Ein Kunstflug durch das Recht und die Governance

Herausgegeben von

Thomas Geiser
Martin Hilb
Kurt Pärli
Manuel Stengel
Andreas Wittmer

Festschrift
zum 65. Geburtstag
von Roland Müller

DIKE

Ein Kunstflug durch das Recht und die Governance

Festschrift
zum 65. Geburtstag
von Roland Müller

Herausgegeben von

Thomas Geiser
Prof. Dr. iur. Dr. h.c.

Martin Hilb
Prof. Dr. oec.

Kurt Pärli
Prof. Dr. iur.

Manuel Stengel
Dr. iur. HSG, Rechtsanwalt und Notar

Andreas Wittmer
Dr. oec. HSG

DIKE

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

ISBN 978-3-03891-278-1

www.dike.ch

myclimate neutral

Inhaltsverzeichnis

Datenschutz und Überwachung im Homeoffice

Zu den rechtlichen Grenzen der technischen Möglichkeiten

*Luca Cirigliano / Jens Niemeyer**

Inhaltsübersicht

* Dr. iur. Luca Cirigliano, Zentralsekretär Schweizerischer Gewerkschaftsbund, Präsident des Forschungsinstituts für Arbeit und Arbeitswelten der Universität St. Gallen FAA-HSG, Alt-Bezirksrichter.
Jens Niemeyer, MLaw, Wissenschaftlicher Mitarbeiter Schweizerischer Gewerkschaftsbund.

I. Einleitung

Die Digitalisierung und Automatisierung der Arbeitswelt ermöglicht Arbeitgebern mittlerweile eine umfassende, beinahe grenzenlose Bearbeitung persönlicher Daten der Arbeitnehmenden. Auch die Covid-19-Pandemie hat einen grossen Teil dazu beigetragen und die Verwendung von Informationstechnologien aufgrund der Notwendigkeit des als Gesundheitsmassnahme im Rahmen des STOP-Prinzips[1] häufig überstürzt eingeführten Homeoffice rasant vorangetrieben. Da im Homeoffice die Grenzen zwischen Berufs- und Privatleben teilweise verschwimmen[2], erscheint eine kritische Auseinandersetzung mit den Auswirkungen und Risiken, beispielsweise von elektronischer Überwachung am Arbeitsplatz, dringend notwendig. Insbesondere auch, da das Thema Datenschutz von Arbeitgebern regelmässig unterschätzt oder sogar nicht beachtet wird, mit verheerenden Folgen für den Persönlichkeitsschutz der Arbeitnehmenden.

Interne Reglemente oder organisatorische Regelungen und technische Sicherheitsmassnahmen zum Schutz von Daten und Informationen lassen sich durch einen sorglosen Umgang sehr einfach aushebeln. Sowohl Mitarbeitende aber auch Vorgesetzte müssen daher für die Gefahren, die mit dem Homeoffice verbunden sind, sensibilisiert werden. Die Unternehmen müssen die entsprechenden Sicherheitsmassnahmen zum Schutz der Persönlichkeit bereitstellen, Arbeitnehmende einweisen sowie im Umgang mit diesen explizit schulen. Analysiert werden dafür die einschlägigen Bestimmungen des OR[3], des DSG[4] sowie des ArG[5].

Eine Rolle spielt auch das revidierte Datenschutzgesetz (nDSG), welches nach knapp vierjährigem Gesetzgebungsprozess Ende September 2020 vom Parlament verabschiedet wurde und voraussichtlich im Jahr 2022 in Kraft treten wird. Es führt zu zahlreichen Angleichungen an die EU-Datenschutzverordnung (DSGVO[6]), behält aber weiterhin eine eigene Grundkonzeption und auch Abweichungen zu dieser. Wichtige Neuerungen des nDSG sind die strengeren Sanktionen, erweiterte Informationspflichten sowie der Ausbau der Rechte der Betroffenen. So bezweckt das nDSG, die Einschränkungen auf das private und selbst-

---

1 Zum STOP-Prinzip vgl. SECO, Merkblatt für Arbeitgeber, Gesundheitsschutz am Arbeitspatz – Neues Coronavirus (Covid-19), Version vom 27. Januar 2021, 4.

2 Als Fussnote: Cirigliano Luca, Niemeyer Jens, Homeoffice, rechtliche Regelungen sowie Mustervertrag für die Praxis, in: Jusletter 30. November 2020, N 30.

3 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Titel: Obligationenrecht) vom 30. März 1911 (OR; SR 220).

4 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

5 Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel vom 13. März 1964 (ArG; SR 822.11).

6 Verordnung (EU) 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 05/46/EG (DSGVO).

bestimmte Leben unter dem Druck der Digitalisierung gering zu halten.[7] Ob der Persönlichkeitsschutz tatsächlich auf ein Niveau gehoben wird, das den Risiken der digitalen Realität Rechnung trägt und dem Standard des umliegenden Europas entspricht, muss sich erst beweisen.

II. Datenschutz und Privatsphäre

1. Schutz der Persönlichkeit

Das DSG konkretisiert das auf Verfassungsebene in Art. 13 Abs. 2 BV[8] und auf Gesetzesebene in Art. 28 ZGB[9] festgehaltene Recht auf informationelle Selbstbestimmung[10] im Zusammenhang mit Personendaten, das heisst das Recht der betroffenen Person, grundsätzlich selbst zu bestimmen, ob und zu welchem Zweck Daten über sie bearbeitet werden dürfen.[11] Der Zweck des Datenschutzrechts liegt somit nicht in dem Schutz von Daten oder deren Wert, sondern in dem Persönlichkeitsschutz der betroffenen Personen vor widerrechtlichen Eingriffen, vgl. Art. 1 DSG.[12] Neben dem Recht auf informationelle Selbstbestimmung zählt auch der Schutz der Privatsphäre als Persönlichkeitsgut im Sinne des DSG bzw. nDSG.

Im Arbeitsvertragsrecht wird der Schutz der Persönlichkeit in Art. 328 OR konkretisiert[13] und durch Art. 328b OR als datenschutzrechtliche Spezialnorm für die Bearbeitung von

---

7 Internationaler Datenschutztag 2021: Keine Erosion der Privatsphäre – trotz Pandemie, Medienmitteilung des Eigenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) vom 28. Januar 2021 (zit. EDÖB, Medienmitteilung 2021).

8 Bundesverfassung der schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

9 Schweizerisches Zivilgesetzbuch (ZGB; SR 210).

10 BGE 128 II 259, 268; BGE 138 II 346, 359 f.; BGE 140 I 2, 22.

11 BGE 140 I 2, 22; Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBI 2017 6941 ff., (zit. Botschaft DSG 2017), 7010.

12 PÄRLI KURT, Evaluieren, kontrollieren, überwachen: Datenschutz in Arbeitsverhältnissen, in: Ueli Kieser/Kurt Pärli (Hrsg), Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen: Referate der Tagung vom 29. November 2011 in Luzern. St. Gallen, Institut für Rechtswissenschaft und Rechtspraxis IRP-HSG, 2012, 29–54, 32; MAURER-LAMBROU URS, in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz (DSG) / Öffentlichkeitsgesetz (BGÖ), 3. Aufl., Basel 2014 (zit. BSK DSG-AUTOR), Art. 1 N 12.

13 GEISER THOMAS, MÜLLER ROLAND, PÄRLI KURT, Arbeitsrecht in der Schweiz, Bern 2019 (zit. GEISER/MÜLLER/PÄRLI), N 338; STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER,

Personendaten ergänzt. Im Rahmen ihrer Fürsorgepflicht[14] haben Arbeitgeber die Persönlichkeit der Arbeitnehmenden zu achten und zu schützen.[15] Die Fürsorgepflicht beinhaltet neben Schutzpflichten die schonende Rechtsausübung gegenüber Arbeitnehmenden. Der Persönlichkeitsschutz umfasst die physische und psychische Unversehrtheit sowie das leibliche und geistige Wohlbefinden.[16]

2. Zulässige Datenbearbeitung

a) Beschränkung auf Daten natürlicher Personen

Der Datenschutz ist beschränkt auf die Bearbeitung von Personendaten.[17] Juristisch wird zwischen Daten mit und ohne Personenbezug unterschieden, also zwischen Personendaten und sog. Sachdaten, wobei sich letztere nicht ausschliesslich auf Sachen beziehen müssen.[18] Nach der Legaldefinition in Art. 3 lit. a DSG; Art. 5 lit. a nDSG sind Personendaten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, d.h. jede Art von Information, welche mit einer Person in Verbindung gebracht werden kann.[19] Eine Abgrenzung zwischen Personendaten und Sachdaten ist nicht immer unproblematisch.[20] Gemäss Bundesgericht ist eine Person bestimmbar, wenn sie zwar mit den Daten allein nicht eindeutig identifizierbar ist, aber aus dem Kontext einer Information oder aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Jede theoretische Möglichkeit der Identifizierung ist jedoch nicht ausreichend. Bestimmbarkeit liegt dann vor, wenn nach der allgemeinen Lebenserfahrung damit gerechnet werden muss, dass ein Interessent den Aufwand für die Bestimmung der betroffenen Person auf sich nehmen würde. Der Aufwand ist dabei nach den aktuellen Möglichkeiten der Technik zu beurteilen.[21] Letztendlich hängt die Bestimmbarkeit somit von den Kompetenzen und Fähigkeiten des individuellen Inhabers der Information ab.[22] Ob ein Personenbezug vorliegt, ist stets kontextabhängig. Personen-

---

Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7. Aufl., Zürich 2012, (zit. STREIFF/VON KAENEL/RUDOLPH), Art. 328 OR N 2.

14 Art. 328 OR.

15 Art. 328 ff. OR.

16 GEISER THOMAS, Überwachung am Arbeitsplatz Arbeits- und datenschutzrechtliche Rahmenbedingungen bei der Überwachung der Arbeitnehmer durch die Arbeitgeberin, in: digma 2004, 98–101 (zit. GEISER), 98.

17 Vgl. Art. 1 DSG.

18 BSK DSK-BLECHTA (FN 12), Art. 3 N 3.

19 BSK DSK-BLECHTA (FN 12), Art. 3 N 6 f.

20 EPINEY ASTRID, Big Data & Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?, in: Jusletter IT vom 21.05.2015, (zit. EPINEY), N 34.

