www.betriebs-berater.de

Betriebs Berater

75 Jahre

4|2021

AWG ... W&I ... Managementbeteiligung ... ESG ... Keylogger ... Recht ... Wirtschaft ...

25.1.2021 | 76. Jg.
Seiten 193–256

Schwerpunktheft M&A

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Dr. Justus Frank, LL.M., RA, und Dipl.-Jur. Maurice Heine

„Corona und die Detektive"? Corona und Keylogger!? – Kontrollmöglichkeiten in Zeiten von Home-Office

Im Zuge der Corona-Pandemie sind viele Arbeitnehmer im *Home-Office* tätig. Das epidemiologisch gebotene *Social distancing* nimmt dem Arbeitgeber jedoch wichtige Kontrollmöglichkeiten gegenüber den Arbeitnehmern. Zwar kann der Arbeitgeber auch die im Home-Office Beschäftigten anweisen, in bestimmten Abschnitten über den Fortschritt von Projekten zu berichten und (Teil-)Arbeitsergebnisse vorzulegen. Die Möglichkeit, dem Arbeitnehmer stichprobenartig „über die Schulter" und „auf die Finger" zu schauen, versiegt indes nahezu völlig. Was des einen Leid ist des anderen Freud: Medienberichten zufolge erleben Privatdetekteien mitunter Hochkonjunktur (*Fischermann*, Die Zeit vom 14.5.2020, 19). Welche präventiven und repressiven Kontrollmaßnahmen des Arbeitgebers zur Überwachung der Arbeitnehmer aber sind erlaubt? Welche Rolle spielen digitale Anwendungen wie *Screenshot Monitoring* oder *Time Tracking*? Der Beitrag nimmt verschiedene Kontrollmöglichkeiten des Arbeitgebers im Zeitalter distanzierter Arbeit in den Blick und ordnet diese systematisch ein.

I. Zulässigkeit

Kontrollmaßnahmen des Arbeitgebers gegenüber Beschäftigten stellen – gleich, ob heimlich (verdeckt) oder offen vorgenommen[1] – rechtfertigungsbedürftige Verarbeitungen personenbezogener Daten dar (Art. 4 Nr. 2 DSGVO). Ihre Zulässigkeit bemisst sich nach § 26 BDSG i.V.m. Art. 88 DSGVO.

1. Einwilligung

Kontrollmaßnahmen können auf eine Einwilligung des Beschäftigten gestützt werden (Art. 6 Abs. 1 S. 1 lit. a) DSGVO). Diese muss allerdings freiwillig erteilt worden sein (Art. 4 Nr. 11 DSGVO). Gemäß § 26 Abs. 2 S. 1 BDSG ist bei der Beurteilung der Freiwilligkeit die im Beschäftigungsverhältnis bestehende Abhängigkeit zu berücksichtigen. Zwar bestehen hiernach keine grundsätzlichen Bedenken gegenüber der Einwilligungsmöglichkeit im Arbeitsverhältnis.[2] Der Gesetzgeber geht im Gegenteil davon aus, dass Freiwilligkeit insbesondere dann vorliegen kann, wenn der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt (§ 26 Abs. 2 S. 2 Alt. 1 BDSG).[3] Ein Vorteil soll etwa darin zu sehen sein, dass dem Beschäftigten die Privatnutzung betrieblicher IT-Systeme erlaubt ist.[4] Jedoch ist ein Vorteil, der die Freiwilligkeit einer Einwilligung in Kontrollmaßnahmen des Arbeitgebers nahelegt, regelmäßig nicht zu verzeichnen.[5] Das Gegenteil dürfte richtig sein: Eine Einwilligung in Kontrollmaßnahmen des Arbeitgebers legt die Abhängigkeit des Arbeitnehmers frei.[6]

2. Erforderlichkeit

Kontrollmaßnahmen können indes nach § 26 BDSG gerechtfertigt sein. Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses u.a. verarbeitet werden, wenn dies für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist (§ 26 Abs. 1 S. 1 BDSG). Demgegenüber dürfen personenbezogene Daten zur Aufdeckung von Straftaten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt (§ 26 Abs. 1 S. 2 BDSG).

