

3. Straftatbestände

- 159 Nach § 42 Abs. 1 BDSG kann der gewerbsmäßige Datenhandel mit Freiheitsstrafe von bis zu drei Jahren oder mit Geldbuße bestraft werden, wenn der Täter **wissentlich ohne Berechtigung** handelt¹. Verarbeitet jemand nicht allgemeinzugängliche Daten ohne Berechtigung gegen Entgelt oder mit Bereicherungsabsicht, wird er mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn ihm wenigstens **Eventualvorsatz** zur Last fällt². Ob der Täter datenschutzrechtlich Verantwortlich iSd des Art. 4 Nr. 7 DSGVO ist, spielt tatbestandlich keine Rolle³. Es handelt sich in beiden Fällen um absolute Antragsdelikt (§ 42 Abs. 3 BDSG). Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Bundesbeauftragte sowie die Aufsichtsbehörde innerhalb von drei Monaten ab Kenntnismahme von Tat und Täter (§ 77b StPO).

4. Sonstige Aufsichtsbefugnisse nach Art. 58 DSGVO

- 160 Die Aufsichtsbehörden genießen umfangreiche Befugnisse zur **Sachaufklärung**. Sie können Verantwortliche, Auftragsverarbeiter und deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind (Art. 58 Abs. 1 lit. a DSGVO). Außerdem führen sie Untersuchungen in Form von Datenschutzüberprüfungen durch (Art. 58 Abs. 1 lit. b DSGVO). Dabei erhalten die Aufsichtsbehörden Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind (Art. 58 Abs. 1 lit. e DSGVO) sowie die Räumlichkeiten des Verantwortlichen und der Auftragsverarbeiter (Art. 58 Abs. 1 lit. f DSGVO).
- 161 Rechnen sie mit zukünftigen **Verstößen** durch einen Verantwortlichen, können sie ihn warnen (Art. 58 Abs. 2 lit. a DSGVO). Wurde ein Verstoß bereits begangen, kommt eine Verwarnung in Betracht (Art. 58 Abs. 2 lit. b DSGVO). Außerdem kann die Aufsichtsbehörde den Verantwortlichen durch Verwaltungsakt ggf. unter Fristsetzung anweisen, seine Datenverarbeitungstätigkeit in Einklang mit der DSGVO zu bringen (Art. 58 Abs. 2 lit. d DSGVO) sowie Beschränkungen und Verbote aussprechen (Art. 58 Abs. 2 lit. f und j DSGVO). Die Aufsichtsbehörde darf auch unmittelbar Interessen der betroffenen Person wahrnehmen. So kann sie den Verantwortlichen anweisen, die betroffene Person über eine Verletzung ihrer Daten zu informieren (Art. 58 Abs. 2 lit. e DSGVO), Anträgen der betroffenen Person insbesondere nach Art. 15 ff. DSGVO zu entsprechen (Art. 58 Abs. 2 lit. c). Die Ansprüche der betroffenen Person auf Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung (Art. 17 DSGVO) und Benachrichtigung über die Empfänger (Art. 19 DSGVO) kann die Aufsichtsbehörde zudem in eigenem Namen durch Verwaltungsakt ausüben (Art. 58 Abs. 2 lit. e DSGVO).

VI. Individualansprüche der Beschäftigten

- 162 Datenschutzverstöße sind mit einem Eingriff in das **allgemeine Persönlichkeitsrecht** verbunden, was bereits unter der herkömmlichen deutschen Rechtsordnung **Individualansprüche** der Beschäftigten zur Folge haben konnte⁴. Daneben sehen die Art. 15 ff. DSGVO einen Katalog besonderer Rechte der betroffenen Person vor, die seit dem 25.5.2018 im Vordergrund stehen.

Für Ansprüche in Bezug auf Daten, die zum Zwecke eines Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt wurden, ist selbst nach dessen Beendigung der Rechtsweg zu den Arbeitsgerichten eröffnet (§ 2 Abs. 1 Nr. 4 lit. a ArbGG)⁵.

1 Kühling/Buchner/Bergt, § 42 BDSG Rz. 25.

2 Kühling/Buchner/Bergt, § 42 BDSG Rz. 42.

3 Kühling/Buchner/Bergt, § 42 BDSG Rz. 3; aA BeckOK Datenschutzrecht/Brodowski/Nowak, § 42 BDSG Rz. 15 ff.

4 Zur unzulässigen Videoüberwachung Grimm/Schiefer, RdA 2009, 329 (343 f.).

5 BAG v. 3.2.2014 – 10 AZB 77/13, NZA 2014, 391.

1. Allgemeines zu Ansprüchen nach Art. 15 ff. DSGVO

Die Ansprüche nach Art. 15 ff. DSGVO beschränken sich gem. Art. 2 Abs. 1 DSGVO auf personenbezogene Daten, die automatisiert verarbeitet oder in Dateisystemen (dh. strukturiert geführten Sammlungen) gespeichert werden (vgl. Rz. 6); § 26 Abs. 2 BDSG findet keine Anwendung¹. Will der Arbeitnehmer diese Ansprüche mit Blick auf eine **Personalakte** geltend machen, muss er darlegen, dass sie automatisiert oder als strukturelles Aktengefüge geführt wird; letzteres hält das BAG nicht für selbstverständlich². 163