21 BGE 138 II 346 E. 6.1.

22 EPINEY (FN 20), N 11.

daten sind bereits ab dem Augenblick vorhanden bzw. erzeugt, sobald ein Personenbezug vorliegt. Das Datenschutzrecht hat allerdings nur Datenbearbeitungen zum Gegenstand, also den Umgang mit Personendaten unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.[23] Zum Beschaffen von Personendaten gehört auch die Überwachung der Mitarbeiter.[24] Ob die Daten tatsächlich von jemandem eingesehen werden, spielt keine Rolle, denn das Sammeln und Speichern an sich stellt bereits eine relevante Datenbearbeitung dar.[25]

Besonders schützenswerte Personendaten unterliegen einem strengeren Schutz für die Datenverarbeitung.[26] Besonders schützenswerte Personendaten sind in Art. 3 lit. c DSG; Art. 5 lit. e nDSG abschliessend definiert und stellen Personendaten dar, welche die Persönlichkeit der Betroffenen in erhöhtem Mass tangieren.[27] Darunter fallen unter anderem Daten über gewerkschaftliche Ansichten oder Tätigkeiten[28], oder die Intimsphäre[29]. Das nDSG erweitert die Auflistung von besonders schützenswerten Personendaten neu um genetische sowie biometrische Daten.[30]

Informationen können sich nach dem DSG sowohl auf natürliche als auch juristische Personen beziehen, vgl. Art. 3 lit. b DSG. Damit handelt es sich um einen insgesamt sehr weitgefassten Begriff. Im Zuge der Totalrevision wird der Anwendungsbereich des DSG demjenigen der europäischen DSGVO angepasst, weshalb sich das nDSG nur noch auf natürliche Personen bezieht.[31]

Was in einigen Bereichen, wie beispielsweise der Datenübermittlung ins Ausland, Vorteile für Schweizer Unternehmen bringt, könnte andererseits die Rechte der Arbeitnehmenden beschränken; auch das nDSG enthält keine kollektiven Rechtsdurchsetzungsmechanismen, wie die Verbandsklage oder -beschwerde. Ohne die Möglichkeiten für Einzelpersonen, Verletzungen ihrer Datenschutzinteressen durch Organisationen, wie zum Beispiel den Gewerkschaften, geltend zu machen, werden die Rechte der Arbeitnehmenden nicht verbessert, sondern eher geschwächt. Aufgrund der gegenüber den Datenbearbeitern in finanzieller und auch organisatorischer Hinsicht deutlich unterlegenen Stellung nehmen von

---

23 Gem. Art. 2 Abs. 1 i.V.m. Art. 3 lit. e DSG.

24 PÄRLI KURT, Observation von Arbeitnehmern/-innen durch die Arbeitgeberin, in: HAVE 2018, 228–229, 228.

25 GEISER (FN 16), 99.

26 Vgl. insbesondere Art. 4 Abs. 5, 11a Abs. 3 lit. a, 12 Abs. 2 lit. c, 14 DSG.

27 BSK DSG-BLECHTA (FN 12), Art. 3 N 27, 30.

28 Art. 3 lit. c, Ziff. 1 DSG; Art. 5 lit. c, Ziff. 1 nDSG.

29 Art. 3 lit. c, Ziff. 2 DSG; Art. 5 lit. c, Ziff. 2 nDSG.

30 Art. 5 lit. c, Ziff. 3, 4 nDSG.

31 Vgl. Art. 2 Abs. 1 sowie Art. 5 lit. a und b nDSG; Botschaft DSG 2017 (FN 11), 6972.

Rechtsverletzungen betroffene Personen ihre Rechte selber nur selten wahr.[32] Für die Wahrung der Chancengleichheit und den Zugang zu den Gerichten sind Einzelpersonen daher auf die Unterstützung eines Verbandes mittels kollektiven Rechtdurchsetzungsmechanismen dringend angewiesen.[33]

Spezialgesetzliche, ideelle Verbandsbeschwerderechte dienen grundsätzlich der Durchsetzung öffentlicher Interessen, selbst bei der Unterstützung einzelner Personen.[34] In anderen Bereichen, wie dem Umweltschutz, hat das ideelle Verbandsbeschwerderecht mit mehrheitlich gutgeheissenen Rechtsmitteln der Verbänden seine Wirksamkeit bereits deutlich unter Beweis gestellt.[35] Auch in der DSGVO, die in gewissen Teilen als Vorbild für das nDSG gilt, ist eine Öffnungsklausel für ein Verbandsklagerecht zur verbesserten Durchsetzung des Rechtsschutzes im Datenschutzbereich enthalten.[36] Dennoch bezeichnete der Bundesrat einen solchen Mechanismus in der Botschaft zum nDSG als nicht opportun.[37] Das in allgemeiner Form bereits in Art. 89 ZPO[38] bestehende Verbandsklagerecht sei ausreichend.[39] Ein ideelles Verbandsbeschwerderecht wurde soweit ersichtlich nicht einmal in Betracht gezogen.

Die allgemeine Verbandsklage beschränkt sich auf den Schutz der Persönlichkeit der Angehörigen bestimmter Personengruppen.[40] In eigenem Namen klageberechtigt sind einzig die über die notwendige Repräsentativkraft verfügenden Organisationen, welche die Interessenwahrung in ihren Statuten ausdrücklich nennen, wie beispielsweise die Gewerkschaften. Beim allgemeinen Verbandsklagerecht geht es aber nicht um den Schutz allfälliger Mitglieder, sondern um die Interessen von Personengruppen, sodass auch Organisationen ohne Mitglieder (z.B. Stiftungen) klageberechtigt sind. Da die Organisationen oder Mitglie-

---

32 Botschaft DSG 2017 (FN 11), 7071.

33 WALTER JEAN-PHILIPPE, L'effectivité des mécanismes de mise en œuvre de la protection des données, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, Zürich/Basel/Genf 2015, 115 ff., 117; MEIER REGINA, Das ideelle Verbandsbeschwerderecht Eine Darstellung der Regelungen auf Bundesebene, in: Zürcher Studien zum öffentlichen Recht, 228, Zürich 2015, 7 N 135 f.

34 MEIER REGINA, Revision des Datenschutzgesetzes: kollektive Rechtsdurchsetzung im Datenschutzrecht? Insbesondere durch die ideelle Verbandsbeschwerde, in: sui-generis 2018 (zit. MEIER), 139 ff. N 5.

35 MEIER (FN 34), 139 ff. N 5.

36 Art. 80 DSGVO.

37 Botschaft DSG 2017 (FN 11), 6984.

38 Schweizerische Zivilprozessordnung (ZPO; SR 272).

39 Vgl. zu den zulässigen Ansprüchen KERN MARKUS/EPINEY ASTRID, Durchsetzungsmechanismen im EU-Recht und ihre Implikationen für die Schweiz, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, Forum Europarecht: Band 35, Zürich/Basel/Genf 2015, 19 ff. N 48.

40 Art. 89 Abs. 1 ZPO.

der gerade nicht in eigenen Interessen betroffen sein müssen, sind sie im Datenschutzbereich auf die Informationen des EDÖB gemäss Art. 30 DSG; Art. 57 Abs. 2 nDSG angewiesen, welcher die Öffentlichkeit in Fällen von allgemeinem Interesse sowie über seine Verfügungen in Kenntnis setzt. Nach erfolgter Kenntnisnahme können z.B. die Gewerkschaften sodann in eigenem Namen mittels Verbandsklage die Verletzung der Persönlichkeit, z.B. durch unzulässige Überwachungsmassnahmen[41], gegenüber dem Arbeitgeber feststellen und beseitigen lassen.

Reparatorische Ansprüche, wie Schadensersatz und Genugtuung, müssen individuell eingeklagt werden. Da der Verbandsklage keine Wirkung für und gegen die einzelnen Mitglieder der Organisation zukommt und die Verjährung für zivilrechtliche Schadensersatzansprüche nicht unterbrochen wird, profitieren die Mitglieder oder Personengruppen lediglich von beispielsweise einem Feststellungsentscheid, der bei der Durchsetzung einer nachfolgend notwendigen Individualklage hilft.[42]

Für Einzelpersonen bleibt es daher weiterhin erschwert, ihre Rechte selbstständig geltend zu machen.

b) Art. 328b OR

Rechte die offline gelten, müssen ebenso online geschützt werden.[43] Gemäss der datenschutzrechtlichen Spezialregelung von Art. 328b OR darf die Arbeitgeberin Personendaten des Arbeitnehmers nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Die zulässige Bearbeitung wird dadurch auf diese beiden Zwecke beschränkt. Bei der Abklärung der Eignung von Arbeitnehmenden geht es hauptsächlich um die Qualifikation von Stellenbewerbern im Hinblick auf den Abschluss eines Arbeitsvertrags, oder um die Beurteilung der Eignung bereits angestellter Arbeitnehmender hinsichtlich einer möglichen Beförderung.[44] Zu den für die Durchführung des Arbeitsverhältnisses erforderlichen Daten zählen neben administrativen Angaben auch Daten für den Vollzug des Arbeitsverhältnisses, wie beispielsweise die Überprüfung von Arbeitsergebnissen, die Kontrolle und Einhaltung von Weisungen, die Überprüfung der Einhaltung von Sicherheitsvorschriften oder Leistungskontrollen. Bei der Überwachung, also der Erfassung von Informationen über Leistung und Verhalten der Arbeitnehmenden sind die Übergänge zwischen den zulässigen Bearbeitungszwecken gemäss

41 Siehe dazu unter Ziff. III.

42 Bericht des Bundesrates vom 3. Juli 2013, Kollektiver Rechtsschutz in der Schweiz – Bestandesaufnahme und Handlungsmöglichkeiten, VPB 2/2013 vom 20. Dezember 2013, 59–112, 39 ff.