a) Repressive Kontrollmaßnahmen

Grundvoraussetzung repressiver Kontrollmaßnahmen ist das Bestehen eines „einfachen" Verdachts einer im Beschäftigungsverhältnis begangenen Straftat oder schwerwiegenden Pflichtverletzung („Anfangsverdacht").[7] Der Anfangsverdacht muss durch konkrete Tatsachen belegt sein.[8] Vage Anhaltspunkte oder bloße Mutmaßungen reichen nicht aus.[9] So genügt es bspw. nicht, wenn der Arbeitnehmer bei einmaligem Antreffen eine stark bebilderte Website hastig wegklickt.[10] Ebenso wenig reicht es aus, wenn der Arbeitgeber beim Arbeitnehmer bloß einen Umsatzrückgang verzeichnet.[11] Ein „dringender" Tatverdacht, der einen „hohen"[12] Wahrscheinlichkeitsgrad für die Begehung einer Straftat voraussetzt, ist dagegen weder nach dem Wortlaut noch nach Sinn und Zweck der Regelung erforderlich.[13] Nach Maßgabe der vom BAG in Bezug genommenen[14] Rechtsprechung des BGH[15] muss der „einfache" Tatverdacht ebenso wenig ein hinreichender sein. Die Eintrittsschwelle des § 26 Abs. 1 S. 2 BDSG erfordert mithin nicht, dass die Begehung einer Straftat

1 BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1329, Rn. 21.
2 Vgl. BAG, 19.2.2015 – 8 AZR 1011/13, AP BGB § 611 Persönlichkeitsrecht Nr. 43, Rn. 30.
3 *Wybitul*, NZA 2017, 413, 416 f.
4 BT-Drs. 18/11325, 97.
5 Ebenso *Ströbel u.a.*, CCZ 2018, 14, 16 (dort zu Compliance-Ermittlungen); ähnlich die Wertung der Artikel 29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, S. 7 f. Das BAG hat sich zu dem Aspekt der Freiwilligkeit einer Einwilligung in umfassende Überwachungsmaßnahmen bislang nicht verhalten. Es stellte lediglich fest, dass in dem Umstand, dass der Arbeitnehmer der angekündigten Verwendung eines *Keylogger* nicht entgegengetreten sei, keine Einverständniserklärung erblickt werden könne (BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1331, Rn. 35).
6 *Tinnefeld/Conrad*, ZD 2018, 391, 396; eine Einwilligung in eine „Totalüberwachung" generell ablehnend *Götz*, Big Data im Personalmanagement, 2020, S. 108 f.; ähnlich *Gola*, BB 2017, 1462, 1468.
7 BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1330, Rn. 29 f.
8 Vgl. BAG, 31.1.2019 – 2 AZR 426/18, K&R 2020, 466, NZA 2019, 893, 899, Rn. 54.
9 *Maschmann*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, BDSG, § 26, Rn. 59; *Kort*, NZA 2018, 1097, 1099.
10 Vgl. BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1331, Rn. 35.
11 LAG Berlin-Brandenburg, 11.9.2020 – 9 Sa 584/20, juris, Rn. 73.
12 Dagegen BAG, 29.11.2007 – 2 AZR 724/06, BB 2008, 721 red. Ls, BeckRS 2008, 51136, Rn. 9: „große" Wahrscheinlichkeit.
13 Vgl. BAG, 20.10.2016 – 2 AZR 395/15, BB 2017, 691 red. Ls, NZA 2017, 443, 446, Rn. 25.
14 BAG, 20.10.2016 – 2 AZR 395/15, BB 2017, 691 red. Ls, NZA 2017, 443, 446, Rn. 25.
15 BGH, 11.8.2016 – StB 12/16, BeckRS 2016, 15673, Rn. 9.

durch den Arbeitnehmer bei vorläufiger Bewertung der Tatsachen wahrscheinlich ist.[16] Je intensiver die Überwachungsmaßnahme in das Persönlichkeitsrecht des Arbeitnehmers eindringt, desto gewichtiger muss allerdings auch der Tatverdacht sein. So kann bei Abwägung zwischen Aufklärungsinteresse und Persönlichkeitsbeeinträchtigung im Ergebnis eine höhere Dringlichkeit des Tatverdachts vonnöten sein.[17]

b) Präventive Kontrollmaßnahmen

Digitale Kontrollanwendungen gegenüber im *Home-Office* Beschäftigten sollen meist jedoch ohne konkreten Tatverdacht implementiert werden. Solche präventiven Kontrollmaßnahmen sind an § 26 Abs. 1 S. 1 BDSG auszurichten. Zur Durchführung des Beschäftigungsverhältnisses gehört es, dass der Arbeitgeber kontrolliert, ob der Arbeitnehmer seinen Pflichten nachkommt.[18] Erlaubt sind Kontrollmaßnahmen freilich nur dann, wenn sie erforderlich sind. Nach der Gesetzesbegründung[19] sind dabei die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwiegen, um die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen.[20] Es dürfen keine anderen gleich wirksamen, das Persönlichkeitsrecht weniger einschränkenden Mittel zur Verfügung stehen. Die Schwere des Eingriffs darf ferner nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen.[21] Eine Datenverarbeitung, die eine übermäßige Belastung für den Arbeitnehmer darstellt, ist daher unzulässig.[22] Hiervon ist etwa auszugehen, wenn eine nahezu lückenlose, dauerhafte sowie sehr detaillierte Erfassung des Arbeitnehmerverhaltens stattfindet, ohne dass ein Anfangsverdacht besteht.[23]