In der Praxis ist von herausgehobener Bedeutung, dass die Ansprüche nach Art. 15 ff. DSGVO nicht nur durch die betroffene Person selbst im Klagewege, sondern zusätzlich durch aufsichtsbehördliche Sanktionen, namentlich Bußgelder (Art. 83 Abs. 5 lit. b DSGVO) und Verwaltungsanordnungen (Art. 58 Abs. 2 lit. g DSGVO) durchgesetzt werden können. Damit es nicht zu einem Verstoß gegen die DSGVO kommt, muss das Unternehmen dem Begehren unverzüglich und jedenfalls innerhalb eines Monats nachkommen und selbst dann, wenn es nicht abhilft, zumindest über die Hintergründe informieren (Art. 12 Abs. 3 Satz 1 DSGVO). Diese **Frist** (zB zur Erfüllung eines Auskunftsanspruch nach Art. 15 DSGVO) kann **nur** dann um weitere **zwei Monate** verlängert werden, wenn dies unter Berücksichtigung der **Komplexität** und der **Anzahl** von Anträgen erforderlich ist und das Unternehmen die betroffene Person **innerhalb eines Monats** nach Eingang des Antrages unter Angabe von **Gründen** über die Fristverlängerung unterrichtet (Art. 12 Abs. 3 Satz 2 und 3 DSGVO). Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen (Art. 12 Abs. 4 DSGVO). 164

Die Kommunikation mit dem Betroffenen erfolgt schriftlich oder in anderer Form (Art. 12 Abs. 3 Satz 2 DSGVO) und in der Praxis meist per E-Mail. Bevor das Unternehmen allerdings Auskünfte per E-Mail erteilt, sollte es sich unbedingt zunächst der Identität des Anfragenden versichern. 165

Hinweis: Unternehmern sollten nachvollziehbare betriebliche Regelungen und Zuständigkeiten schaffen, um die Ansprüche nach Art. 15 ff. DSGVO jederzeit kurzfristig und ausreichend erfüllen zu können³. Wenn Arbeitnehmer ihre Ansprüche ausüben, empfiehlt es sich für Unternehmen, die Begehren ernst zu nehmen und die eigene Reaktion gründlich zu durchdenken. Nicht selten legen es die Anfragenden ohnehin auf einen Konflikt mit dem Unternehmen an und hoffen, dass ihnen eine mangelhafte Bearbeitung ihrer Anfragen dazu Anlass gibt. Wenn die Anfragenden die Reaktion des Unternehmens für unzureichend halten, können sie jederzeit Beschwerden bei der Aufsichtsbehörde erheben, ohne dabei ein Prozesskostenrisiko eingehen zu müssen (Art. 77 DSGVO). Die Aufsichtsbehörden sind dann verpflichtet, aktiv tätig zu werden und den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer über den Stand der Untersuchung zu unterrichten (Art. 57 Abs. 1 lit. f, Art. 77 Abs. 2 und Erwägungsgrund 141 DSGVO)⁴. Auf Beschwerden und eine sich anschließende Anhörung (§ 40 Abs. 4 BDSG) durch die Aufsichtsbehörde sollten Unternehmen bei ihrer Reaktion also vorbereitet sein. 166

Nur bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann das Unternehmen deren Behandlung verweigern oder vorab ein angemessenes Entgelt verlangen (Art. 12 Abs. 5 DSGVO). Das Unternehmen hat dann allerdings den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen, insbesondere wenn es zu einer Untersuchung der Aufsichtsbehörde kommt. Hier ist also Zurückhaltung geboten.

1 So unter der alten Rechtslage schon BAG v. 16.11.2010 – 9 AZR 573/09, NZA 2011, 453; aA *Riesenhuber*, NZA 2014, 753 (755).

2 BAG v. 16.11.2010 – 9 AZR 573/09, NZA 2011, 453; aA *Riesenhuber*, NZA 2014, 753 (754).

3 *Dzida*, BB 2018, 2677 (2679).