43 Botschaft DSG 2017 (FN 11), 6962

44 STREIFF/VON KAENEL/RUDOLPH (FN 13), Art. 328b OR N 5.

Art. 328b OR fliessend, da sie sowohl durch den Eignungstatbestand gedeckt sind als auch zur Durchführung des Arbeitsvertrages dienen.[45]

Gemäss Art. 328b Abs. 2 OR gelten im Übrigen die Bestimmungen des DSG. Dieser überflüssige Verweis wird teilweise als Konkretisierung des Verhältnismässigkeitsprinzips gemäss Art. 4 Abs. 2 DSG; Art. 6 Abs. 2 nDSG angesehen, wodurch sich eine i.S.v. Art. 328b OR unzulässige Datenbearbeitung durch Vorliegen von Rechtfertigungsgründen[46] rechtfertigen liesse.[47] Die wohl herrschende Lehre vertritt dagegen die Ansicht, dass Art. 328b OR die zulässigen Zwecke einer Datenbearbeitung im Arbeitsverhältnis auf Fälle mit Arbeitsplatzbezug beschränkt.[48] Anders als im Bereich des DSG kann also selbst ein Rechtfertigungsgrund i.S.v. Art. 13 DSG; Art. 31 nDSG die Rechtswidrigkeit nicht beseitigen.[49] Das Bearbeiten anderer Daten ohne Arbeitsplatzbezug ist folglich verboten und als Vertragspflichtverletzung zu qualifizieren, selbst wenn sie nach dem DSG erlaubt wäre.[50]

3. Datenschutzrechtliche Grundsätze

Bei der Datenbearbeitung, beispielsweise der Überwachung im Homeoffice, sind neben den in Art. 328b OR genannten Beschränkungen auch die allgemeinen datenschutzrechtlichen Bearbeitungsgrundsätze gem. Art. 4 f. DSG; Art. 6 f. nDSG zu beachten. Ein Verstoss gegen die nachfolgend genannten Datenbearbeitungsgrundsätze bewirkt eine widerrechtliche Persönlichkeitsverletzung.[51]

Mit Inkrafttreten des nDSG werden Datenverarbeitende nochmals höhere Sorgfaltspflichten auferlegt. So muss das Risiko einer Persönlichkeitsverletzung bereits bei der Planung der Datenbearbeitung durch angemessene Massnahmen verringert werden.[52] Zudem ist der Datenverantwortliche verpflichtet, durch Voreinstellungen zu gewährleisten, dass standard-

---

45 PÄRLI KURT, Kapitel 17 Datenschutz, in: Wolfgang Portmann/Adrian Von Kaenel (Hrsg.), Fachhandbuch Arbeitsrecht Expertenwissen für die Praxis, Zürich/Basel/Genf 2018 (zit. PÄRLI), 685–704, 689 N 17.14.

46 Gemäss Art. 13 Abs. 1 DSG; Art. 31 Abs. 1 nDSG.

47 ROSENTHAL DAVID, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008 (zit. Handkommentar DSG-AUTOR), Art. 328b OR N 5 ff. mit weiteren Hinweisen.

48 STREIFF/VON KAENEL/RUDOLPH (FN 13), Art. 328b OR N 3; STAEHLIN ADRIAN, Kommentar zum schweizerischen Zivilrecht, Band V/2c – Das Obligationenrecht, Der Arbeitsvertrag, Art. 319–330a OR, 4. Aufl., Zürich 2006, Art. 328b OR N 1.

49 STREIFF/VON KAENEL/RUDOLPH (FN 13), Art. 328b OR N 3.

50 Ebenda.

51 Art. 12 Abs. 2 lit. a DSG. Zur allfälligen Rechtfertigung siehe unter Ziff. 6.

52 Art. 7 Abs. 1 nDSG.

mässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.[53]

a) Treu und Glauben

Bei der Datenbearbeitung ist der Grundsatz von Treu und Glauben[54] zu beachten. Eine treuwidrige Datenbearbeitung ist missbräuchlich und damit rechtswidrig.[55] Gegen Treu und Glauben verstösst, wer Personendaten ohne das Wissen oder gegen den Willen der betroffenen Person beschafft, beispielsweise durch die Verwendung von Spyware[56], oder die betroffene Person hinsichtlich der Datenbearbeitung absichtlich über den Zweck der Bearbeitung täuscht.[57] Arbeitnehmende müssen vorab mit konkreten Informationen über Einsatzzeit, -ort und Zweck einer Überwachung informiert werden, beispielsweise mittels Datenschutzerklärung oder Klausel im Arbeitsvertrag.

Unübersichtliche und überschiessende Einwilligungserklärungen verstossen gegen den Grundsatz von Treu und Glauben, wenn dabei in Datenbearbeitungen eingewilligt wird, mit denen die betroffene Person nicht rechnen muss.[58] Mit Verweis auf die Einwilligung[59] ist jedoch vorwegzunehmen, dass im Arbeitsverhältnis der Arbeitsvertrag an sich bereits in gewissem Umfang eine Einwilligung in Kontrollen durch die Arbeitgeber darstellt. Aber Überwachungen dürfen nicht heimlich erfolgen. Arbeitnehmende müssen vorab mit konkreten Informationen über Einsatzzeit, -ort und Zweck der Überwachung informiert werden.

b) Verhältnismässigkeit

Der Grundsatz der Verhältnismässigkeit[60] besagt, dass nur Daten bearbeitet werden dürfen, die geeignet, erforderlich und zumutbar sind, um den verfolgten Zweck zu erreichen.[61] Zwischen dem Zweck der Datenbearbeitung und der damit verbundenen Beeinträchtigung der Persönlichkeit soll ein vernünftiges Verhältnis bestehen.[62] Mit anderen Worten sollen im-

---

53 Art. 7 Abs. 3 nDSG.

54 Art. 4 Abs. 2 DSG; Art. 6 Abs. 2 nDSG

55 BSK DSG-MAURER-LAMBROU/STEINER (FN 12), Art. 4 N 8.

56 BGE 139 II 7.

57 BSK-DSG-MAURER-LAMBROU/STEINER (FN 12), Art. 4 N 8.

58 Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBI 1988 413 ff., (zit. Botschaft DSG 1988), 449.

59 Zur Einwilligung siehe unter Ziff. 5 lit. a.

60 Art. 4 Abs. 2 DSG; Art. 6 Abs. 2 nDSG.

61 <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html> (28.02.2021).

62 BSK DSG-MAURER-LAMBROU/STEINER (FN 12), Art. 4 N 8 11.

mer nur so viele Personendaten wie nötig und dabei so wenig Personendaten wie möglich bearbeitet werden. Bearbeitungszweck und Beeinträchtigung der Persönlichkeit müssen in einem angemessenen Verhältnis stehen und betroffenen Personen soll die Möglichkeit bleiben, die Bearbeitung ihrer Daten zu kontrollieren und notfalls auch zu verhindern.

c) Zweckbindungsprinzip

Beim Grundsatz der Zweckbindung[63] handelt es sich um eine Bearbeitungsregel, gemäss der Daten stets nur zu dem Zweck bearbeitet werden dürfen, der für die Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[64] Eine Datenbeschaffung durch den Arbeitgeber auf Vorrat verstösst nicht nur gegen das Zweckbindungsprinzip, sondern auch gegen Treu und Glauben, sowie gegen das Verhältnismässigkeitsprinzip und ist damit rechtswidrig.[65] Gemäss Art. 6 Abs. 5 nDSG müssen diese Daten gelöscht oder vernichtet werden.

Schliesslich muss gemäss Art. 4 Abs. 4 DSG; Art. 6 Abs. 3 nDSG das Beschaffen von Personendaten und vor allem auch der Zweck der Datenbearbeitung für die Betroffenen erkennbar sein. Die Erkennbarkeit umfasst neben der Datenbeschaffung und dem Zweck der Datenbearbeitung auch mindestens die Grundzüge der Datenbearbeitung.[66] Die Norm soll – zusammen mit den Regelungen über die Informationspflichten – die Transparenz bei Datenbearbeitungen erhöhen. Personen soll und muss grundsätzlich möglich sein, sich einer Datenbearbeitung zu widersetzen. Die Erkennbarkeit bemisst sich nach den konkreten Umständen.[67] Je weniger offensichtlich erkennbar eine Datenverarbeitung und deren Zweck für die betroffene Person ist, desto mehr zusätzliche Informationen muss der Datenbearbeiter zur Verfügung stellen.[68] Dabei sind insbesondere die Grundsätze der Verhältnismässigkeit sowie von Treu und Glauben zu beachten.

---

63 Art. 4 Abs. 3 DSG; Art. 6 Abs. 3 nDSG.

64 Art. 4 Abs. 3 DSG.

65 BSK DSG-MAURER-LAMBROU/STEINER (FN 12), Art. 4 N 14.

66 Botschaft vom 19. Februar 2003 zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz den Menschen bei der automatisierten Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung, BBI 2003 2101 ff. (zit. Botschaft DSG 2003), 2125.

67 BEARISWIL BRUNO, Datenschutzgesetz (DSG), in: Bruno Baeriswil/Kurt Pärli, (Hrsg.), Stämpflis Handkommentar, Bern 2015 (zit. SHK DSG-Baeriswyl), Art. 4 N 49.

68 Botschaft DSG 2003 (FN 66), 2125.

4. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Mit Art. 7 nDSG kommt ein neuer Rechtsgrundsatz hinzu, wonach Arbeitgeber in Anlehnung an Art. 25 DSGVO verpflichtet werden, die Datenbearbeitung ab der Planung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften und insbesondere die Datenschutzgrundsätze eingehalten werden (privacy by design).[69] Die gesetzlichen Anforderungen für eine datenschutzkonforme Bearbeitung werden damit bereits so ins System verankert, dass die Gefahr von Verstössen reduziert bzw. ausgeschlossen werden kann.[70] Dies kann vor allem mittels Datenminimierung erfolgen, wobei personenbezogene Daten nur in möglichst geringem Umfang bearbeitet, nur für kurze Zeit aufbewahrt, oder mittels standardmässiger Anonymisierung umgesetzt werden.[71] Absatz 2 von Art. 7 nDSG präzisiert diese Anforderungen und bringt einen risikobasierten Ansatz zum Ausdruck. Danach ist eine Abwägung vorzunehmen und zu prüfen, ob die technischen und organisatorischen Massnahmen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken für den Persönlichkeitsschutz und die Grundrechte der Arbeitnehmenden angemessen Rechnung tragen. Je höher das Risiko und umfangreicher die Datenbearbeitung, desto höher sind auch die Anforderungen an die technischen Vorkehrungen.[72] Des Weiteren müssen Arbeitgeber mittels Voreinstellung geeignete Massnahmen treffen, dass nur diejenigen Personendaten bearbeitet werden, deren Verarbeitung für den jeweiligen Zweck unbedingt erforderlich ist und die Bearbeitung damit auf das nötige Mindestmass beschränkt wird (privacy by default).[73] Im Zusammenhang mit Datenbearbeitung bedeutet dies, dass der Vorgang standardmässig möglichst datenschutzfreundlich eingerichtet werden muss. Viele Software-Programme enthalten heute Analysetools, die im Hintergrund verdeckt ablaufen und über die ihre Verwender oftmals nicht einmal Kenntnis haben. Da datenschutzrechtliche Voreinstellungen betroffenen Personen bestenfalls eine Zustimmungsmöglichkeit zur Datenverarbeitung erlauben, hängen diese eng mit der Einwilligung[74] der betroffenen Person zusammen.