aa) Screenshot Monitoring

Zu einer lückenlosen Erfassung des Arbeitnehmerverhaltens kommt es dann nicht, wenn der Arbeitgeber anhand digitaler Anwendungen bloß stichprobenartig *Screenshots* vom Monitor anfertigen lässt. Demgemäß hat auch das BAG anerkannt, dass die vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers anlasslos zulässig sein könne, um die Einhaltung eines Verbots der Privatnutzung betrieblicher IT-Systeme zu kontrollieren.[24] Hierbei werden die Adressen und Titel der aufgerufenen Seiten und der Zeitpunkt des Aufrufs protokolliert, was mit Blick auf das Kontrollinteresse des Arbeitgebers keine übermäßige Belastung des Arbeitnehmers darstellen solle.

Die Anfertigung von Screenshots geht hierüber hinaus. Die visuelle Erfassung speichert mehr Daten, als für die Identifikation eines möglichen Missbrauchs eingeräumter Nutzungsrechte erforderlich ist.[25] Andererseits stellt die Anfertigung von Screenshots dem Wesen nach nichts anderes dar, als würde der Arbeitgeber dem Beschäftigten im Betrieb bei Gelegenheit „über die Schulter schauen". Der Vergleich gelingt freilich nur dann, wenn die Anfertigung der Screenshots nur stichprobenartig erfolgt und keinen Arbeitnehmer besonders unter Verdacht stellt.[26] Ob die Anfertigung bloß stichprobenartiger Natur ist, bemisst sich allen voran nach dem Intervall zwischen zwei Screenshots. Einzelne Anbieter werben mit einer Frequenz von 30 Screenshots pro Stunde.[27] Dem analogen „Blick über die Schulter" entspricht es jedoch eher, wenn sich das *Screenshot Monitoring* auf die Anfertigung von drei Screenshots pro Arbeitstag beschränkt.[28] Dass die angefertigten Screenshots – anders als der „Blick über die Schulter" – überdies vorübergehend elektronisch gespeichert werden, dürfte bei Abwägung der betroffenen Interessen indes hinzunehmen sein, könnten etwaige Zuwiderhandlungen gegen Regelungen der Privatnutzung betrieblicher IT-Systeme andernfalls nicht identifiziert werden.[29]

bb) Detektiveinsatz

Anders ist zu entscheiden, wollte der Arbeitgeber der Informationsasymmetrie im Home-Office durch Einsatz von Privatermittlern begegnen. Nach der Rechtsprechung des BAG ist die Einschaltung von Detektiven an das Vorliegen eines Anfangsverdachts einer Straftat oder einer schwerwiegenden Pflichtverletzung des Arbeitnehmers gebunden.[30] Es genügt nicht, dass der Verdacht durch Hinzuziehung des Detektivs erst begründet wird.[31] Ein präventives Kontrollinteresse gegenüber im Home-Office Beschäftigten oder bloß Zweifel daran, ob der Arbeitnehmer im Home-Office weiterhin so gut wie möglich arbeitet, reichen daher nicht aus.[32] Ein Anfangsverdacht könnte sich etwa dadurch einstellen, dass der Arbeitgeber Kenntnis von einer E-Mail eines Wettbewerbers erhält, in der als dessen Dienstleistung die (unzulässige) Konkurrenztätigkeit seines Arbeitnehmers angepriesen wird.[33]

Es könnte im Einzelfall allerdings zweifelhaft sein, ob der Detektiveinsatz ein geeignetes Mittel darstellt, den Anfangsverdacht gegenüber Arbeitnehmern im Home-Office zu verifizieren. Verlässt der Arbeitnehmer während der Arbeitszeit nicht seine Wohnung, dürfte es dem Detektiv häufig an den notwendigen Einsichtsmöglichkeiten fehlen, um zu ermessen, was der Arbeitnehmer im Home-Office tatsächlich treibt. Der Arbeitgeber könnte deshalb daran denken, das Screenshot Monitoring zu intensivieren und nunmehr als repressive Kontrollmaßnahme zu verwenden.