4 Paal/Pauly/Körffler, Art. 77 DSGVO Rz. 5.

2. Informationsrechte

a) Europarechtlicher Auskunftsanspruch

- 167 Die betroffene Person kann nach Art. 15 DSGVO Auskunft über die sie betreffenden verarbeiteten personenbezogenen Daten verlangen. Dieser Auskunftsanspruch gilt auch im Verhältnis Arbeitnehmer zum Arbeitgeber¹. Art. 15 Abs. 1 lit. a–h DSGVO enthält den umfangreichen Katalog der zu erteilenden Informationen.
- 168 Die Auskunft ist im ersten Schritt darauf gerichtet, ob der Verantwortliche überhaupt personenbezogene Daten der betroffenen Person verarbeitet (Art. 15 Abs. 1 Halbs. 1 DSGVO). Sollte der Auskunftsanspruch gerichtlich geltend gemacht werden, muss für weitergehende Auskünfte dargelegt werden, dass dies der Fall ist². Insoweit bietet sich also eine Stufenklage (§ 254 ZPO) an.
- 169 Maßgeblich für die **Frist** zur Erfüllung der Auskunftsverpflichtung ist Art. 12 Abs. 3 DSGVO. Danach ist die Auskunft unverzüglich, in jedem Fall innerhalb eines Monats zu erteilen. Eine Verlängerung um zwei weitere Monate ist zulässig, wenn dies im Hinblick auf die Komplexität und die Anzahl von Anträgen erforderlich ist³.
- 170 Verarbeitet der Verantwortliche personenbezogene Daten, hat die betroffene Person im zweiten Schritt Anspruch auf Information über Verarbeitungszwecke, verarbeitete Datenkategorien, Empfänger, Speicherdauer, Datenherkunft sowie ihre weitergehenden Rechte. Diese in Art. 15 Abs. 1 Halbs. 2 DSGVO genannten Auskunftsinhalte gehen nicht über die ohnehin bestehenden Informationspflichten nach Art. 13, 14 DSGVO hinaus, sondern bleiben hinter diesen sogar zurück⁴. Der Arbeitgeber kann den Auskunftsanspruch deshalb prinzipiell durch Vorlage seines allgemeinen datenschutzrechtlichen Informationsschreibens für Beschäftigte (dazu Rz. 30) erfüllen, das er allerdings ggf. aktualisieren oder ergänzen muss, soweit sich seit der Datenerhebung Veränderungen ergeben haben oder das Informationsschreiben Mängel aufweist⁵.
- 171 Bedeutender ist dagegen, dass der Arbeitgeber nach Art. 15 Abs. 3 Satz 1 DSGVO **Kopien der personenbezogenen Daten** zur Verfügung stellen muss, die Gegenstand der Verarbeitung sind. Bei wörtlichem Verständnis der Vorschrift wären jedwede personenbezogenen Daten zu der betroffenen Person erfasst, die innerhalb der Organisation des Verantwortlichen irgendwo iSd. Art. 2 Abs. 1 DSGVO automatisiert verarbeitet oder in Datensystemen gespeichert werden. Dieses Verständnis würde den Auskunftsanspruch allerdings ins Unzumutbare ausufern lassen. Streng genommen müsste der Arbeitgeber dann zB jede E-Mail mit dem Namen der betroffenen Person herausgeben, die sich bei irgendeinem Mitarbeiter des Unternehmens im dienstlichen E-Mail-Postfach befände. Deshalb kann der Arbeitgeber verlangen, dass der antragsstellende Beschäftigte präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich sein Auskunftersuchen konkret bezieht, bevor er dem Auskunftersuchen nachkommt (vgl. Erwägungsgrund 63 DSGVO)⁶.
- 172 Dies folgt analog § 275 Abs. 2 BGB aus dem auch europarechtlich anerkannten Grundsatz von Treu und Glauben⁷. Nimmt der Beschäftigte trotz Aufforderung keine Präzisierung vor, wird die Auskunftspflicht auf solche personenbezogenen Daten zu beschränken sein, welche für die Leitungsorganisation des Verantwortlichen unter vertretbarem Aufwand zentral zugänglich sind, dh. ohne dass sie dafür aufwendige interne Ermittlungen betreiben muss (also die insbesondere die Personalakte, die Akte der Lohnbuchhaltung und die Arbeitszeitaufzeichnungen).

1 *Dzida*, BB 2018, 2677 (2679).

2 LAG Hess. v. 29.1.2013 – 13 Sa 263/12, ZD 2013, 392 Rz. 103.

3 *Dzida*, BB 2018, 2677 (2679).

4 Kühling/Buchner/Bäcker, Art. 15 Rz. 10 DSGVO.

5 Kühling/Buchner/Bäcker, Art. 15 Rz. 15 DSGVO.

6 Bei Bewerberinnen dürfte das aber nicht der Fall sein, da der Arbeitgeber nur über eine überschaubare Menge an Informationen verfügt, *Dzida*, BB 2018, 2677 (2679).

7 *Gola/Franck*, Art. 15 DSGVO Rz. 38.

Die Auskunft kann verweigert werden, soweit hierdurch Rechte und Freiheiten anderer Personen (Art. 15 Abs. 4 DSGVO), Berufsgeheimnisse¹ oder ein sonstiges überwiegendes Geheimhaltungsbedürfnis (§ 29 Abs. 1 Satz 2 BDSG)² beeinträchtigt würde. 173

Schwierig ist die Erfüllung des Auskunftsanspruchs, wenn dieser geltend gemacht wird, um die Identität eines **Whistleblowers** zu erfahren, was ein zulässiges Auskunftziel ist³. Sinnvoll und von der Datenschutzkonferenz (DSK) empfohlen ist, hierüber den Whistleblower bei der ersten Kontaktaufnahme mit der Hotline zu informieren⁴. Das führt alldings oft zu dem – nicht gewünschten – Ergebnis, dass der Whistleblower entweder anonym bleibt, was kritisch gesehen wird, oder von der Meldung Abstand nimmt⁵. 174

Hinweis: Aus Arbeitnehmersicht sollten Auskunftsansprüche zu Beginn eines Konfliktes geltend gemacht werden, um Informationen zu gewinnen und Lästigkeitspotentiale zu schaffen⁶. Arbeitgeber sollten ein Konzept bzw. standardisiertes Verfahren entwickeln, wie Auskunftsansprüche erfüllt werden⁷. Mit Blick auf die recht kurzen Fristen ist auch eine zuständige Stelle zu definieren. 175

b) Einsichtsrecht

Nach § 83 Abs. 1 BetrVG und § 26 Abs. 2 SprAuG steht Arbeitnehmern und leitenden Angestellten das Recht zur **Einsichtnahme in die Personalakte**⁸ (vgl. Teil 2 A Rz. 780 ff., 785) zu⁹. Der Anspruch folgt auch aus § 241 Abs. 2 BGB¹⁰. Vom **Begriff** der Personalakte erfasst werden alle Unterlagen über den einzelnen Arbeitnehmer, die das Arbeitsverhältnis angehen und in innerem Zusammenhang stehen¹¹. Gestattet der Arbeitgeber, Kopien aus der Personalakte zu fertigen, ist es dem Arbeitnehmer **nicht** gestattet, einen **Rechtsanwalt** zur Einsichtnahme hinzuzuziehen¹². Das Einsichtsrecht in die Personalakte besteht auch **nach** Beendigung des Arbeitsverhältnisses¹³. 176

