Articles

The Impact of Digitalisation on the Protection to One's Own Image in the Employment Context

Sarah Deutschmann[*]

Due to increasing digitalisation, employees are confronted with technologies in the employment relationship that enable the monitoring of their entire behaviour. A particularly valuable protected right, the right to one's own image, is being particularly threatened by the increased use of smart glasses and video surveillance.
So far, the German Bundesdatenschutzgesetz (Federal Data Protection Act) and the European General Data Protection Regulation have provided a legal framework. In order to comprehensively protect the rights of employees, but still take into account the economic interests of employers, the laws offer various authorisations that allow a comprehensive balancing of interests.

The author shows under which conditions and for which purposes employees' images may be collected and processed. In doing so, she deals with the individual phases of the employment relationship and shows how the interests of employees and employers are to be balanced in detail. The author also assesses the extent to which the authorisations can be appropriately applied to new technologies. She concludes that the flexible authorisations can also lead to appropriate results with regard to new technologies and illustrates her argument using the example of data glasses.

However, she also claims that the current legal situation entails legal uncertainties and difficulties with implementation and proposes the establishment of an independent Employee Data Protection Act. She suggests creating specific regulations for different phases of the employment relationship and including criteria developed by case law. Nevertheless, she also argues in favour of retaining a general clause with a flexible assessment in order to be able to include new technologies that emerge in the future.

---

[*] Law student, HHU Düsseldorf. The author gives her thanks to Professor Jan Busche. All errors are entirely the author's.

A. Introduction

The production and distribution of employee portraits has always played a significant role in the external appearance of companies.[1] Images in booklets, on posters or in newspapers have always been intended to give customers a personal impression and an overview of the company structure.[2] While the editions were mainly regionally limited and spread slowly, nowadays large amounts of data can be collected and distributed at high speed,[3] which also makes the possibilities for producing and distributing images much more diverse. Companies present themselves through promotional films in which their employees can be seen, with photos of the team on their website, in newsletters or on social media.[4] Content on websites and social media platforms can be accessed worldwide and employees are confronted with video surveillance at their workplace.[5] It is important to be aware of the need to find appropriate solutions for balancing the interests of employees and employers.[6] On the employee side, the general right of personality enshrined in Article 2 (1) in conjunction with Article 1 (1) GG (Grundgesetz, German Constitution), which gives the individual the right to decide for themselves about the production of photographs of their image and any utilisation.[7] Moreover, Article 8 CFR

[1] Martina Benecke and Nadja Groß, 'Das Recht am eigenen Bild im Arbeitsverhältnis, Voraussetzungen und rechtliche Probleme einer Einwilligung durch den Arbeitnehmer' (2015) 32 NZA 833.

[2] Karl Riesenhuber, '§ 26 BDSG Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses' in Amadeus Wolff, Stefan Brink and Antje v Ungern-Sternberg (eds), *Beck´scher Online Kommentar Datenschutzrecht* (48th edn, C.H.Beck 2024) para 179; Michael Fuhlrott and Julia Madeleine Remy, '"Neuer" Datenschutz in Kanzleien – Anwälte als Arbeitgeber, Datenverarbeitende und Werbende' (2018) 35 NZA 609, 612.

[3] Rüdiger Krause, Expertise Digitalisierung und Beschäftigtendatenschutz (research report 482, Federal Ministry of Labour and Social Affairs 2016) 7; Marita Körner, 'Beschäftigtendatenschutz in Betriebsvereinbarungen unter der Geltung der DS-GVO' (2019) 36 NZA 1389, 1393.

[4] Ubbo Assmuss and Florian Winzer, 'Mitarbeiterfotos im Intranet, auf Websites und in sozialen Netzwerken, Anforderungen an Einwilligung und Widerruf nach dem KUG und der DS-GVO' (2018) 9 ZD 508, 509; Joachim Ritter von Strobl-Albeg, '7. Kapitel Bildberichterstattung – Bildnisse und Bilder' in Karl Egbert Wenzel, *Das Recht der Wort- und Bildberichterstattung, Handbuch des Äußerungsrechts* (6th edn, Otto Schmidt 2018) 192.

[5] LAG Hamm Case 11 Sa 858/16, 12 June 2017, ZD 2018, 92; Frank Venetis and Christian Oberwetter, 'Videoüberwachung von Arbeitnehmern' (2016) 69 NJW 1051.