cc) Keylogger-Einsatz

Deutlich weiter als das Screenshot Monitoring gehen *Keylogger-Anwendungen*. Ein Keylogger zeichnet alle Tastatureingaben an einem Computer auf und verschafft damit dem Arbeitgeber einen Überblick über sämtliche Bildschirmaktivitäten seines Arbeitnehmers. Aus der elektronischen Protokollierung sämtlicher digitaler Bewegungen ergibt sich so ein detaillierter Tätigkeitsnachweis.[34] Das BAG erkennt daher in dem heimlichen Keylogger-Einsatz einen seiner Intensität nach vergleichbaren Eingriff in das Persönlichkeitsrecht wie bei einer verdeckten Videoüberwachung des Arbeitnehmers.[35] Eine Anwen-

16 Vgl. BGH, 29.11.2018 – StB 34/18, NJW 2019, 2108, 2109, Rn. 16.
17 Vgl. *Franzen*, in: ErfK, 2021, BDSG, § 26, Rn. 39.
18 BAG, 31.1.2019 – 2 AZR 426/18, K&R 2020, 466, NZA 2019, 893, 898, Rn. 50.
19 BT-Drs. 18/11325, 97.
20 Vgl. BAG, 9.4.2019 – 1 ABR 51/17, BB 2019, 2810, NZA 2019, 1055, 1059, Rn. 39.
21 BAG, 29.6.2017 – 2 AZR 597/16, BB 2017, 2364, NZA 2017, 1179, 1183, Rn. 32.
22 BAG, 31.1.2019 – 2 AZR 426/18, K&R 2020, 466, NZA 2019, 893, 898, Rn. 51.
23 BAG, 28.3.2019 – 8 AZR 421/17, BB 2019, 2035 Ls, NZA 2019, 1212, 1216, Rn. 39.
24 BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1330 f., Rn. 31.
25 Vgl. *Chandna-Hoppe*, NZA 2018, 614, 617.
26 Vgl. *Stück*, ArbRAktuell 2019, 216, 217 m. w. N.; entgegen *Günther/Böglmüller*, ArbRAktuell 2020, 186, 188: nur bei Tatverdacht.
27 Vgl. etwa https://screenshotmonitor.com/tour (Abruf: 8.1.2021).
28 Gegen derart „regelmäßig" angefertigte Screenshots wohl *Suwelack*, ZD 2020, 561, 565 (dort aber im Zusammenhang mit dem Keylogger-Einsatz).
29 Vgl. BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1331, Rn. 31.
30 BAG, 29.6.2017 – 2 AZR 597/16, BB 2017, 2364, NZA 2017, 1179, 1182, Rn. 30.
31 *Thüsing/Rombey*, NZA, 2018, 1105, 1107.
32 LAG Berlin-Brandenburg, 11.9.2020 – 9 Sa 584/20, juris, Rn. 73; ebenso *Byers*, NZA 2017, 1086, 1087.
33 Vgl. BAG, 29.6.2017 – 2 AZR 597/16, BB 2017, 2364, NZA 2017, 1179, 1184, Rn. 40.
34 Vgl. etwa https://www.protectcom.de/homeoffice-kontrolle/ (Abruf: 8.1.2021).
35 BAG, 27.7.2017 – 2 AZR 681/16, BB 2017, 2682, NZA 2017, 1327, 1331, Rn. 33.

dung, die irreversibel alle Eingaben einschließlich des Zeitpunkts der Eingabe sowie des zeitlichen Abstands zwischen zwei Eingaben erfasst und dadurch ein nahezu umfassendes und lückenloses Nutzungsprofil zeichnet, ist nach herrschender Meinung demgemäß nur bei einem Anfangsverdacht einer Straftat oder schwerwiegenden Pflichtverletzung zulässig.[36] Ein solcher Anfangsverdacht kann sich etwa aus der vorherigen stichprobenartigen Anfertigung von Screenshots ergeben. Es ist jedoch zweifelhaft, eine identische Eingriffsschwelle für den Einsatz eines Detektivs und für die Verwendung eines Keylogger zu formulieren. Die Eingriffstiefe des Keylogger-Einsatzes geht deutlich über den Grad der Beeinträchtigung eines Detektiveinsatzes hinaus. Eine vollständige Protokollierung sämtlicher Bildschirmaktivitäten unter Dokumentation aller Tastaturanschläge wird man daher nur bei einem hinreichenden Verdacht einer Straftat oder schwerwiegenden Pflichtverletzung anzunehmen haben. Ein bloß präventiver Keylogger-Einsatz scheidet dagegen in jedem Fall aus.