69 Art. 7 Abs. 1 nDSG.

70 Botschaft DSG 2017 (FN 11), 7029.

71 Ebenda.

72 Ebenda.

73 Art. 7 Abs. 3 nDSG.

74 Zur Einwilligung siehe unter Ziff. 6 lit. a.

5. Exkurs: Datensicherheit

Die Datensicherheit bildet gemeinsam mit dem Grundsatz der Richtigkeit der Daten[75] und den datenschutzrechtlichen Grundsätzen aus Art. 4 DSG; Art. 6 nDSG einen Leitfaden für sämtliche Datenbearbeitungen. Arbeitgeber müssen die nötigen technischen und organisatorischen Vorkehrungen treffen, um die Datensicherheit zu gewährleisten.[76] Dies bedeutet zum Beispiel auch, dass nur berechtigte Personen auf eine Datenbank Zugriff haben dürfen. Die Abgrenzung zum neuen Datenschutz durch Technik[77] ergibt sich daraus, dass die Datensicherheit den Verantwortlichen der Bearbeitungen verpflichtet, eine geeignete Sicherheitsarchitektur für die Systeme zu installieren und damit gegen Schadsoftware oder Datenverlust zu schützen.[78] Art. 7 nDSG bezweckt hingegen die Verhältnismässigkeit der Datenbearbeitung, beispielsweise durch Anonymisierung der Daten.[79] Da durch Verletzungen der Datensicherheit ein hohes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen besteht, müssen diese von den Verantwortlichen umgehend dem EDÖB gemeldet werden.[80] Als Konkretisierung der gesetzlichen Vorgaben haben verschiedene Datenschutzbehörden Leitlinien zu den organisatorischen und technischen Massnahmen publiziert.[81] Auch zu den aus datenschutzrechtlicher Sicht besonders risikoreichen Videoplattformdiensten geben die Datenschutzbehörden Hinweise zur Einhaltung der gesetzlichen Vorgaben.[82]

Daten lassen sich praktisch per Mausklick vervielfachen und stehen potenziell einer unbegrenzten Zahl von Nutzern zur Verfügung.[83] Gerade im Homeoffice, wo die Kommunikation und Arbeitsleistung der Mitarbeitenden hauptsächlich digital erfolgt, entsteht ein erhöhtes Risiko für die Datensicherheit. Im Homeoffice kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie in den Büroräumen eines Unternehmens. Ist der häusliche Arbeitsplatz auch für Besucher oder unbefugte Dritte zugänglich, müssen Massnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau, vergleichbar dem eines Büroplatzes im Unternehmen, erreichen lässt. Die Homeoffice-Mitarbeiter müssen dahingehend sensibilisiert werden, das im Homeoffice erhöhte Sicherheitsmassnahmen zu be-

75 Art. 5 Abs. 1 DSG.

76 Art. 7 DSG; Art. 8 nDSG.

77 Art. 7 nDSG.

78 Botschaft DSG 2017 (FN 11), 7031.

79 Ebenda.

80 Art. 24 nDSG.

81 <https://www.zh.ch/de/politik-staat/datenschutz/datenschutz-in-oeffentlichen-organen/digitale-zusammenarbeit.html> (28.02.2021).

82 <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/merkblaetter/videokonferenzloesungen.html> (28.02.2021).

83 THOUVENIN FLORENT, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, in: SJZ 113/2017, 21–32, 24.

achten sind. So muss beispielsweise darauf hingewiesen werden, Fenster zu schliessen und Türen abzuschliessen, wenn das Homeoffice nicht besetzt ist. Generell muss sichergestellt werden, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Datenmissbrauch kann nur verhindert werden, solange die Daten verschlüsselt und damit unlesbar sind.[84] Wurden Daten einmal öffentlich zugänglich gemacht, ist eine Geheimhaltung aufgrund der einfachen Kopier- bzw. Reproduzierbarkeit nicht mehr möglich.[85]

a) Risikosphäre Homeoffice

«Persönliche Daten sind das neue Öl für das Internet und die Währung der digitalen Welt».[86] Im Rahmen der Covid-19-Homeofficepflicht versuchten Kriminelle vermehrt, sich über die externen Homeoffice-Verbindungen Zutritt in die Firmennetzwerke zu verschaffen. Die Fallzahlen des nationalen Zentrums für Cybersicherheit verdeutlichen, dass für den Zugriff aus dem Homeoffice auf die internen Ressourcen der Firma oft kein sicherer und geschützter Fernzugriff, optimaler Weise via Virtual Private Network (VPN), ermöglicht wird.[87] Ein gesicherter remote-Zugang bietet allein jedoch keine Garantie, denn Datensicherheit ist mehr als nur IT-Sicherheit. Eine grosse Schwachstelle im System bildet immer noch der Mensch. Mittels «Phishing-mails» gelangen Cyberkriminelle an vertrauliche Daten, indem sie ihre Opfer unter Vorwand zur Angabe ihrer Passwörter oder weiteren persönlichen Informationen verleiten. Mit den persönlichen Zugangsdaten ist das Umgehen bzw. hacken der Schutzmechanismen gar nicht nötig; Kriminelle verschaffen sich mit dem Schlüssel quasi durch die Eingangstür des Unternehmens Zutritt zu den internen Ressourcen. Aus diesem Grund ist die Investition in firmeninterne Prävention durch Schulung der Arbeitnehmenden und Arbeitgeber besonders wichtig.

b) Nutzung privater Geräte

Ein besonders zusätzliches Datenschutzrisiko besteht zudem bei der Verwendung von Privatgeräten für die geschäftliche Nutzung (Bring Your Own Device; BYOD). Grundsätzlich haben Arbeitgeber die Mitarbeiter mit Arbeitsgeräten und Material auszurüsten, die zur Verrichtung der Arbeit benötigt werden (Art. 327 Abs. 1 OR). Zu den Arbeitsgeräten gehört in jedem Fall die IT-Infrastruktur. Die Bereitstellung der Arbeitsgeräte für das Homeoffice

---

84 ZECH HERBERT, Information als Schutzgegenstand, Jus Privatum, Band 166, Tübingen 2012 (zit. ZECH), 117 ff.

85 ZECH (FN 84), 118.

86 KUNEVA MEGLENA, European Consumer Commissioner – Keynote Speech – Roundtable on Online Data Collection – Targeting and Profiling, Brussels, 31. March 2009, Speech/09/156.

87 Siehe Anzahl Meldungen pro Woche während des pandemiebedingten Teillockdowns Mitte April 2020, als fast die Hälfte der Arbeitnehmenden im Homeoffice arbeitete, sowie der Homeoffice-Pflicht seit 18. Januar 2021 unter: <https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html> (06.03.2021).

hat den Vorteil, sicherstellen zu können, dass diese ordentlich gewartet sind und alle technischen Massnahmen (Virenschutz, Firewall, Passwortschutz, etc.) getroffen wurden, um die Sicherheit zu gewährleisten. Gerade während der Covid-19-Pandemie und der präventiv dringlich eingeführten Homeofficeempfehlung bzw. -pflicht war es Arbeitgebern aufgrund der Kürze der Zeit nicht immer möglich, mobile Arbeitsgeräte für sämtliche Mitarbeiter in ausreichendem Masse lückenlos bereitzustellen, bzw. die Überwachung und Umsetzung technischer Massnahmen durchzuführen. Die Gefahr beim BYOD besteht in einer Persönlichkeitsverletzung durch ungewollte Einsichtnahme in die Privatspähre aufgrund der Vermischung von privaten und geschäftlichen Daten einerseits, und der Sicherheit der Daten durch allfällige Manipulationen, zum Beispiel Jailbraking, oder ungenügender Umgang mit den Aufbewahrungspflichten, zum Beispiel fehlende backups, andererseits.[88] Des Weiteren erhoffen sich wohl gewisse Arbeitgeber auch eine erweiterte Erreichbarkeit der Arbeitnehmenden, da die Möglichkeit zur Abschaltung des Gerätes nach Feierabend zumeist entfällt. Im Ergebnis kann dies zu Stress, Überlastung, bis hin zum Burnout führen.[89] Die ständige Erreichbarkeit von Arbeitnehmenden verstösst gegen die einschlägigen Bestimmungen des ArG, und wirft Fragen zur Anrechnung von Arbeitszeit und sogar zur Abgrenzung von «Pikettdienst[90]» auf.[91]

Die Anbindung und Integration von privaten oder selbst administrierten Geräten an das Firmennetzwerk bedarf daher verschiedener Anpassungen und der Einhaltung von Regeln, um Arbeitnehmende zu schützen.

- Das Unternehmen trägt die wiederkehrende Lizenzkosten für Software oder Verbindungskosten bei mobilem Einsatz. Geräte müssen mit vom Arbeitgeber bereitgestellten aktuellsten Sicherheitsupdates ausgerüstet sein.
- Die Geräte müssen über einen ausreichenden und aktuellen Schutz gegen Viren, Malware etc. verfügen sowie mit einer aktiven Firewall gegenüber ungeschützten Zugriffen aus dem Netz gesichert werden.
- Sobald die Integration in das Firmennetzwerk erfolgt ist, werden die Geräte einem firmeneigenen Gerät gleichgestellt. Dabei dürfen Arbeitgeber weder Zugriff noch Einblick in die privaten Daten haben und müssen eine Trennung zu den geschäftlichen Daten mittels geeigneter Software zur Verfügung stellen.[92]

---

88 <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/bring-your-own-device--byod-.html> (28.02.2021).

89 REUTTER MARK/KLAUS SAMUEL, Rechtliche Stolpersteine bei «BYOD», in: Bruno Beariswil/Beat Rudin/Bernhard Hämmerli/Rainer Schweizer/Günter Krajoth/David Vasella (Hrsg.), digma 2012, 160–165, 162.