Die Anwendungsbereiche des Einsichtnahmerechts und des Auskunftsanspruchs nach Art. 15 DSGVO sind nicht identisch¹⁴. Das Einsichtsrecht hat keinen Ausnahmekatalog und bezieht sich auf Einsicht in die Originalakte, nicht bloß in Kopien. Der Auskunftsanspruch hingegen ist weiter, denn er erfasst auch sich nicht aus der Personalakte ergebende Informationen. Auch wenn ein konkretes Interesse an der Einsichtnahme nicht mehr notwendig ist¹⁵, darf der Anspruch nicht in unangemessen kurzen Zeitabständen geltend gemacht werden¹⁶. 177

1 Gola/Franck, Art. 15 DSGVO Rz. 36, 37.

2 § 29 Abs. 1 Satz 2 BDSG wird teilweise für europarechtswidrig und unanwendbar gehalten, so Gola/Franck, Art. 15 DSGVO Rz. 48.

3 Dzida, BB 2018, 2677 (2680).

4 DSK: Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz (Stand: 14.11.2018), S. 9.

5 So prägnant Dzida, BB 2018, 2677 (2680).

6 Jacobi/Jantz, ArbRB 2017, 22.

7 So auch Dzida, BB 2018, 2677 (2679).

8 Zu den Arbeitnehmerrechten in Bezug auf die Personalakte Müller, DB 2011, 2604.

9 Vergleichbare Rechte enthalten § 110 Abs. 1 BBG und § 3 Abs. 5 Satz 1 TVöD.

10 GK-BetrVG/Franzen, vor § 81 Rz. 13 ff.

11 BAG v. 7.5.1980 – 4 AZR 214/78, ArbuR 1981, 124 Ls. 1; Fitting, § 83 BetrVG Rz. 3; WPK/Preis, § 83 BetrVG Rz. 3 mwN.

12 BAG v. 12.7.2016 – 9 AZR 791/14, NZA 2016, 1344 (1345). Ob das allgemein gilt, hat das BAG offengelassen.

13 BAG v. 16.11.2010 – 9 AZR 573/09, NZA 2011, 453; exemplarisch für die Abmahnung Kleinebrink, DB 2012, 1508 (1511 f.).

14 Ausführlich MünchArbR/Reichold, § 96 Rz. 74.

15 BAG v. 16.11.2010 – 9 AZR 573/09, NZA 2011, 453.

16 Müller, DB 2011, 2604 (2407).

3. Berichtigung, Löschung, Widerspruch und Sperrung

a) Europarechtliche Ansprüche

- 178 Nach Art. 16 DSGVO haben Beschäftigte einen Anspruch gegen den Arbeitgeber, dass dieser **unrichtig gespeicherte Daten berichtigt**. Zudem sind unrichtige Daten nach Art. 5 Abs. 1 lit. d DSGVO autonom – also ohne Aufforderung des Betroffenen – zu korrigieren oder zu löschen¹. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person zudem das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. Dabei kann nicht jede beliebige Vervollständigung des Datensatzes verlangt werden, sondern nur diejenigen Informationen sind zu ergänzen, die im Hinblick auf den Verarbeitungszweck notwendig sind, um ein zutreffendes Bild der betroffenen Person zu zeichnen².
- 179 Nach Art. 17 DSGVO kann die betroffene Person die **Löschung** der zu ihr gespeicherten personenbezogenen Daten verlangen, sofern die Speicherung der Daten nicht durch ihre Verarbeitung (Art. 17 Abs. 1 DSGVO) oder aus anderen Gründen (Art. 17 Abs. 3 DSGVO) gerechtfertigt ist. Der Löschantrag der betroffenen Person reicht allerdings nicht weiter, als die ohnehin bestehende Pflicht der Verantwortlichen, solche personenbezogenen Daten von sich aus zu löschen (dazu Rz. 34 ff.)³. Die betroffene Person kann hiervon abweichend die Löschung von eigentlich löschpflichtigen personenbezogenen Daten ablehnen und lediglich verlangen, dass der Verantwortliche deren Verarbeitung einschränkt (Art. 18 Abs. 1 lit. b DSGVO).
- 180 Kann die betroffene Person auf außergewöhnliche Gründe verweisen, die sich aus ihrer besonderen persönlichen Situation ergeben, hat sie nach Art. 21 DSGVO das Recht zum **Widerspruch**. Der Verantwortliche darf die personenbezogenen Daten nach Ausübung des Widerspruchsrechts nur dann noch verarbeiten, wenn zwingende schutzwürdige Gründe bestehen, welche die vorgebrachten besonderen Interessen der betroffenen Person im Einzelfall überwiegen. Andernfalls muss der Verantwortliche die personenbezogenen Daten gem. Art. 17 Abs. 1 lit. c DSGVO löschen.
- 181 Für die Dauer, während der der Verantwortliche die Richtigkeit personenbezogener Daten oder die Voraussetzungen eines Widerspruchs prüft, kann die betroffene Person die **Einschränkung** der Verarbeitung gem. Art. 18 DSGVO verlangen. Ein Anspruch auf Einschränkung der Verarbeitung besteht auch dann, wenn der Verantwortliche die personenbezogenen Daten nur aus demjenigen Grund aufbewahrt, um sie zu einem späteren Zeitpunkt ggf. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen zu nutzen. Wurde die Verarbeitung eingeschränkt, dürfen personenbezogene Daten nur noch aus besonderen in Art. 18 Abs. 2 DSGVO genannten Gründen verarbeitet werden. Bevor der Verantwortliche die Einschränkung aufhebt, ist die betroffene Person nach Art. 18 Abs. 3 DSGVO zu unterrichten.
- 182 Der Verantwortliche ist nach Art. 19 Satz 1 DSGVO verpflichtet, etwaige Empfänger, denen die berichtigten Daten offengelegt wurden, über die Berichtigung, Löschung und Einschränkung zu informieren. Die betroffene Person kann verlangen, dass ihr diese Empfänger mitgeteilt werden (Art. 19 Satz 2 DSGVO).