[6] Maxi Nebel, 'Big Data und Datenschutz in der Arbeitswelt, Risiken der Digitalisierung und Abhilfemöglichkeiten' (2018) 9 ZD 520, 523; Axel von Walter, *Datenschutz im Betrieb* (Haufe 2018) 17.

[7] BVerfG Case 1 BvR 653/96, 15 December 1999, BVerfGE 101, 361, 381; Tristan Barczak 'GG Art. 2 Abs. 1' in Frauke Brosius-Gersdorf (ed), *Dreier Grundgesetz-Kommentar Band 1* (4th edn, Mohr Siebeck 2023) para 80.

(Charter of the fundamental rights of the EU) ensures the protection of personal data. However, this is accompanied by the interests of the employer, for example to optimise operational processes and thus economic benefits or to protect property or employees through surveillance measures.[8] These interests are guaranteed by the freedom of occupation arising from Article 12 (1) GG or the right to property under Article 14 (1) GG.[9] New challenges for legislators to strike a balance between these interests arise as technologies such as video conferencing, biometric access systems or working with assistance systems including smart glasses and artificial intelligence make it increasingly easy to monitor employees and control their behaviour.[10]

This article will answer the question of whether the regulations on the right to one's own image in the employment relationship are still contemporary with regard to the effects of digitalisation and new technologies. It will provide an overview of the permissibility of the processing of employee images before, during and after the employment relationship has ended, as well as highlighting and discussing new problems and adjustments already made by the legislator as a result of digitalisation. It will also outline the legislative need for action to create an independent Employee Data Protection Act.

B. Legal framework

I. Special need for protection of the right to one's own image in the employment relationship

The right to one's own image is a specification of the general personality right under Article 2 (1) in conjunction with Article 1 (1) GG and guarantees that everyone may decide for themselves on the production and use of their own image.[11]

Modern technologies make it possible to capture and process a person's appearance unnoticed and at any time,[12] making it impossible for individuals to decide which image data they wish to disclose. The risk of the unnoticed profiling, for example using facial recognition technology, data glasses or video surveillance, is increasing.[13]

The employment relationship in particular bears considerable risks for the individual

[8] BAG Case 8 AZR 1010/13, 11 December 2014, BAGE 150, 195 para 38; Nebel (n 6) 523.

[9] OVG Saarlouis Case 2 A 662/17, 14 December 2017, ZD 2018, 134 para 39; BAG Case 2 AZR 133/18, 23 August 2018, ZD 2019, 226 para 30.

[10] Rüdiger Krause, 'Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0' (2017) 34 NZA-Beilage 53; Alexander Roßnagel, 'Datenschutzgesetzgebung für öffentliche Interessen und den Beschäftigungskontext, Chancen für risikoadäquate Datenschutzregelungen?' (2017) 41 DuD 290.

[11] BVerfG Case 1 BvR 653/96 (n 7) 381.

[12] BVerfG Cases 1 BvR 1602/07, 1 BvR 1606/07 and 1 BvR 1626/07, 26 February 2008, BVerfGE 120, 180, 198; Udo Di Fabio, 'GG Art. 2 Abs. 1' in Günter Düring and others (eds), *Grundgesetz Kommentar* (103th edn, C.H.Beck 2024) para 193.

[13] Thomas Klebe, 'Betriebsrat 4.0 – Digital und global?' (2017) 34 NZA-Beilage 77, 82; Florian Klein, *Personenbildnisse im Spannungsfeld von Datenschutzgrundverordnung und Kunsturhebergesetz* (Peter Lang 2017) 254.

employee's right to their own image. Due to the personal dependency on the employer, which characterises the employment relationship (see Section 611a (1) sentence 1 BGB, German civil code), the two parties do not meet as equals and the employee is in a particularly vulnerable position.[14] It is often the case that the employee grants the employer comprehensive access to their image data during the employment relationship.[15] Photos in application documents, on employee ID cards or video surveillance are mandatory requirements in some companies.[16]

In view of these circumstances, the protection of the right to one's own image in the employment relationship is of great importance so that comprehensive legal regulations are required in order to find solutions that are in line with the interests of the parties involved.