90 Siehe dazu: GEISER/MÜLLER/PÄRLI (FN 13), N 958b.

91 Siehe dazu: MÜLLER ROLAND, Was ist Arbeitszeit, in: ZBJV 153/2017, 453–477, 456 ff.

92 Siehe dazu auch unter Ziff. 4 (Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen).

- Bei technischen Problemen erfolgt vom Unternehmen ein Support an den privaten, nicht firmeneigenen IT-Geräten. Arbeitnehmende haben einen Anspruch auf ein kostenloses Ersatzgerät während der Durchführung allfälligen Reparaturen gegenüber dem Arbeitgeber.
- Das Unternehmen trägt die Haftung bei Beschädigung während eines geschäftlichen Einsatzes oder Verlust. Arbeitnehmende haften für Vorsatz und Grobfahrlässigkeit.[93]

Neben Nutzung privater Geräte für geschäftliche Zwecke (BYOD) zeigt der EDÖB auch mögliche Alternativen für Unternehmen auf. Beim «Corporate Owned Personally Enabled» (COPE) handelt es sich um das Gegenteil von BYOD. Geschäftliche Tätigkeiten werden nicht mehr auf privaten Geräten erledigt, sondern die Firmengeräten dürfen auch zur privaten Nutzung verwendet werden. Das Unternehmen ist die Eigentümerin und bestimmt die Benutzungsbedingungen und die Kostenlimite. Als Zwischenvariante wird weiter das «Choose Your Own Device» (CYOD) vorgeschlagen, bei der Arbeitnehmende ein vom Unternehmen genehmigtes Gerät (mit oder ohne Kostenbeteiligung der Firma) kaufen und die Firma die Konfiguration des Gerätes bestimmt. Änderungen der eingestellten Konfigurationen sind für den Arbeitnehmenden dann verboten. Bei «Bring Your Own Connection» (BYOC) werden private Smartphones oder Tablets mit 4G bzw. 5G als Hotspot eingesetzt, und bei Bring Your Own Software (BYOS), das sich auf portable Anwendungen beschränkt, wird die Einhaltung der firmeneigenen internen Regelung vorgeschrieben. Bei sämtlichen Alternativen handelt es sich um eine Umwälzung der Kostentragungspflicht i.S.v. Art. 327 OR zulasten der Arbeitnehmenden und sind daher, auch wenn sie aus datenschutzrechtlicher Sicht Alternativen darstellen, so weit möglich zu vermeiden bzw. wenn sie trotzdem erfolgen, durch Zahlung einer Pauschale bzw. der effektiven Kosten durch den Arbeitgeber abzugelten.

c) Internationale Sicherheitsstandards

Nach der weltweiten Zunahme von Cyberattacken gegen Unternehmen, wie zum Beispiel mittels der Erpressersoftware Petya, könnten auch internationale Sicherheitsstandards vermehrt an Bedeutung gewinnen. Die Norm ISO/IEC 27001 gilt zum Beispiel als ganzheitliches Managementsystem für die Informationssicherheit und bildet die strukturelle Basis zum Schutz von vertraulichen Daten. Unternehmen können freiwillig durch eine interne Begutachtung ein korrektes Vorgehen hinsichtlich der IT-Sicherheit überprüfen und durch aufstellen, überwachen und/oder verbessern ihrer Sicherheitsrichtlinien auch zum Schutz der Persönlichkeitsrechte ihrer Arbeitnehmenden beitragen. Während die ISO/IEC 27001 im Anhang A die Massnahmenziele und Massnahmen zur Risikoreduzierung fordert, liefert die ISO/IEC 27002 Leitlinien, wie diese Anforderungen umgesetzt werden können. Bei-

[93] Vertiefend dazu: MÜLLER ROLAND, Die Bedeutung des Verschuldens im schweizerischen Arbeitsrecht, in: Susan Emmenegger/Stephanie Hrubesch-Millauer/Frédéric Krauskopf/Stephan Wolf (Hrsg.), Brücken Bauen – Festschrift für Thomas Koller, Bern 2018, 657–684, 670.

spielsweise fordert die ISO/IEC 27001 als Massnahme «Regelungen zum Zugriff auf Netze und Netzwerkdienste». Die ISO/IEC 27002 empfiehlt hierzu einzelne Punkte, die in einer Richtlinie enthalten sein sollten.

6. Rechtfertigungsgründe

Die Datenbearbeitung durch private Personen ist gemäss Art. 12 Abs. 1 DSG; Art. 30 Abs. 1 nDSG grundsätzlich erlaubt, wenn die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzt wird. Art. 12 Abs. 2 DSG; Art. 30 Abs. 2 nDSG bestimmen, wann eine Persönlichkeitsverletzung vorliegt. Das allgemein verankerte Grundkonzept des Persönlichkeitsschutzes gemäss Art. 28 ZGB wird dabei übernommen und durch die vorgenannten Datenbearbeitungsgrundsätze[94] ergänzt.[95] Eine Persönlichkeitsverletzung ist dabei immer das Resultat der konkreten Art und Weise oder der Umstände einer Datenbearbeitung und erfordert eine gewisse Intensität der Beeinträchtigung. Wie beim Persönlichkeitsschutz gemäss Art. 28 ZGB verlangt also auch das DSG die Vornahme einer Interessensabwägung zur Bestimmung des Vorliegens einer Persönlichkeitsverletzung.[96]

Die gesetzlichen Fiktionen in Art. 12 Abs. 2 DSG, Art. 30 Abs. 2 nDSG schliessen nicht aus, dass die Persönlichkeitsverletzung durch Rechtfertigungsgründe[97] gerechtfertigt ist. Allerdings können gemäss der bundesgerichtlichen Rechtsprechung Rechtfertigungsgründe in diesen Fällen nur mit grosser Zurückhaltung bejaht werden.[98] Jede Persönlichkeitsverletzung, die nicht gerechtfertigt ist, ist widerrechtlich.[99] Rechtfertigungsgründe sind neben der Einwilligung ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Grundlage. Diese Rechtfertigungsgründe decken sich mit jenen in Art. 28 Abs. 2 ZGB.[100] Artikel 13 Abs. 2 DSG, Art. 31 Abs. 2 nDSG zählen weitere Fälle auf, in denen ein überwiegendes Interesse der bearbeitenden Person gegeben sein kann.

---

94 Art. 4 DSG; Art. 6 nDSG.

95 Handkommentar DSG-ROSENTHAL (FN 47), Art. 1 N 2; BELSER EVA MARIA/HOUSSEIN NOUREDDINE, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht, Bern 2011, § 8 N 69.

96 Handkommentar DSG-ROSENTHAL (FN 47), Art. 12 N 2.

97 Art. 13 DSG; Art. 31 nDSG

98 BGE 136 II 520, E. 5.2.4.

99 Art. 13 Abs. 1 DSG; Art. 31 nDSG.

100 BGE 138 II 346, E. 10.1.

a) Einwilligung

Die Einwilligung hat nach einer angemessenen Information freiwillig zu erfolgen.[101] Hinsichtlich einer informierten Einwilligung in die Nutzung der erhobenen Personendaten stellen sich diverse Probleme. Falls die Einwilligung der betreffenden Person oder ein gesetzlicher Rechtfertigungsgrund vorliegt, erfolgt grundsätzlich keine Interessenabwägung und die Abwägungsgründe[102] kommen nicht zum Zug.[103] Viele Datenbearbeiter wollen sich daher mittels Einholen einer Einwilligung auf einfache Weise absichern und stützen die Bearbeitung auf diesen Rechtfertigungsgrund.[104] Die Einwilligung verlangt wie gesagt lediglich eine angemessene Information.[105]

Im Arbeitsverhältnis bildet die Einwilligung einen Spezialfall, denn Art. 328b OR erlaubt Arbeitgebern einzig Bearbeitungen, die im Zusammenhang mit der Eignung von Arbeitnehmenden für das Arbeitsverhältnis oder zur Durchführung des Arbeitsvertrages erlaubt sind, wodurch eine Einwilligung a priori ausser Betracht fällt.[106] Mit dieser Regelung trägt der Gesetzgeber dem Subordinationsverhältnis Rechnung, wodurch die Freiwilligkeit sehr begrenzt wird. Geht es um die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen[107], muss die Einwilligung ausdrücklich erteilt werden.[108] Daraus ergeben sich die weiteren Voraussetzungen, wie zum Beispiel des Zeitpunkts der Erteilung der Einwilligung vor der Datenbearbeitung. Zudem muss die betroffene Person angemessen informiert werden über sämtliche Punkte[109], die zum Treffen einer freien Entscheidung unter Abwägung der Konsequenzen und Risiken notwendig sind. Die besonderen Informationspflichten gemäss Art. 14 DSG, 19 nDSG gelten neu nicht mehr nur für besonders schützenswerte, sondern sämtliche Personendaten.

Online sind die meisten Personen – sowohl die Bearbeiter von Daten, als auch die Personen, über die Daten bearbeitet werden – noch nicht genügend für Fragen des Persönlichkeitsschutzes sensibilisiert und gehen leichtfertig mit persönlichen Daten um. So nehmen Internetuser beispielsweise das Ausfüllen von Wettbewerbsformularen oder eine sofortige Belohnung in Form von Rabattgutscheinen wichtiger als die daraus allfällig resultierenden

---

101 Art. 4 Abs. 5 DSG; Art. 6 Abs. 6 nDSG.

102 Art. 31 Abs. 2 nDSG.

103 Botschaft DSG 2017 (FN 4), 7073.

104 Handkommentar DSG-ROSENTHAL (FN 43), Art. 13 N 6.

105 Art. 6 Abs. 6 nDSG.

106 Vgl. auch Art. 362 OR.

107 Persönlichkeitsprofile werden durch das Profiling gemäss Art. 4 lit. f nDSG ersetzt.

108 Art. 6 Abs. 7 lit. a nDSG.

109 Zweck, Art und Weise, Umfang der Datenbearbeitung, Kategorie der bearbeiteten Daten, Verantwortlicher Datenbearbeiter.

negativen Konsequenzen.[110] Privatsphäre und Datenschutz werden zwar als wichtig empfunden, diese Erkenntnis spiegelt sich aber nicht zwangsläufig im Verhalten der betroffenen Personen im Umgang mit ihren Daten wieder.[111] «Leistung gegen Daten» wird von vielen Personen als kostenlos wahrgenommen und die Reichweite der Einwilligung in die Bearbeitung ihrer persönlichen Daten kaum überblickt.

Der sorglose Umgang mit Personendaten kann auch zu Problemen bei der Umsetzung des DSG führen.[112] Das DSG ist ein Rahmengesetz und erlaubt als solches einen Spielraum bei der Beurteilung von Daten- und Persönlichkeitsschutzschutzverletzungen. Vordergründig zählt der Einzelfall in Form von bestimmten Datenbearbeitungen, die es zu beurteilen gilt. Dabei können sich sowohl technische als auch organisatorische Probleme ergeben.[113] Die Informationstechnologie macht stetig Fortschritte, so dass es möglich ist, enorme Mengen von Personendaten zu erfassen und miteinander in Verbindung zu setzen.[114] Leider hält das Sicherheitsbewusstsein sowohl der Datenbearbeiter, als auch der Personen, über die Daten bearbeitet werden, oft nicht mit dem technischen Fortschritt mit, was vor allem im Homeoffice aufgrund der räumlichen Distanz beider Parteien problematisch erscheint. Die Revision des DSG hat zum Ziel, das Schutzniveau für Betroffene den technischen Entwicklungen und der Digitalisierung anzupassen und die Stellung der Bürgerinnen und Bürger zu stärken.[115]

b) Überwiegendes privates Interesse

Neben der Einwilligung stehen gem. Art. 13 Abs. 1 DSG; Art. 31 nDSG eine gesetzliche Grundlage und überwiegende private Interessen als weitere Rechtfertigungsgründe zur Verfügung. Ein überwiegendes privates Interesse der datenbearbeitenden Person kommt infrage, wenn in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über den Vertragspartner bearbeitet werden, beispielsweise im Falle der Rekrutierung oder Selektionierung von Arbeitnehmenden oder auch zur Leistungsmessung. Der Rechtfertigungsgrund gilt allerdings jeweils nur zum Zweck der Reduktion des Vertragsrisikos und muss sowohl verhältnismässig sein als auch nach einer Interessenabwägung die Datenschutzinteressen der betroffenen Person überwiegen. Bei der

110 ENGELS BARBARA, Datenschutzpräferenzen von Jugendlichen in Deutschland, IW-Trends Nr. 2 vom 21. Mai 2018, (zit. ENGELS), 5.