b) Sonstige Berichtigungsansprüche

- 183 Die Berichtigungs- und Löschanträge nach Art. 16, 17 DSGVO decken sich mit dem aus der arbeitsvertraglichen Fürsorgepflicht abgeleiteten Anspruch, **unrichtige Tatsachenbehauptungen** aus der **Personalakte** zu entfernen oder zu berichtigen⁴.

¹ Gola/Pötters, Art. 5 DSGVO Rz. 24; BeckOK Datenschutzrecht/Schantz, Art. 5 DSGVO Rz. 28.

² Simitis/Dix, Art. 16 DSGVO Rz. 18.

³ Gola/Nolte/Werkmeister, Art. 17 DSGVO Rz. 9.

⁴ Vgl. BAG v. 8.5.2001 – 9 AZR 208/00, EzA § 611 BGB Fürsorgepflicht Nr. 60. Zur Abmahnung: Müller, DB 2011, 2604 (2408).

Bedeutend ist das sich auf die Personalakte beziehende, besondere **Gegendarstellungsrecht** nach § 83 Abs. 2 BetrVG bzw. § 26 Abs. 2 Satz 4 SprAuG. Anders als der Anspruch auf Vervollständigung personenbezogener Daten durch eigene Erklärungen nach Art. 15 Satz 2 DSGVO bezieht sich das Gegendarstellungsrecht auch auf **Werturteile**¹. Wie das Recht zur Einsichtnahme ist auch das Gegendarstellungsrecht als **Ableitung aus dem Persönlichkeitsrecht** des Arbeitnehmers dem Arbeitsvertragsrecht (§ 241 Abs. 2 BGB) zuzuordnen und gilt deshalb über das BetrVG hinaus². Ein Bezug zu einem bestimmten Element der Personalakte ist nicht notwendig, der Arbeitnehmer kann seine Personalakte auch schlicht ergänzen³. Der Arbeitgeber hat dabei nur ein **formelles Prüfungsrecht**, ob die Erklärung überhaupt Bestandteil der Personalakte sein kann⁴.

Hinweis: In arbeitsrechtlichen Auseinandersetzungen werden Berichtigungs- und Löschungsansprüche vorrangig geltend gemacht, um die Richtigkeit von Abmahnungen⁵ und dienstlichen Beurteilungen⁶ in Frage zu stellen und deren Entfernung aus der Personalakte zu erreichen. Ob sich die neu geschaffenen Ansprüche der DSGVO hierbei als effektives Instrumentarium erweisen, bleibt abzuwarten. Voraussetzung für die Anwendbarkeit der DSGVO-Ansprüche wäre nur, dass die Abmahnung oder Beurteilung zu einer Personalakte genommen wird, die als Dateisystem iSd. Art. 2 Abs. 1 DSGVO geführt ist (vgl. Rz. 6). Wird ein Arbeitnehmer abgemahnt, wäre als Reaktion zB denkbar, unter Widerspruch gegen die Verarbeitung die Löschung, hilfsweise Berichtigung der Abmahnung geltend zu machen und für die Dauer der Prüfung die Einschränkung ihrer Verarbeitung zu fordern. Solange die Verarbeitung einer Abmahnung infolge einer solchen Antragsstellung eingeschränkt wird, ist fraglich, ob der Arbeitgeber eine weitergehende Kündigung auf die Abmahnung stützen darf, insbesondere im Anhörungsverfahren nach § 102 Abs. 1 BetrVG. Der Arbeitgeber müsste die gestellten Anträge des Arbeitnehmers zwingend innerhalb des Fristenregimes nach Art. 12 Abs. 3 DSGVO behandeln. Gegen die Reaktion des Arbeitgebers oder dessen Untätigkeit kann der Arbeitnehmer im nächsten Schritt Beschwerde bei der Aufsichtsbehörde einreichen.

4. Datenübertragbarkeit

Die verantwortliche Person hat nach Art. 20 Abs. 1 DSGVO einen Anspruch darauf, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Der Anspruch setzt voraus, dass die Verarbeitung aufgrund einer Einwilligung oder zur Erfüllung eines Vertrages (zB des Arbeitsvertrages) erfolgt und mithilfe automatisierter Verfahren (dh. durch EDV⁷) durchgeführt wird. Der Arbeitgeber ist hingegen nicht verpflichtet, in Papierform geführte Akten einzuscannen. Welche personenbezogenen Daten als durch die betroffene Person „bereitgestellt“ gelten und dem Anwendungsbereich unterfallen, ist umstritten⁸. In jedem Fall erfasst sind die bei Eingehung des Beschäftigungsverhältnisses übermittelten Stammdaten⁹.