dd) Time Tracking-Anwendungen

Von besonderem Interesse für die Ausgestaltung von Home-Office-Arbeitsplätzen erweisen sich ferner sog. *Time Tracking-Anwendungen*. Diese erlauben es Arbeitgebern, produktive und unproduktive Zeiten im Detail zu erfassen.[37] Anhand der so protokollierten Zeiten können Arbeitgeber bspw. einsehen, wie Arbeitnehmer ihre Arbeitszeit konkret nutzen, zu welchen Zeitpunkten sie sich an- und abmelden und wie viel Arbeitszeit sie für die Erledigung bestimmter Arbeitsaufgaben benötigen.

Die Relevanz von Time Tracking-Anwendungen rührt nicht zuletzt von der europarechtlichen Pflicht zur Erfassung der Arbeitszeit.[38] Die Pflicht wird mit Blick auf die Tätigkeit von im Home-Office Beschäftigten zum Teil dahingehend präzisiert, dass deren Zeiterfassung nicht durch einen händisch auszufüllenden Stundenzettel erfolgen dürfe.[39] Die Selbsterfassung stelle gerade keine „objektive" und „verlässliche" Zeiterfassungsmethode dar.[40] Vielmehr müsse der Login in das betriebliche System ebenso elektronisch protokolliert werden wie etwa das Lesen und Beantworten von E-Mails. Dem wird entgegengehalten, dass aus dem Gebot der Arbeitszeiterfassung keine Pflicht zur *automatisierten* Erfassung folge.[41] Im Übrigen würde die Erfassung reiner Bildschirmarbeiten den Umstand übergehen, dass viele Tätigkeiten auch im Home-Office „offline" erfolgen und nicht elektronisch erfasst und automatisiert protokolliert werden können.[42]

Beschränkt sich das Time Tracking auf die Aufzeichnung der An- und Abmeldezeiten in das betriebliche IT-System, ist dies unter datenschutzrechtlichen Aspekten gleichwohl nicht zu beanstanden.[43] Der Arbeitgeber hat ein berechtigtes Interesse an einer verlässlichen Feststellung der Arbeitszeiten. Die digitale Protokollierung des Login geht dabei nicht weiter als analoge Erfassungsmethoden, wie etwa der Einsatz von Stempeluhren.[44]

Ermittelt das Time Tracking jedoch darüber hinaus, wie lange Beschäftigte für die Erledigung bestimmter Aufgaben benötigen, ist zu differenzieren: Sollen Bearbeitungszeiten lediglich stichprobenartig protokolliert werden, dürfte das Interesse des Arbeitgebers an einer effektiven Gestaltung der Arbeitsabläufe das Interesse des Arbeitnehmers überwiegen. Anders ist zu entscheiden, wenn das Time Tracking mit einer dauerhaften, nahezu lückenlosen Erfassung einzelner Arbeitsschritte verbunden ist.[45] In diesem Fall führt das Time Tracking zu einer dezidierten Leistungs- und Verhaltenskontrolle, wodurch es in seiner Anwendung und seiner Intensität nach mit einem Keylogger vergleichbar wird.[46] Entsprechend ist die dauerhafte und lückenlose Dokumentation aktiver Bildschirmarbeitszeiten vorbehaltlich eines hinreichenden Tatverdachts unzulässig.[47]

II. Informationspflichten

1. Ausschluss verdeckter Kontrollmaßnahmen?

Ungeachtet des Kontrollinstruments wird der Arbeitgeber regelmäßig daran interessiert sein, Kontrollen ohne Kenntnis des Arbeitnehmers durchzuführen. Andernfalls könnte die Kontrollmaßnahme ihren Sinn und Zweck verfehlen, würde sich der Arbeitnehmer auf diese einstellen und ein vertragsgemäßes Verhalten an den Tag legen können.

Das Ansinnen des Arbeitgebers steht in einem Spannungsfeld zu Art. 5 Abs. 1 lit. a) Var. 3 DSGVO. Danach müssen personenbezogene Daten in einer für den Betroffenen nachvollziehbaren Weise verarbeitet werden. Der Transparenzgrundsatz wird durch Art. 13 und Art. 14 DSGVO konkretisiert. Danach hat der Arbeitgeber den Arbeitnehmer u. a. über die Zwecke zu informieren, für die seine personenbezogenen Daten verarbeitet werden sollen (Art. 13 Abs. 1 lit. c) DSGVO). Die Information ist dem Arbeitnehmer zum Zeitpunkt der Erhebung seiner Daten mitzuteilen. Muss der Arbeitnehmer indes bereits bei Vornahme der Kontrollmaßnahme hierüber in Kenntnis gesetzt werden, ist ein heimliches Vorgehen de facto ausgeschlossen,[48] und eine gleichwohl heimlich vorgenommene Kontrolle bußgeldbewehrt (Art. 83 Abs. 5 lit. b) DSGVO).

