automatisierten Einzelentscheidungen[118] statuiert das Schweizer Pendant lediglich eine Informationspflicht des Verantwortlichen.[119]

39 *Stimmerkennende Zutrittskontrollen* funktionieren i.d.R. automatisiert. Es ist allerdings anzuzweifeln, dass diese Entscheidung über die geforderte Komplexität verfügt. Rudimentäre Wenn-Dann-Entscheidungen werden vom gesetzlichen Begriff nicht abgedeckt. Vielmehr muss dem System hinsichtlich der Entscheidung ein gewisser Interpretationsspielraum zukommen.[120]

40 Vollständig automatisierte Einzelentscheidungen können vorliegen, wenn *Sprachassistenten* selbständig Handlungen vornehmen, wie bspw. automatisierte Terminplanung oder Dienstreisebuchungen.[121]

41 Entscheidet ein *Rekrutierungssystem* über die Berücksichtigung eines Kandidaten,[122] ist zunächst ausschlaggebend, ob das System gänzlich autonom entscheidet oder der Endentscheid von einer Person zumindest beeinflusst werden kann.[123] Zudem muss die Entscheidung mit einer Rechtsfolge verbunden sein oder die betroffene Person erheblich beeinträchtigen. Der Nichtabschluss eines Vertrages zieht noch keine rechtlichen Folgen nach sich,[124] jedoch ist die Arbeitsstelle grundsätzlich jenen Bereichen zuzuordnen, die eine hohe Bedeutung für die individuelle Lebenssituation und -gestaltung aufweisen. Der Arbeitnehmer ist aus wirtschaftlicher Sicht abhängig vom Entscheid im Rekrutierungsprozess und wird dadurch erheblich beeinträchtigt.[125] Die Kündigung eines *bestehenden Arbeitsverhältnisses* ist klar mit einer Rechtsfolge verbunden und fällt folglich in den Anwendungsbereich von Art. 21 rDSG.[126]

2. Datenschutz-Folgenabschätzung

42 In Art. 22 schreibt das rDSG neu eine Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung vor, wenn die Datenbearbeitung voraussichtlich mit einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person einhergeht. Ein solches kann sich namentlich aufgrund der Art der Daten oder der Art und dem Zweck der Bearbeitung manifestieren.[127] Werden besonders schützenswerte Personendaten umfangreich bearbeitet, so ist die Datenschutz-Folgenabschätzung in jedem Fall durchzuführen.[128] Im Umkehrschluss dürften gelegentliche Bearbeitungen der Stimme, wie der situationsbedingte Abgleich des Stimmabdruckes unterhalb der Hürde der Datenschutz-Folgenabschätzung liegen. Im Grundsatz gilt: Je umfangreicher die Bearbeitung besonders schützenswerter Personendaten, desto eher drängt sich eine Datenschutz-Folgenabschätzung auf, bspw. wenn ein Rekrutierungsprozess unter Zuhilfenahme der Stimmanalyse mit einer Vielzahl von Bewerbern durchgeführt wird.

3. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

43 Die Arbeitgeberin muss durch technische und organisatorische Massnahmen sicherstellen, dass die Datenschutzvorschriften eingehalten werden *(Privacy by Design)*[129] und mittels geeigneter Voreinstellungen dafür sorgen, dass die Bearbeitung möglichst datenschutzfreundlich erfolgt *(Privacy by Default)*[130].

44 Privacy by Design ist im Grunde nichts Neues, zumal bereits heute die Voraussetzungen für eine datenschutz-

118 Vgl. Art. 22 DSGVO; Art. 9 Abs. 1 lit. a SEV 108 (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [SEV]); vgl. m.w.H. FLORENT THOUVENIN / ALFRED FRÜH / DAMIAN GEORGE, Datenschutz und automatisierte Entscheidungen, Jusletter vom 26. November 2018, Rz. 23 und 26; Art. 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, Brüssel 6. Februar 2018, S. 12.

119 Ausführlich Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 39), S. 7056; ebenso ROSENTHAL (Fn. 30), Rz. 100; THOUVENIN/FRÜH/GEORGE (Fn. 118), Rz. 27.

120 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 39), S. 7057; ROSENTHAL (Fn. 40), Rz. 108.

121 JAKSCH (Fn. 2), S. 170.

122 CHRISTOPH BETZ, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, S. 148 ff.; DANIELA HERDES, Datenschutzrechtliche Herausforderungen beim Einsatz von KI im Bewerbungsverfahren, Compliance Berater 2020, S. 95; KASPER/WILDHABER (Fn. 3), S. 203.

123 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 39), S. 7057; DAEDELOW (Fn. 9), Rz. 15; ebenso GOLA (Fn. 4), Rz. 2474.