Die betroffene Person ist berechtigt, die zur Verfügung gestellten elektronischen Daten einem anderen Verantwortlichen zu übermitteln. Die betroffene Person kann verlangen, dass der Verantwortliche selber direkt an einen anderen Verantwortlichen übermittelt (Art. 20 Abs. 2 DSGVO), dh. dass sich – zB bei einem Arbeitgeberwechsel – der alte Arbeitgeber zum Zwecke der Datenübermittlung direkt mit dem neuen Arbeitgeber in Verbindung setzt. Dies erscheint allerdings wenig praxisgerecht.

1 Richardi/*Thüsing*, § 83 BetrVG Rz. 39, 41.

2 WPK/*Preis*, Vor § 81 ff. BetrVG Rz. 2 f.

3 GK-BetrVG/*Franzen*, § 83 Rz. 33 mwN; WPK/*Preis*, § 83 BetrVG Rz. 14.

4 HM, vgl. GK-BetrVG/*Franzen*, § 83 Rz. 34 mwN; WPK/*Preis*, § 83 BetrVG Rz. 14.

5 ASP/*Vossen*, § 1 KSchG Rz. 415 ff.

6 BAG v. 24.1.2007 – 4 AZR 629/06, NZA-RR 2007, 608; LAG Rh.-Pf. v. 22.8.2018 – 7 Sa 71/18, öAT 2019, 18.

7 Kühling/*Buchner/Herbst*, Art. 20 DSGVO Rz. 13.

8 Eingehend mwN Plath/*Kamlah*, Art. 20 DSGVO Rz. 6 f.

9 Plath/*Kamlah*, Art. 20 DSGVO Rz. 6.

5. Schadensersatzansprüche

188 Materielle Schäden durch Datenschutzverletzungen im Arbeitsverhältnis sind selten¹. Bedeutung erlangt immer mehr der Ersatz immaterieller Schäden².

a) Ansprüche nach Art. 82 DSGVO

189 Nach Art. 82 DSGVO kann jede Person, der wegen eines Datenschutzverstößes ein materieller oder immaterieller Schaden entstanden ist, Schadensersatz von dem Verantwortlichen oder dessen Auftragsverarbeiter verlangen. Haftungsgrund ist jeder Verstoß gegen die DSGVO. Als Verstoß gegen die DSGVO gelten auch Verstöße gegen die auf Grundlagen der DSGVO ergangenen mitgliedstaatlichen Datenschutzbestimmungen (Erwägungsgrund 145 Satz 5 DSGVO)³, also zB § 26 BDSG und einschlägige Kollektivvereinbarungen⁴.

190 Der Verantwortliche oder der Auftragsverarbeiter kann sich von der Haftung befreien, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 83 Abs. 3 DSGVO). An der Verantwortlichkeit in diesem Sinne fehlt es, wenn den Verantwortlichen kein Verschulden trifft⁵. Ungeklärt ist, unter welchen Voraussetzungen dem Verantwortlichen Datenschutzverstöße seiner Mitarbeiter zugerechnet werden⁶.

191 Die Bedeutung des Art. 82 DSGVO wird in erster Linie in der ausdrücklichen Anerkennung eines ersatzfähigen **immateriellen Schadens** gesehen. In der Vergangenheit wurden Ansprüche nach richterrechtlicher Rechtsfortbildung nur in Fällen „schwerwiegender“ Persönlichkeitsrechtsverletzungen⁷ und dann auch nur in vergleichsweise überschaubarer Höhe⁸ zugesprochen. In der Literatur wird damit gerechnet, dass die Rechtsprechung die Schmerzensgeldansprüche nunmehr ausweitet und der Höhe nach deutlich anhebt⁹. Art und Inhalt des Schadens muss die betroffene Person beweisen, welche Ersatz fordert¹⁰.

1 Denkbar wäre dies beispielsweise, wenn ein Arbeitnehmer eine Stelle nicht erhält, nachdem unrichtige Daten an eine einstellungsbefugte Stelle weitergegeben worden waren.

2 Beispiele bei *Grimm/Freh*, ArbRB 2012, 151 (153 f.).

3 *Plath/Becker*, Art. 82 DSGVO Rz. 4; *Kühling/Buchner/Bergt*, Art. 82 DSGVO Rz. 24.

4 Der mitgliedstaatliche Schadensersatzanspruch nach § 83 BDSG gilt demgegenüber nur für Verstöße gegen den dritten Teil des BDSG und spielt für den Beschäftigtendatenschutz daher keine Rolle, *Plath/Becker*, § 83 BDSG Rz. 1; *Paal/Pauly/Frenzel*, § 83 BDSG Rz. 2.

5 *Kühling/Buchner/Bergt*, Art. 82 DSGVO Rz. 80; *Gola/Gola/Piltz*, Art. 82 Rz. 18.

6 Für eine generelle Zurechnung *Gola/Gola/Piltz*, Art. 82 Rz. 18; für die Anwendbarkeit der Exkulpationsmöglichkeiten des § 831 Abs. 1 Satz 2 BGB hingegen *Plath/Becker*, Art. 82 DSGVO Rz. 5b.