2. Ausnahmeregelung § 32 Abs. 1 Nr. 4 BDSG

Die Informationspflichten gelten indes nicht, sofern die Mitgliedstaaten ihre Anwendbarkeit beschränkt haben (Art. 23 Abs. 1 DSGVO). Der deutsche Gesetzgeber hat von dieser Ermächtigung durch Erlass von §§ 32 f. BDSG Gebrauch gemacht. Gemäß § 32 Abs. 1 Nr. 4 BDSG besteht eine Pflicht zur Information nach Art. 13 Abs. 3 DSGVO dann nicht, wenn die Informationserteilung die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde. Diese Beschränkung gilt ausweislich des Bezugs auf

36 *Fuhlrott*, NZA 2017, 1308, 1309; *Däubler*, NZA 2017, 1481, 1486; *Stück*, CCZ 2018, 88, 89; a. A. *Kort*, RdA 2018, 24, 25: generell unzulässig; *ders.*, NZA 2018, 1097, 1100; ähnlich *Tiedemann*, in: Kramer, IT-Arbeitsrecht, 2. Aufl. 2019, B, Rn. 570.
37 Vgl. https://www.interguardsoftware.com/remote-employee-monitoring/ (Abruf: 8.1.2021).
38 EuGH, 14.5.2019 – C-55/18 – CCOO/Deutsche Bank SAE, BB 2019, 1978, NZA 2019, 683, 686, Rn. 60.
39 *Ulber*, NZA 2019, 677, 678.
40 Vgl. hierzu auch *Latzel*, EuZA 2019, 469, 479.
41 *Bayreuther*, NZA 2020, 1, 6.
42 *Bayreuther*, EuZW 2019, 446, 448 f.; *Reinhard*, NZA 2019, 1313, 1315.
43 Vgl. aber *Reinhard*, NZA 2019, 1313, 1315: „bereits als nicht unerhebliche Überwachung einzustufen".
44 Ebenso *von Steinau-Steinrück/Burmann*, NJW-Spezial 2018, 754, 755; *Suwelack*, ZD 2020, 561, 565.
45 Vgl. BAG, 25.4.2017 – 1 ABR 46/15, BB 2017, 2428, NZA 2017, 1205, 1212, Rn. 36 f.
46 Vgl. *Bayreuther*, NZA 2020, 1, 6: „schlicht unzulässig"; *Reinhard*, NZA 2019, 1313, 1315.
47 Vgl. *Byers*, Mitarbeiterkontrollen, 2017, Rn. 116: „regelmäßig unzulässig"; a. A. wohl *Krause*, Forschungsbericht 482: Digitalisierung und Beschäftigtendatenschutz, April 2017, S. 32: Ausnahme „zweifelhaft"; *Günther/Böglmüller*, in: Arnold/Günther, Arbeitsrecht 4.0, 2018, Kap. 4, Rn. 94: nur mit Einwilligung.
48 So *Maschmann*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, BDSG, § 26, Rn. 22; *ders.*, NZA-Beilage 2018, 115, 121; *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO, Art. 5, Rn. 18; auch *Roßnagel*, NJW 2019, 1, 5.

Art. 13 Abs. 3 DSGVO jedoch nur für den besonderen Fall der Verarbeitung von Daten zu einem anderen Zweck als ursprünglich vorgesehen.[49] Nach ausdrücklicher Klarstellung des Gesetzgebers bezieht sich die Beschränkung hingegen nicht auf die Informationspflicht nach Art. 13 Abs. 1 DSGVO.[50]

Ebenso wenig kann ein heimliches Vorgehen auf § 26 Abs. 1 BDSG gestützt werden.[51] Die Regelung nimmt keine Beschränkung i. S. d. Art. 23 Abs. 1 DSGVO vor.[52] Insbesondere ergibt sich aus ihrem Wortlaut nicht, dass Überwachungsmaßnahmen – entgegen Art. 13 Abs. 1 DSGVO – auch verdeckt erfolgen können.[53] § 26 Abs. 5 BDSG bringt im Gegenteil zum Ausdruck, dass der Arbeitgeber bei Verarbeitung von Beschäftigtendaten den Grundsätzen des Art. 5 DSGVO, einschließlich des Transparenzgrundsatzes, vollumfänglich Rechnung zu tragen hat.