111 Ebenda.

112 <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html> (28.02. 2021).

113 Ebenda.

114 Ebenda.

115 <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (28.02.2021).

Bearbeitung arbeitsrelevanter Daten bemisst sich das überwiegende Interesse zudem an Art. 328b OR.

c) Gesetz

Im Rahmen der COVID-19-Pandemie besteht eine gesetzliche Grundlage für die Bearbeitung der Personendaten in Art. 58 ff. EpG. Es bestehen umfassende Rechtsgrundlagen für die Bearbeitung von Personendaten[116], die Bekanntgabe von Personendaten an Dritte[117] sowie auch die Übermittlung von Personendaten ins Ausland und an ausländische Behörden[118]. Zusätzlich ist der Betrieb von Informationssystemen geregelt. Zur Datenbearbeitung ermächtigt sind das BAG, die zuständigen Behörden der Kantone und die nach dem EpG beauftragten öffentlichen und privaten Institutionen.[119] Der zulässige Zweck der Datenbearbeitung umfasst neben den krankheitsspezifischen Informationen, die Rückschlüsse auf die Infektionsquelle und auf das Gefahrenpotenzial zulassen, auch personenidentifizierende Angaben wie den Name, das Geburtsdatum und die Wohnadresse der Betroffenen, um die epidemiologisch notwendigen Rückschlüsse und Nachforschungen tätigen zu können.[120]

Bundesorgane dürfen Personendaten zudem generell nur bearbeiten, wenn eine gesetzliche Grundlage besteht.[121] Hieran spiegelt sich die konzeptionelle Ausrichtung des DSG wieder, es folgt dem Legalitätsprinzip im öffentlich-rechtlichen Bereich und dem Prinzip der Rechtfertigung im privatrechtlichen Bereich. Für die Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen/Profiling wird grundsätzlich eine formelle gesetzliche Grundlage verlangt.[122] Die Bekanntgabe von Personendaten an Dritte ist ebenfalls an das Vorliegen einer Rechtsgrundlage geknüpft, dies unter Vorbehalt der in Art. 19 Abs. 1 DSG, Art. 36 nDSG vorgesehenen Ausnahmen. Personendaten dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich vorgesehen ist. Die Anforderungen sind noch strenger für besonders schützenswerte Personendaten und für Persönlichkeitsprofile, welche nur durch ein Abrufverfahren zugänglich gemacht werden dürfen, wenn ein formelles Gesetz es ausdrücklich vorsieht.[123]

---

116 Art. 58 EpG.

117 Art. 59 EpG.

118 Art. 62 EpG.

119 Art. 58 Abs. 1 EpG.

120 Botschaft zur Revision des Bundesgesetzes über die Bekämpfung übertragbarer Krankheiten des Menschen vom 3. Dezember 2010, BBI 2011 311 ff., (zit. Botschaft Bekämpfung Krankheiten 2010), 406.

121 Art. 17 Abs. 1 DSG; Art. 34 Abs. 1 nDSG.

122 Art. 17 Abs. 2 DSG; 34 Abs. 2 nDSG.

123 Art. 19 Abs. 3 DSG; Art. 36 Abs. 3 nDSG.

7. Rechtsansprüche und Sanktionen

Die Rechtsansprüche betroffener Personen richten sich nach Art. 15 DSG und gelten auch weiterhin, neu in Art. 32 nDSG. Betroffene Personen werden auf Klagen zum Schutz der Persönlichkeit der Art. 28, 28a und 281 ZGB verwiesen. Art. 281 ZGB bezieht sich auf das Recht auf Gegendarstellung und ist deshalb vorliegend nicht von Interesse. Arbeitnehmende, deren Persönlichkeit widerrechtlich verletzt wurde, können gemäss Art. 28 Abs. 1 ZGB gegen jeden, der an der Verletzung mitgewirkt hat, das Gericht anrufen. Art. 28a Abs. 1 ZGB enthält sodann Beseitigungs-, Feststellungs- und Unterlassungsansprüche. Deliktische Ansprüche und Ansprüche aus der Geschäftsführung ohne Auftrag ergeben sich aus Art. 28a Abs. 3 DSG, wonach Klagen auf Schadensersatz[124] und Genugtuung[125] sowie auf Herausgabe eines Gewinns entsprechend den Bestimmungen über die Geschäftsführung ohne Auftrag (GoA)[126] vorbehalten sind.

Dem EDÖB werden bei Verletzungen von Datenschutzvorschriften in Art. 51 nDSG erweiterte Kompetenzen zugewiesen. Neu kann er nicht nur Massnahmen empfehlen, sondern Verwaltungsmassnahmen auch verfügen. Dies betrifft beispielsweise das Abbrechen, ganz oder teilweise Löschen oder Vernichten von Personendaten. Oder ein Verbot, Personendaten ins Ausland bekannt zu geben, die Anordnung einer Datenschutz-Folgenabschätzung, oder einer betroffenen Person die Auskünfte zu erteilen. Nach wie vor kann der EDÖB jedoch keine Bussen[127] aussprechen, was die Wirksamkeit der neugewonnen Kompetenz sehr relativiert. Der EDÖB muss bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten und die Rolle als Privatklägerschaft wahrnehmen.[128] Die Sanktions-Kompetenz bleibt somit auch weiterhin ausschliesslich bei den Kantonen. Aufgrund der eher knappen Ressourcen des EDÖB ist somit auch weiterhin zu erwarten, dass drohende Reputationsschäden, welche für Unternehmen oftmals zu immensen finanziellen Verlusten führen, durch öffentliche Bekanntmachungen von Verstössen das stärkste Mittel des EDÖB bleiben.

Seit dem Inkrafttreten der DSGVO werden Unternehmen bei Datenschutz-Verletzungen mit hohen Bussen bestraft werden. Unternehmen drohen Bussen von bis zu 10 Millionen Euro oder 2 % des Jahresumsatzes, je nachdem, welcher Wert höher ist.[129] Im schweizerischen nDSG können nach wie vor nur vorsätzlich handelnde natürliche Personen, etwa Führungskräfte eines Unternehmens, sanktioniert werden. Nur wenn eine Busse unter CHF 50’000 in Betracht fällt und die Ermittlung der strafbaren Person im Hinblick auf die

124 Art. 41 Abs. 1 OR.

125 Art. 49 Abs. 1 und 2 OR.

126 Art. 419 ff. OR.

127 Bezüglich die Missachtung von Verfügungen siehe Art. 63 nDSG.

128 Art. 65 nDSG.

129 Art. 83 Abs. 4 DSGVO.

verwirkte Strafe einen unverhältnismässigen Aufwand bedingt, kann ein Unternehmen zur Bezahlung verurteilt werden.[130] Das Strafmass der Sanktionen ist dafür deutlich geringer gegenüber jenem der DSGVO und sieht Sanktionen in der Höhe bis maximal CHF 250'000 vor.[131] Mit einer Busse können neu auch Verstösse gegen die Mindestanforderungen der Datensicherheit belegt werden. Gleichermassen strafbar ist auch eine unzulässige Auslandsübermittlung, oder beispielsweise die Verletzung von Informationspflichten.

III. Unzulässige Verhaltenskontrolle gemäss ArG/ArGV3

1. Rechtsgrundlagen

Eine Überwachung oder Kontrolle stellt immer eine Gefährdung für die Gesundheit und die persönliche Integrität der Mitarbeitenden gemäss Art. 6 ArG dar.[132] Art. 26 ArGV 3 verankert den Persönlichkeitsschutz entsprechend im öffentlichen Recht. Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmenden am Arbeitsplatz überwachen, sind unzulässig.[133] Vor dem Hintergrund, dass im Homeoffice die Grenzen zwischen Berufs- und Privatleben teilweise verschwimmen, erscheint das Überwachungsverbot für das Homeoffice umso bedeutender. Als Überwachungs- und Kontrollsysteme gelten namentlich Videoanlagen, Computersysteme und -netzwerke, Telefonanlagen, Gegensprechanlagen, Fotokopiergeräte und GPS.[134] Allgemein geht es um alle technischen Einrichtungen, durch die einzelne oder mehrere Tätigkeiten oder Verhaltensweisen der Arbeitnehmenden erfasst werden können.[135] Ist eine Überwachung aus anderen Gründen erforderlich, sind sie gemäss Art. 26 Abs. 2 ArGV 3 erlaubt, sofern sie analog Art. 6 ArG die Gesundheit und Bewegungsfreiheit der Arbeitnehmenden nicht beeinträchtigt. Von einer unzulässigen Verhaltensüberwachung im Arbeitsverhältnis ist im Allgemeinen die Rede, wenn die betroffene Person nicht nur während der eigentlichen Arbeit, sondern auch während der unproduktiven Zeiten überwacht werden. Ob eine allfällige Beeinträchtigung der Gesundheit und der Bewegungsfreiheit besteht, ist jeweils einzelfallabhängig zu bewerten.

---

130 Art. 64 Abs. 2 nDSG.

131 Art. 60 nDSG.

132 PÄRLI (FN 45), 700 f. N 17.35.

133 Art. 26 Abs. 1 ArGV 3.

134 SECO, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Art. 26, 326-2.

135 EDÖB, Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich Bearbeitung durch private Personen, Bern, Oktober 2014, 16 ff.