7 BAG v. 19.2.2015 – 8 AZR 1007/13, NZA 2015, 994; v. 18.12.1984 – 3 AZR 389/83, NZA 1985, 811.

8 Das BAG hatte unter der alten Rechtslage über den Fall einer rechtswidrigen Videoobservation durch einen Detektiv zu entscheiden, für die letztlich ein Schmerzensgeld von 1 000 Euro festgesetzt wurde, BAG v. 19.2.2015 – 8 AZR 1007/13, NZA 2015, 994. Gegen einen Arbeitgeber, der seinen Betriebsratsvorsitzenden über 20 Arbeitstage beschatten ließ und einer Detektei dafür ein Honorar von 40 000 Euro zahlte, setzte das LAG Rh.-Pf. (v. 27.4.2017 – 5 Sa 449/16, ArbR 2017, 367) ein Schmerzensgeld von 10 000 Euro fest. In einem Fall einer schwerwiegenden und „hartnäckigen“ Verletzung des informationellen Selbstbestimmungsrechts und einer schweren Persönlichkeitsverletzung durch eine dreimonatige Videoüberwachung hat das LAG Hessen v. 25.2.2010 – 7 Sa 1586/09, ArbRB 2011, 138 (*Jacobi*) den Arbeitgeber zu einer Entschädigung von 7 000 Euro verurteilt, nachdem die Vorinstanz noch 15 000 Euro zugesprochen hatte. Weitere Fälle bei *Grimm/Freh*, ArbRB 2012, 151 (153 f.).

9 *Dzida*, BB 2018, 2677 (2678); *Plath/Becker*, § 83 BDSG Rz. 4c; *Kühling/Buchner/Bergt*, Art. 82 DSGVO Rz. 18; *Schantz*, NJW 2016, 1841 (1847).

10 *Kühling/Buchner/Bergt*, Art. 82 DSGVO Rz. 20.

b) Ansprüche nach § 280 Abs. 1, § 241 Abs. 2 BGB

Die öffentlich-rechtlichen Pflichten des Arbeitgebers bestimmen zugleich dessen **arbeitsvertragliche Nebenpflichten**¹. Damit stellt ein Verstoß gegen die DSGVO und § 26 BDSG auch eine Vertragsverletzung des Arbeitgebers dar. Führt der nach § 276 Abs. 1 BGB schuldhaftige Verstoß des Arbeitgebers zu einem Schaden nach den §§ 249 ff. BGB, so hat er diesen nach § 280 Abs. 1 Satz 1, § 241 Abs. 2 BGB zu ersetzen. Der Anspruch besteht neben Ansprüchen aus Art. 82 DSGVO². Über § 278 Satz 1 BGB haftet der Arbeitgeber auch für Erfüllungsgehilfen, wovon auch der **Datenschutzbeauftragte** erfasst wird³. Das Verschulden wird nach § 280 Abs. 1 Satz 2 BGB widerlegbar vermutet. Die **Beweislast** für die haftungsbegründende Kausalität liegt bei der betroffenen Person⁴. 192

Besteht kein Arbeitsvertragsverhältnis, jedoch bereits ein **vorvertragliches Schuldverhältnis**, gelten nach § 311 Abs. 2 BGB die Pflichten nach § 241 Abs. 2 BGB. Entsprechend kann ein Schadensersatzanspruch auf § 280 Abs. 1, § 241 Abs. 2, § 311 Abs. 2 BGB (culpa in contrahendo) gestützt werden⁵. 193

c) Ansprüche nach §§ 823 ff. BGB

In Betracht kommen kann auch eine Haftung nach **§ 823 Abs. 1 BGB**, wenn durch den Datenschutzverstoß das **allgemeine Persönlichkeitsrecht** des Betroffenen verletzt wird⁶. Soweit nicht Organe selbst, sondern Mitarbeiter gehandelt haben, greift **§ 831 Abs. 1 Satz 1 BGB**, wobei hier die Exkulpationsmöglichkeit nach § 831 Abs. 1 Satz 2 BGB bei Wahrung der erforderlichen Sorgfalt bei Auswahl und Leitung besteht. Sofern diese greift, kann dennoch weiterhin ein Organisationsverschulden bestehen⁷. In Einzelfällen kann auch ein Anspruch nach **§ 824 Abs. 1** oder **§ 826 BGB** gegeben sein⁸. Möglich ist auch ein Anspruch aus **§ 823 Abs. 2 BGB** in Verbindung mit der Verletzung eines **Schutzgesetzes**. Das setzt voraus, dass die Norm nach Inhalt und Zweck nicht nur dem Schutz des öffentlichen Interesses, sondern **auch dem Schutz von individuellen Rechtsgütern** und Interessen dient⁹. Bei Bestimmungen über die Verarbeitung personenbezogener Daten wird dies **meist** der Fall sein¹⁰. Die ausschließlich den Datenschutzbeauftragten betreffenden Regelungen wie die Art. 37 ff. DSGVO bezwecken keinen Individualschutz¹¹. 194

6. Unterlassungsansprüche

Aus **Art. 79 Abs. 1 DSGVO** ergibt sich ein **europarechtlicher Unterlassungsanspruch** gegen die ordnungswidrige Verarbeitung personenbezogener Daten¹². Während die Rechte der betroffenen Person auf Löschung (Art. 17 DSGVO), Einschränkung (Art. 18 DSGVO) und Widerspruch 195

1 MünchArbR/Reichold, § 96 Rz. 89.

2 Gola/Gola/Piltz, Art. 82 Rz. 21; MünchArbR/Reichold, § 96 Rz. 89.

3 Da der Datenschutzbeauftragte aber lediglich beratende Funktion hat, ist kaum denkbar, dass seine Tätigkeit einen kausalen Schaden verursacht, s. DWWS/Däubler, Art. 39 DSGVO Rz. 9.

4 Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 12.