124 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 39), S. 7057; ansonsten *de facto* ein Kontrahierungszwang eingeführt würde, SEBASTIAN SCHULZ, in: Gola (Hrsg.), Kommentar Datenschutz-Grundverordnung VO (EU) 2016/679, 2. Aufl., Wiesbaden 2018, Art. 22 DSGVO N 25.

125 So sind «Online-Einstellungsverfahren» explizit in Erwägungsgrund 71 DSGVO genannt; MATTHIAS GLATTHAAR, Robot Recruiting, SZW 2020, S. 45.

126 Vgl. GOLA (Fn. 4), Rz. 2478.

127 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 39), S. 7060.

128 Art. 22 Abs. 2 lit. a rDSG.

129 Art. 7 Abs. 1 und 2 rDSG.

130 Art. 7 Abs. 3 rDSG.

kompatible Bearbeitung *ex ante* zu treffen sind.[131] Privacy by Default setzt in erster Linie voraus, dass eine Datenbearbeitung vorliegt, die der betroffenen Person Eingriffsmöglichkeiten gewährt. Ob und in welchem Umfang die betroffene Person Einstellungen ändern darf, liegt im Ermessen der Arbeitgeberin.[132] Ermöglicht allerdings eine Bearbeitung keine Einflussnahme von aussen durch die betroffene Person, fällt auch das Regelungskonzept des Privacy by Design mangels möglicher Einstellungen ausser Betracht.[133] Dies dürfte bei den meisten Stimmerkennungs- und -analysesystemen der Fall sein. Hingegen gewähren Sprachassistenten regelmässig solche Einflussmöglichkeiten im Rahmen von Benutzereinstellungen. Zu beachten ist, dass der Umfang solcher Benutzereinstellungen in der Disposition des Herstellers liegt. Die Arbeitgeberin kann den entsprechenden Datenschutz nur bei der Auswahl des Produktes bzw. der Software berücksichtigen.[134]

131 ROSENTHAL (Fn. 30), Rz. 40.

132 SEBASTIAN BRÜGGEMANN, in: Esser/Kramer/von Lewinski (Hrsg.), Auernhammer Kommentar DSGVO BDSG, 6. Aufl., Köln 2018, Art. 25 DSGVO N 27 (zit. Auernhammer/BEARBEITERIN).

133 Vgl. ROSENTHAL (Fn. 30), Rz. 42.

134 AUERNHAMMER/BRÜGGEMANN, Art. 25 DSGVO N 6 und 23; SEBASTIAN CONRAD, Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017, S. 744.

VI. Schlussbetrachtung

Voice Recognition umfasst vielversprechende Technologien, die bereits heute mannigfaltig und nutzenbringend in der Arbeitswelt eingesetzt werden. Jedoch bringen die vielseitigen Einsatzmöglichkeiten und die Fülle an bearbeiteten Daten eine Gefährdung der Persönlichkeitsrechte des Arbeitnehmers mit sich. Anknüpfungspunkte zur Vermeidung solcher Persönlichkeitsverletzungen ergeben sich vordergründig aus dem Datenschutzrecht. 45

Die datenschutzrechtliche Analyse hängt von vielen Umständen ab – eine Universallösung lässt sich nicht konstruieren. Ausgangspunkt ist stets die Unterscheidung nach Sprach- und Stimmdaten. Sodann liegt der Fokus auf der Frage, ob der Einsatz im konkreten Fall verhältnismässig ist. Insgesamt findet Voice Recognition im Arbeitsverhältnis ihre Grenzen an der unzulässigen Arbeitnehmerüberwachung. 46

Mit dem rDSG wird sich das Datenschutzniveau dem DSGVO-Standard angleichen. Obwohl viele Regelungskonzepte an die europäische Blaupause erinnern, wurden sie im *Swiss Finish* bedeutend abgeschwächt. Sodann werden für den Einsatz von Voice Recognition im Arbeitsverhältnis unter dem zukünftigen Datenschutzregime nur wenige nennenswerte Praxisänderungen notwendig sein. 47

Résumé

Dans le cadre des relations de travail, Voice Recognition est utilisée comme un outil de travail, de mesure des performances, de contrôle d'accès ou d'indicateur de santé. Du point de vue de la protection des données, l'utilisation de Voice Recognition doit présenter un lien suffisant avec le poste. Dans de nombreux cas, la proportionnalité du traitement et, en particulier dans le cas des solutions « Cloud », la préservation de la sécurité des données sont des facteurs décisifs. Même si l'accord du travailleur est expressément requis dans la plupart des cas, le caractère volontaire doit être fortement relativisé. La révision de la loi sur la protection des données permet de reprendre du RGPD européen certains concepts de réglementation tels que le profilage, l'évaluation de l'impact sur la protection des données, les décisions individuelles automatisées et les exigences techniques. La conception suisse n'apporte toutefois pas de changements significatifs et concrets concernant Voice Recognition.