Eine Abgrenzung zwischen verbotener Verhaltens- und zulässiger Leistungs- oder Sicherheitsüberwachung kann in vielen Fällen Schwierigkeiten bereiten, beziehungsweise sogar unmöglich sein.[136] Kommen beispielsweise zur Optimierung von Arbeitsabläufen und -prozessen Überwachungs- und Assistenzsysteme zum Einsatz, produzieren und speichern diese riesige Datenmengen (sog. Big Data).[137] Eine Verknüpfung der unterschiedlichen Datenquellen durch Algorithmen ermöglicht die Erstellung von virtuellen Persönlichkeitsprofilen und könnte auch zur Verhaltenskontrolle und damit zur unzulässigen Überwachung verwendet werden. Arbeitnehmende werden für die Unternehmen zu «gläsernen Beschäftigten».[138] Selbst wenn die Daten nicht gezielt zu Überwachungszwecken erhoben werden, bilden sie ein risikobehaftetes Nebenprodukt modernen Informations- und Kommunikationstechnologie und beinhalten ein hohes Missbrauchspotenzial. Im Rahmen der Revision des DSG und in Annäherung an die DSGVO ist bzgl. Analytics-Anwendungen auch auf das neue Recht auf «menschliches Gehör» hinzuweisen. Es handelt sich dabei um das Recht einer Person, nicht einer Entscheidung unterworfen zu werden, die ausschliesslich auf einer automatisierten Verarbeitung beruht und ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

2. Enge Grenzen der Überwachung

Bei der Verwendung von Überwachungstechnologien kollidieren unterschiedliche Interessen. Arbeitnehmende haben ein Recht auf Schutz ihrer Persönlichkeit.[139] Tangiert werden vor allem die Privatsphäre, aber auch die Intimsphäre oder die familiären Verhältnisse.[140] Der Schutz ist jedoch nicht absolut; die Schutzwürdigkeit der Arbeitnehmenden steht in Konkurrenz zu den berechtigten Arbeitgeberinteressen.[141] Arbeitgeber haben im Rahmen ihrer gesetzlichen Fürsorgepflicht[142] auch die Verpflichtung, die Einhaltung der vertraglichen Arbeitsleistung und die zweckmässige Organisation der Arbeitsabläufe zu beaufsich-

136 SECO, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Art. 26, 326-1.

137 Sog. «People Analytics», siehe dazu: KASPER GABRIEL/WILDHABER ISABELLE, Big Data am Arbeitsplatz: Datenschutz- und arbeitsrechtliche Herausforderungen von People Analytics in Schweizer Unternehmen, in: Ueli Kieser/Kurt Pärli/Ursula Uttinger (Hrsg.) Datenschutztagung 2018, Zürich/St. Gallen 2019.

138 DÄUBLER WOLFGANG, Gläserne Belegschaften? Das Handbuch zum Beschäftigtendatenschutz, 7. Aufl. 2017, Frankfurt a. M., 37 N 5.

139 Vgl. unter Ziff. II. 1; Art. 13 BV, Art. 17 UNO Pakt II, Art. 328 OR.

140 <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz/erlaeuterungen-zur-videoueberwachung-am-arbeitsplatz.html> (20.02.2021).

141 GEISER/MÜLLER/PÄRLI (FN 13), N 453 ff.

142 Art. 328 OR.

tigen und zu überwachen.[143] Des Weiteren sind sie zur Beaufsichtigung und Überwachung der Gesundheit und Arbeitssicherheit der Arbeitnehmenden sowie der Gewährleistung der Datensicherheit schützenswerter Informationen des Unternehmens verpflichtet.[144]

Neben ihrer gesetzlichen Verpflichtung motiviert auch deviantes Verhalten der Arbeitnehmenden Arbeitgeber zur elektronischen Überwachung, beispielsweise bei Verdacht auf nicht arbeitsplatzbezogene Aktivitäten wie übermässiger privater Internetnutzung. Gerade aufgrund der räumlichen Distanz wird das Vertrauen der Arbeitgeber in die Produktivität der Arbeitnehmenden beim Homeoffice auf die Probe gestellt. Vertrauen ist der subjektive Glaube bzw. die individuelle Überzeugung, dass sich eine Person oder Organisation nicht zum Nachteil verhält. Da Überwachung und Kontrolle häufig auf mangelndem Vertrauen basiert («Vertrauen ist gut, Kontrolle ist besser»), assoziieren Arbeitnehmende mit Überwachungs- und Kontrollsystemen mehrheitlich eine negative Affektivität.[145] Diese spiegelt sich bei den Betroffenen in einer ablehnenden Haltung wieder und kann ein Gefühl von Misstrauen, Stress und Angst hervorrufen sowie den Verlust von Privatsphäre und Freiheit bedeuten.[146] Zudem wird davon ausgegangen, dass auch die Arbeitsmotivation und -zufriedenheit durch Überwachung gemindert wird, woraus eine Beeinträchtigung der Leistungsfähigkeit resultiert.[147]

---

143 GEISER THOMAS, Überwachung am Arbeitsplatz – Der schmale Grat zwischen rechtlicher Notwendigkeit und den rechtlichen Schwanken, in digma 2/2015 50–51 (zit. GEISER, Überwachung 2015) 50.

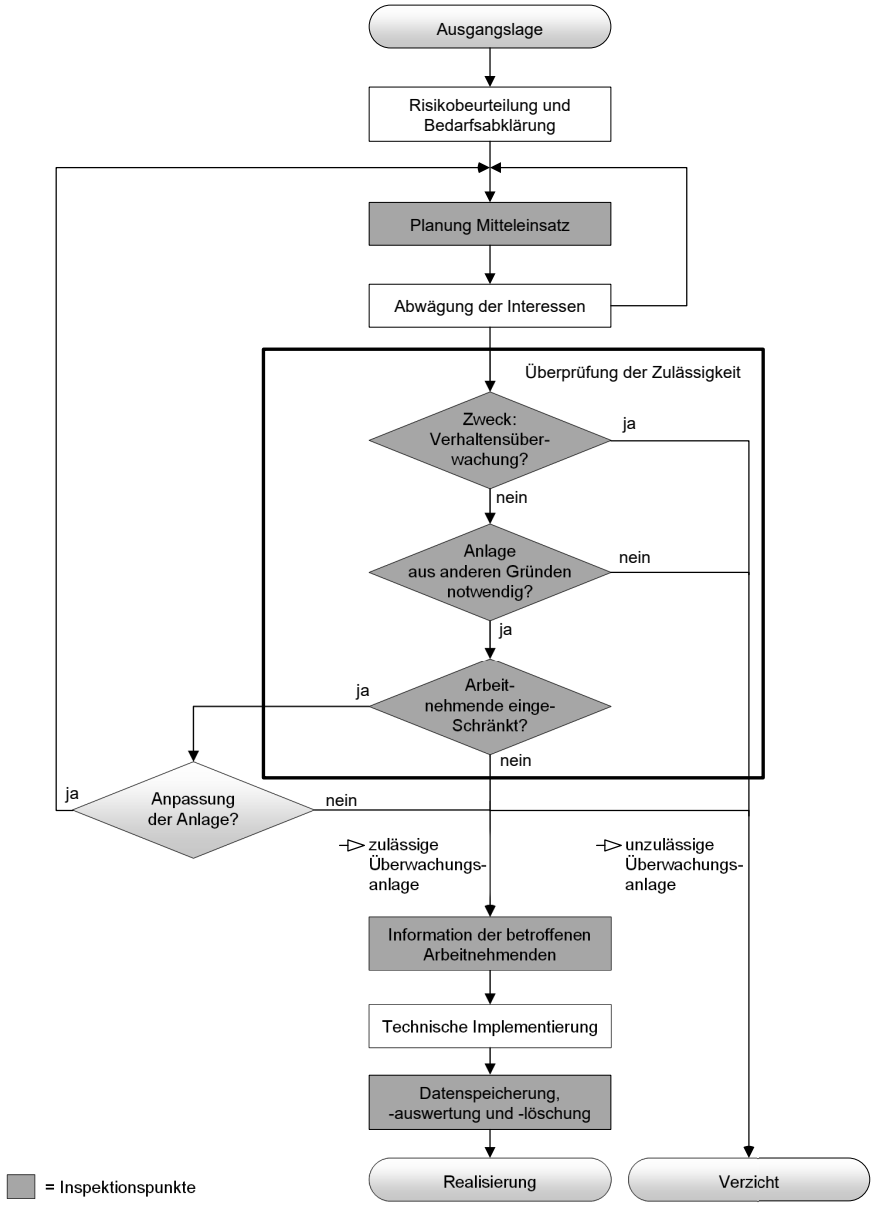
144 Ebenda; HUGL ULRIKE, Workplace surveillance: examining current instruments, limitations and legal backround issues, in: Tourism & Management Studies, 9/2013, 58–63

145 SCHOORMAN DAVID, WOOD MALLORY, BREUER CHRISTINA, Would trust by any other name smell as sweet? Reflections on the meanings and uses of trust across disciplines and context, in: Brian Bornstein/Alan Tomkins (Hrsg.) Motivating Cooperation and Compliance with Authority, Springer 2015, 13–35

146 BECKER THOMAS, MARIQUE GÉRALDINE, Observer Effects without Demand Characteristics: An Inductive Investigation of Video Monitoring and Performance, in: Journal of Business and Psychology, 4/2014, 541–553, 542 ff.; BACKHAUS NILS, Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz: Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte, Zeitschrift für Arbeitswissenschaft 73, 2019, 3.

147 BARTELS LYNN, NORDSTROM CYNTHIA, Examing big brother's purpose for using electronic performance moitoring, in: Performance Improvement Quaterly, 25, 2012, 65–77; SECO, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Art. 26, 326-1.

Vor der Installation eines neuen Überwachungs- und Kontrollsystem ist folgende Planungs- und Entscheidgrundlage[148] heranzuziehen und zu befolgen:



148 SECO, Empfohlene Planungs- und Entscheidgrundlage für ein neues Überwachungs- und Kontrollsystem, Abbildung 326-1, in: Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Art. 26, 326-3.

Für die Zulässigkeit eines Überwachungs- und Kontrollsystems im Hinblick auf Art. 26 ArGV 3 müssen – zusätzlich zu den Bearbeitungsgrundsätzen des DSG – kumulativ drei Voraussetzungen erfüllt sein.[149] Zunächst muss ein klar überwiegendes Interesse des Betriebs an der Überwachung gegenüber dem Interesse der Arbeitnehmenden am Schutz seiner Privatsphäre vorliegen. Ist ein überwiegendes Interesse an Überwachungssystemen zu bejahen, dürfen sie nur so eingesetzt, dass der Persönlichkeitsschutz und der Gesundheitsschutz der Arbeitnehmenden so weit wie möglich gewahrt bleibt (Verhältnismässigkeit).[150] Es muss dasjenige Überwachungsmittel gewählt werden, mit dem sich das Überwachungsziel gerade noch erreichen lässt. Dabei kommt es auf den angestrebten Überwachungszweck und die konkreten Umstände an. Die getroffenen Massnahmen müssen zudem regelmässig überprüft werden.