3. Zweckvereitelung (Art. 14 Abs. 5 lit. b) Hs. 2 Var. 5 und 6 DSGVO)

Eine Ausnahme von der Pflicht zur Information des Arbeitnehmers könnte ferner in Art. 14 Abs. 5 lit. b) Hs. 2 Var. 5 und 6 DSGVO erblickt werden.[54] Danach wird die Informationspflicht suspendiert, soweit diese voraussichtlich die Verwirklichung der mit der Datenverarbeitung verfolgten Ziele unmöglich macht oder ernsthaft beeinträchtigt.

Was auf den ersten Blick als verordnungsgeberische Anerkennung verdeckter Kontrollmaßnahmen erscheint, findet genau besehen nur dann Anwendung, wenn die Daten nicht „*bei*" dem Arbeitnehmer erhoben werden (Art. 14 Abs. 1 DSGVO). Nach teilweise vertretener Ansicht soll hiervon auszugehen sein, wenn der Betroffene für den Verantwortlichen erkennbar weder körperlich noch mental wissentlich an der Datenverarbeitung beteiligt sei.[55] So wären Konstellationen heimlicher Detektiveinsätze und verdeckt operierender Keylogger von Art. 14 DSGVO erfasst. Richtigerweise wird man Art. 14 DSGVO allerdings nur auf Fälle anwenden können, in denen der Verantwortliche die Daten von einer anderen Person als dem Betroffenen (z. B. einem anderen Verantwortlichen) oder aus öffentlichen Quellen bezieht.[56] Hierfür spricht der systematische Vergleich gegenüber Art. 13 DSGVO: Während Art. 13 DSGVO eine Information bereits zum Zeitpunkt der Datenerhebung verlangt, trägt Art. 14 Abs. 3 lit. a) DSGVO den spezifischen Umständen der Fremderhebung insofern Rechnung, als die Information (bloß) innerhalb einer angemessenen Frist nach Erlangung der Daten zu erteilen ist. Ist es dem Verantwortlichen hingegen möglich, den Betroffenen direkt zu kontaktieren und ihm die Informationen zu erteilen, bedarf es dieser Rücksicht nicht.[57] Stellt der Arbeitnehmer die unmittelbare Datenquelle dar, ist von einer Informationspflicht nach Art. 13 Abs. 1 DSGVO auszugehen.

Anders soll zu entscheiden sein, wenn die Daten „*beim*" Arbeitnehmer etwa durch einen Detektiv erhoben werden.[58] Übermittle der Detektiv seine Erkenntnisse in einem weiteren Verarbeitungsschritt an den Arbeitgeber, könne dieser sich *insofern* auf die Privilegierung nach Art. 14 Abs. 5 lit. b) Hs. 2 Var. 5 und 6 DSGVO berufen – die Daten würden aus seiner Sicht nicht „beim" Betroffenen erhoben.[59] Das würde allerdings voraussetzen, dass der Arbeitgeber bei der Datenerhebung durch den Detektiv nicht selbst als Verantwortlicher anzusehen wäre. Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Danach ist der Arbeitgeber derjenige, der jedenfalls über den Zweck der Überwachung (Überprüfung seines Anfangsverdachts) und eingeschränkt auch über die Mittel der Überwachung (Erforderlichkeit) entscheidet. Die Datenerhebung „*beim*" Arbeitnehmer durch den Detektiv ist dem Arbeitgeber folglich zurechnen. Der Arbeitgeber kann sich nicht auf eine Privilegierung nach Art. 14 Abs. 5 lit. b) Hs. 2 Var. 5 und 6 DSGVO berufen, er ist nach Art. 13 DSGVO zur Offenlegung verpflichtet. Auch eine analoge Anwendung von Art. 14 Abs. 5 lit. b) Hs. 2 Var. 5 und 6 DSGVO kommt wegen fehlender planwidriger Regelungslücke nicht in Betracht.[60]