5 MünchArbR/Reichold, § 96 Rz. 89.

6 Etwa BGH v. 22.5.1984 – 6 ZR 105/82, NJW 1984, 1886; Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 17 mwN.

7 MünchKomm/Wagner, § 823 BGB Rz. 97 f.

8 Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 20.

9 Etwa BGH v. 14.5.2005 – VI ZR 185/04, NJW 2005, 2923 (2924); vgl. MünchKommBGB/Wagner, § 823 BGB Rz. 405.

10 DWWS/Sommer, Art. 82 DSGVO Rz. 45; zumindest für die §§ 28 ff., 32 und 33 ff. BDSG EAS/Franzen, Datenschutz im Arbeitsverhältnis B 5300, Rz. 103; für die §§ 4, 6, 27 ff., 33 ff. BDSG MünchArbR/Reichold, § 96 Rz. 89.

11 Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 19.

12 Plath/Becker, Art. 79 DSGVO Rz. 2; aA Sydow/Krefe, Art. 79 DSGVO Rz. 10 ff.

(Art. 21 DSGVO) gegen die Verarbeitung bestimmter personenbezogener Daten gerichtet sind, kann sich die betroffene Person auf diese Weise auch gegen eine bestimmte Art und Weise der Verarbeitung wehren.

- 196 Daneben können der betroffenen Person entsprechend §§ 12, 862, 1004 BGB analog Beseitigungs- und Unterlassungsansprüche zustehen¹. Voraussetzung hierfür ist ein rechtswidriger Eingriff in das allgemeine Persönlichkeitsrecht sowie Wiederholungsgefahr, auf ein Verschulden kommt es jedoch nicht an². Da dieser Anspruch jedoch richterrechtlich aus allgemeinen Rechtsgrundsätzen abgeleitet wird, hat er in erster Linie lückenfüllenden Charakter³.

7. Zurückbehaltungsrecht

- 197 Mit Blick auf die Rechtsfolge von § 615 Satz 1 BGB besteht ein Zurückbehaltungsrecht nach § 273 Abs. 1 BGB nur unter dem Vorbehalt der **Verhältnismäßigkeit** von Nebenpflichtverletzung und Arbeitspflicht⁴. Die **Erheblichkeit** ist bei Datenschutzverletzungen sorgfältig zu prüfen⁵. Das **Prognoserisiko** trägt der Arbeitnehmer. Der geltend gemachte Gegenanspruch muss konkret bezeichnet werden, um dem Arbeitgeber die Möglichkeit zur Abhilfe zu geben⁶.

VII. Datenerhebungen von A–Z

1. Bewerberdaten

- 198 **Bewerbungsunterlagen** geben einen Gesamtüberblick über das Persönlichkeitsprofil einer Person und sind **datenschutzrechtlich** besonders **sensibel**. Die Datenschutzbehörden setzen sich daher mit dem Bewerberdatenmanagement von Unternehmen intensiv auseinander. Um Bewerberdaten angemessen zu schützen, müssen Arbeitgeber unbedingt konzeptmäßige Maßnahmen ergreifen⁷:
- 199 Der **Zugriff auf Bewerberdatenbanken** ist nach einem Berechtigungskonzept zu beschränken. Bewerben sich Mitarbeiter auf eine ausgeschriebene Stelle, dürfen grundsätzlich nur Mitarbeiter Einsicht in die Bewerbungsunterlagen erhalten, die am Verfahren um die Besetzung genau dieser Stelle auch tatsächlich beteiligt sind. Nur wenn der Bewerber eine Initiativbewerbung eingereicht oder ausdrücklich seine Einwilligung erteilt, dürfen die Bewerbungsunterlagen einem größeren Kreis von Führungskräften zur Verfügung gestellt werden, damit umfassend gesucht werden kann, ob es irgendwo im Unternehmen eine geeignete Stelle gibt⁸.
- 200 Für gespeicherte Bewerbungsunterlagen müssen **automatisierte Löschfristen** definiert werden. Bewerben sich Interessenten auf eine bestimmte Stelle und willigen sie nicht darin ein, dass das Unternehmen ihre Bewerbung auch für andere in Betracht kommende Stellen heranziehen darf, beginnt die Löschfrist mit Abschluss des Bewerbungsverfahrens für die ausgeschriebene Stelle zu laufen. Von da an darf das Unternehmen die Bewerbungsunterlagen gemäß Art. 17 Abs. 3 lit. e DSGVO noch für eine begrenzte Zeit aufbewahren, um sich notfalls gegen mögliche Entschädigungs-

1 MünchArbR/Reichold, § 96 Rz. 91; Kock/Francke, NZA 2009, 646 (651).

2 MünchArbR/Reichold, § 96 Rz. 91.

3 EAS/Franzen, Datenschutz im Arbeitsverhältnis B 5300, Rz. 106.

4 BAG v. 13.3.2008 – 2 AZR 88/07, AP Nr. 87 zu § 1 KSchG 1969; ausführlich Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 7.

5 Vgl. ErfK/Preis, § 611a BGB Rz. 617, 690; Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 8.

6 BAG v. 13.3.2008 – 2 AZR 88/07, AP Nr. 87 zu § 1 KSchG 1969; Thüsing/Pötters, Beschäftigtendatenschutz und Compliance, § 21 Rz. 7.

7 Eingehend hierzu Grimm/Kühne, ArbRB 2018, 245.

8 LfDI Baden-Württemberg: Der Ratgeber – Beschäftigtendatenschutz, S. 33.