Die Installation von Spyware zur Überprüfung, ob beispielsweise das Internet privat genutzt wird, ist gemäss bundesgerichtlicher Rechtsprechung ohne vorherige, detaillierte Information der betroffenen Arbeitnehmenden unverhältnismässig und damit unzulässig.[151] Arbeitgeber dürfen nur im Rahmen der Verhältnismässigkeit technische Massnahmen ergreifen, um unzulässige oder dienstfremde Websites zu sperren. Des weiteren könnten, wenn keine milderen Massnahmen bestehen, schwere Missbräuche auch durch Überprüfung der Logfiles aufgedeckt werden, welche nicht die konkrete Website oder E-Mail offenlegen, sondern lediglich Randdaten enthalten, die in anonymisierter Form auswertbar sind.[152] Die personenbezogene Auswertung ist ausschliesslich dem konkreten Missbrauchsfall vorbehalten.[153]

3. Mitwirkung

Zuletzt muss auch die Mitwirkung der Arbeitnehmenden an der Planung, Einrichtung und Einsatzzeit sichergestellt werden. Soll ein Überwachungs- und Kontrollsystem eingeführt werden, haben diese Anspruch auf vorherige, aktive Information und Anhörung.[154] Die Pflicht zur Konsultation lässt sich ebenfalls auf den Gesundheitsschutz der Arbeitnehmenden stützen.[155] Das Recht auf Anhörung umfasst das Recht, Einwände zu erheben und Vorschläge zu unterbreiten, bevor ein Entscheid über die Installation eines Kontroll- oder

---

149 SECO, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Art. 26, 326-1 und 2; GEISER/MÜLLER/PÄRLI (FN 13), N 457.

150 BGE 130 II 435 E. 4.2 und 4.4; Urteil des Bundesgerichts 6B_536/2009 vom 12.11.2009 E. 3.6.2.

151 BGE 139 II 7 E. 5.5.

152 EDÖB, Leitfaden über die Internet- und E-Mailüberwachung am Arbeitsplatz, Für die Privatwirtschaft, Bern, September 2013 (zit. EDÖB Überwachung), 3.

153 EDÖB Überwachung (FN 152), 9.

154 Art. 5 f. ArGV 3.

155 Art. 48 Abs. 1 lit. a ArG.

Überwachungssystems getroffen wird.[156] Entsprechend hat die Information über die Massnahmen gegenüber den Mitarbeitenden in präziser und verständlicher Form zu erfolgen. Arbeitgeber sollten ihre Mitarbeitenden grundsätzlich über die Handhabung von elektronisch generierten Daten im Unternehmen informieren. Empfehlenswert wäre, diese Angaben beispielsweise im betriebsinternen IT-Nutzungsreglement festzuhalten.

Die Einhaltung der Vorgaben zu Überwachungs- und Kontrollsystemen kann von den Vollzugsbehörden des Arbeitsgesetzes überprüft werden.

IV. Homeoffice aus dem Ausland

Arbeiten Mitarbeitende von Schweizer Arbeitgebern mit Sitz in der Schweiz aus dem Homeoffice im Ausland, könnte dies neben steuer- und sozialversicherungsrechtlichen Besonderheiten auch Auswirkungen auf den Datenschutz haben. Betroffenen Personen droht der Verlust über die Kontrolle über ihre eigenen Daten und das Risiko für eine Persönlichkeitsverletzung steigt.[157] In einem ersten Schritt ist stets das anwendbare Recht zu prüfen. Art. 121 IPRG[158] sieht vor, dass der Arbeitsvertrag demjenigen Recht unterworfen ist, in dem Arbeitnehmende gewöhnlich ihre Arbeit verrichten. Für Mitarbeitende, die permanent aus dem ausländischen Homeoffice ihre Arbeit verrichtet, ist damit das jeweilige ausländische Recht anwendbar. Um Rechtsunsicherheiten vorzubeugen, ist in diesen Fällen der Gebrauch der beschränkten Rechtswahlmöglichkeit gemäss Art. 121 Abs. 3 IPRG zu empfehlen, wonach die Parteien den Arbeitsvertrag schweizerischem Recht unterstellen können.

Der grenzüberschreitende Datenverkehr wird im Einklang mit der DSGVO und der Mehrheit der Rechtsordnungen der EU-Mitgliedstaaten mit Inkrafttreten des nDSG durch Verzicht des Schutzes der Daten juristischer Personen insgesamt erleichtert. Insofern nimmt voraussichtlich auch die mit Risiken verbundene Datenbearbeitung aus dem Ausland an Bedeutung zu, welche nach dem DSG mit speziellen Sorgfaltspflichten des Arbeitgebers verbunden ist. Der Tatbestand der Datenübermittlung ins Ausland gilt bereits als erfüllt, sobald die Möglichkeit besteht, aus dem Ausland auf einen Server in der Schweiz zuzugreifen. Ob Mitarbeiter tatsächlich davon Gebrauch machen, ist nicht entscheidend. Arbeitgeber müssen stets die allgemeinen Bearbeitungsgrundsätze einhalten und die Angemessenheit des Schutzes im Ausland gewährleisten. Gemäss Art. 6 Abs. 1 und 2 DSG; Art. 16 nDSG dürfen Personendaten nicht ins Ausland bekannt gegeben und von Arbeitnehmenden im Homeoffice bearbeitet werden, wenn die Gesetzgebung des Staates keinen angemessenen

156 Art. 6 Abs. 3 ArG.

157 EDÖB, Leitfaden für die Bearbeitung von Personendaten im privaten Bereich, Bern, August 2009, 6.

158 Bundesgesetz über die Internationale Privatwirtschaft vom 18. Dezember 1987 (IPRG; SR 291).

Schutz sicher stellt. Zu diesem Zweck bedarf eine Datenübermittlung gemäss Art. 16 Abs. 1 nDSG grundsätzlich der Genehmigung durch den Bundesrat. Die besondere Genehmigungspflicht entfällt jedoch beim Bestehen geeigneter Garantien, welche den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stellen. Geeignete Garantien bieten völkerrechtliche Verträgen, oder – jeweils nach vorheriger Mitteilung und allenfalls Genehmigung durch den EDÖB – vertragliche Datenschutzklauseln, spezifische Garantien des zuständigen Bundesorgans, Standarddatenschutzklauseln[159] oder verbindliche unternehmensinterne Datenschutzvorschriften.[160] Der EDÖB publiziert zudem eine Liste jener Staaten, welche einen angemessenen Datenschutz gewährleisten.[161] Ausnahmen werden für bestimmte Fälle in Art. 17 nDSG bezeichnet. Hat die betroffene Person beispielsweise ausdrücklich – nach vorgängiger Information über die Risiken – in die Bekanntgabe ins Ausland eingewilligt, ist weder ein Angemessenheitsbeschluss noch das Vorliegen geeigneter Garantien erforderlich. Die Rechtfertigungsgründe gemäss Art. 6 Abs. 2 DSG; Art. 17 nDSG sind dabei gegenüber denjenigen von Art. 13 Abs. 1 DSG; Art. 31 nDSG eingeschränkt, wobei insbesondere ein überwiegendes privates Interesse zwar eine Datenbekanntgabe nach Art. 12 DSG[162]; Art. 30 nDSG, nicht jedoch eine solche nach Art. 6 Abs. 1 DSG[163]; Art. 16 Abs. 1 nDSG zu rechtfertigen vermag.[164]

V. Fazit

Die Arbeit vom Homeoffice ist aus datenschutzrechtlicher Sicht mit grossen Risiken verbunden, sowohl für Arbeitnehmende wie auch für Arbeitgeber. Auch wenn interne Reglemente oder organisatorische Regelungen und technische Sicherheitsmassnahmen zum Schutz von Daten und Informationen bestehen, lassen sich diese durch einen sorglosen Umgang auf einfache Weise umgehen. Den Königsweg sowohl für den Schutz der Privatsphäre und der Integrität und Arbeitnehmenden als auch für Arbeitgeber zur Einhaltung der gesetzlichen Bestimmungen bildet ein Gesamtarbeitsvertrag (GAV).

Arbeitnehmende und Vorgesetzte müssen für die aus datenschutzrechtlicher Sicht lauernden Gefahren, die mit dem Homeoffice verbunden sind, sensibilisiert werden und bezüglich der bereitzustellenden Sicherheitsmassnahmen explizit geschult werden. So sollte beispielsweise auf das mit grossen Risiken verbundene BYOD zumindest im Homeoffice u.E. ver-

159 Art. 6 Abs. 3 Verordnung zum Bundesgesetz über den Datenschutz vom 14. juni 1993 (VDSG; SR 235.11).

160 Art. 16 Abs. 2 nDSG.

161 Art. 7 VDSG.

162 Vgl. Art. 13 Abs. 1 DSG.

163 Vgl. Art. 6 Abs. 2 DSG.

164 OGer ZH, LF140075-O, Urteil vom 3. März 2015, 16, E. 3.1.

zichtet werden und Arbeitgeber sollten die geschützten und gewarteten Arbeitsgeräte ihren Mitarbeitern zur Verfügung stellen. Des Weiteren haben Arbeitgeber jede Verhaltenskontrolle der Arbeitnehmenden im Homeoffice zu unterlassen. Beim Homeoffice aus dem Ausland bestehen neben besonderen Gefahren für den Datenschutz auch besondere Anforderungen, welche mit einer allfälligen Datenbearbeitung aus dem Ausland einhergehen.

Im Rahmen der Revision des DSG wäre die Einführung von kollektiven Rechtsdurchsetzungsmechanismen im Datenschutz aufgrund der zunehmenden Technologisierung wünschenswert gewesen. Neben der allgemeinen Verbandsklage (Art. 89 ZPO) bestehen anderenorts bereits besondere Verbandsklagen im Gleichstellungsgesetz (GlG)[165], im Lauterkeitsgesetz (UWG)[166] oder im Mitwirkungsgesetz[167], sodass diese in Anlehnung an Art. 80 DSGVO auch im revidierten DSG die Rechte der Arbeitnehmenden E-DSG im Bereich des Datenschutzes gestärkt hätten.

165 Bundesgesetz über die Gleichstellung von Frau und Mann vom 24. März 1995 (GlG; SR 151.1).

166 Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (UWG; SR 241).

167 Bundesgesetz über die Information und Mitsprache der Arbeitnehmerinnen und Arbeitnehmer in den Betrieben vom 17. Dezember 1993 (Mitwirkungsgesetz; SR 822.14).

ISBN 978-3-03891-278-1