4. Informationspflicht „zum Zeitpunkt" der Datenerhebung

Der Arbeitgeber wird den Beschäftigten daher bereits zum Zeitpunkt der Datenerhebung über diese in Kenntnis setzen müssen (Art. 13 Abs. 1 DSGVO). Das schließt ein heimliches Vorgehen zwar aus. Der Kontrollzweck wird gleichwohl nicht zwingend gefährdet. Die Information des Arbeitnehmers muss *nur* „zum Zeitpunkt" der Datenerhebung, nicht aber – etwa unter Einhaltung einer bestimmten Frist – *vor* dieser erfolgen.[61] Das bedeutet, dass der Beschäftigte, wie die englische Sprachfassung bekräftigt („*at the time when personal data are obtained*"), spätestens gleichzeitig mit der Datenerhebung über diese zu informieren ist.[62] Die stichprobenartige Anfertigung von Screenshots kann demnach ohne eine den Zweck der Kontrollmaßnahme gefährdende Vorabinformation erfolgen. So ist der Arbeitnehmer bloß gleichzeitig mit Anfertigung des Screenshots hierüber zu informieren – etwa durch Versand einer E-Mail oder Schaltung eines Informationsfensters im Desktop. Nichts anderes gilt bei repressiven Kontrollmaßnahmen.

III. Fazit

Ganz im Sinne von „*Vertrauen ist gut, Kontrolle ist besser*" verlangt die Beschäftigung von Arbeitnehmern im Home-Office ein hohes Vertrauen des Arbeitgebers und entsprechende Kontrollmöglichkeiten gegenüber den Arbeitnehmern. Dabei ist der Rückgriff auf digitale Kontrollinstrumente nur in begrenztem Maße zulässig. Als Einstiegsmaßnahme könnte sich die stichprobenartige Anfertigung von Screenshots durch den Arbeitgeber als digitaler „*Blick über die Schulter*" des Arbeitnehmers etablieren. Ebenso ist der Arbeitgeber berechtigt, die An- und Abmeldezeiten in das be-

49 Ebenso *Byers/Wenzel*, BB 2017, 2036, 2039.
50 BT-Drs. 18/11325, 102.
51 So aber *Kort*, RdA 2018, 24, 27.
52 *Byers/Wenzel*, BB 2017, 2036, 2039.
53 *Byers*, NZA 2017, 1086, 1089.
54 Hierfür *Fuhlrott/Oltmanns*, NZA 2019, 1105, 1110.
55 S. nur *Schmidt-Wudy*, in: BeckOK DatenschutzR, 34. Ed., Stand: 1.11.2020, DS-GVO, Art. 14, Rn. 31.
56 *Knyrim*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, DS-GVO, Art. 14, Rn. 2; *Mester*, in: Taeger/Gabel, 3. Aufl. 2019, DS-GVO, Art. 14, Rn. 5.
57 *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO, Art. 13, Rn. 13.
58 *Byers*, NZA 2017, 1086, 1088.
59 Stattdessen für einen Rückgriff auf die vergleichbare Ausnahmevorschrift des § 33 Abs. 1 Nr. 2 lit. a) BDSG *Thüsing/Rombey*, NZA 2018, 1105, 1110.
60 S. nur *Schmidt-Wudy*, in: BeckOK DatenschutzR, 34. Ed., Stand: 1.11.2020, DS-GVO, Art. 13, Rn. 95; entgegen *Byers*, NZA 2017, 1086, 1090; dem folgend *Bach*, EuZW 2020, 175, 178.
61 Vgl. *Schmidt-Wudy*, in: BeckOK DatenschutzR, 34. Ed., Stand: 1.11.2020, DS-GVO, Art. 13, Rn. 79; *Walter*, DSRITB 2016, 367, 374; a. A. *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO, Art. 13, Rn. 56.
62 *Knyrim*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, DS-GVO, Art. 13, Rn. 11.

triebliche IT-System elektronisch aufzuzeichnen. Besteht (danach) der Anfangsverdacht einer Straftat oder schwerwiegenden Pflichtverletzung ist der Arbeitgeber darüber hinaus berechtigt, sich eines Detektivs zu bedienen oder das Screenshot Monitoring zu intensivieren. Die Nutzung einer Keylogger-Software ist ihm mit Blick auf die hiermit verbundene Eingriffstiefe dagegen erst bei einem hinreichenden Tatverdacht gestattet. Zwar ist dem Arbeitgeber bei all dem ein verdecktes Vorgehen *de lege lata* untersagt. Es genügt jedoch, dass der Arbeitgeber erst mit der Datenerhebung informiert und der Arbeitnehmer die Kontrollmaßnahme dadurch nicht mehr vereiteln kann.

Dr. Justus Frank, LL.M., Maître en droit, ist Rechtsanwalt bei Hogan Lovells International LLP in Düsseldorf. Er berät nationale und internationale Mandanten zu allen Fragen des individuellen und kollektiven Arbeitsrechts.

Dipl.-Jur. Maurice Heine ist wissenschaftlicher Mitarbeiter bei Hogan Lovells International LLP in Düsseldorf und Doktorand an der Leibniz Universität Hannover.