II. Legal Sources

1. Kunsturhebergesetz (German Law for the protection of images)

In German law, the protection of the right to one's own image is initially governed by the Kunsturhebergesetz (KUG, German Law for the protection of images),[17] which has been in existence for over 115 years.[18] Sections 22 ff KUG protects the distribution and public display of images, but not their production. According to Section 22 KUG, images of the person shown may only be published with the consent of the person concerned. Section 23 (1) KUG makes exceptions in this respect, according to which consent may be waived, but these are subject to the condition under Section 23 (2) KUG that they must not infringe any legitimate interests of the person depicted.

2. General Data Protection Regulation

The General Data Protection Regulation (GDPR) has provided far-reaching protection for the processing of personal data at European level since 2018, as set out in Section 1(1) of the Regulation. According to Art. 4 (1) GDPR, 'personal data' is any information relating to an identified or identifiable natural person. If it is possible to recognise the person depicted on the basis of the photo or video recording, this allows conclusions to be drawn about the individual employee and is therefore to be classified as personal data within the

[14] Federal Ministry of Labour and Social Affairs, *Weißbuch Arbeiten 4.0* (2017) 142 <https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/a883-weissbuch.pdf?_blob=publicationFile&v=2> accessed 24 July 2024; Tim Wybitul, 'Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO' (2017) 34 NZA 413, 416.

[15] Kerstin Reiserer and others, 'Beschäftigten-Datenschutz und EU-Datenschutz-Grundverordnung, Der Countdown ist abgelaufen – Anpassungsbedarf umgesetzt?' (2018) 56 DStR 1501, 1502; Fuhlrott and Remy (n 2) 612.

[16] Assmuss and Winzer (n 4) 511; Riesenhuber (n 2) 159.

[17] Benecke and Groß (n 1) 834; Klein (n 13) 93.

[18] RGBL 1907, number 3, page 7 (official Law Journal of the German Empire).

meaning of Art. 4 (1) GDPR.[19] According to Art. 4 (2) GDPR, the processing of this data includes any operation relating to personal data, such as the collection, storage, distribution or deletion of such data. In the employment context, the General Data Protection Regulation therefore regulates the period between the initiation and the termination of the employment relationship.

3. Bundesdatenschutzgesetz (Federal Data Protection Act)

However, images of employees are also subject to the provisions of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). The scope of protection in Section 1 BDSG covers the processing of personal data by public bodies of the federal government and the federal states as well as by non-public bodies, whereby the scope of application for these is limited by Section 1 (1) sentence 2, (4) sentence 2 BDSG. The terms 'processing' and 'personal data' are identical to those of the General Data Protection Regulation,[20] meaning that any process relating to information of identifiable natural persons is covered. If it is possible to recognise the person depicted and conclusions can be drawn about the individual employee, personal portraits are also covered by the scope of protection of the German Federal Data Protection Act.

III. Current legal situation

1. Primacy of the General Data Protection Regulation

The protection of the right to one's own image therefore falls within the scope of protection of the General Data Protection Regulation as well as the German Kunsturhebergesetz and the German Federal Data Protection Act. However, as a European regulation, the GDPR is binding in its entirety pursuant to Article 288 TFEU (Treaty on the Functioning of the European Union) and applies directly in every member state. It therefore takes primacy over national law, which means that both the BDSG and the KUG are inapplicable.[21]

2. Opening clauses

However, the General Data Protection Regulation provides so-called opening clauses, through which the European member states are granted regulatory autonomy.[22]

---

[19] Benecke and Groß (n 1) 836; von Strobl-Albeg (n 4) 29.

[20] Riesenhuber (n 2) 32.

[21] Fuhlrott and Remy (n 2) 610; Peter Gola and Yvette Reif, 'BDSG § 1' in Peter Gola and Dirk Heckmann (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (3rd edn, C.H.Beck 2022) para 19.

[22] Assmuss and Winzer (n 4) 511; Pascal Schumacher, 'Scope of application of the GDPR' in Daniel Rücker and Tobias Kugler (eds), *New European General Data Protection Regulation A Practitioner´s Guide* (C.H.Beck 2018) para 206; Stefan Brink, 'Aktuelle Tendenzen im Beschäftigtendatenschutz der Europäischen Union' (2023) 40 NZA-Beilage 86, 87.

a. Opening clause in Art. 88 GDPR

In the context of employees, Article 88 (1) GDPR provides for an authorisation to adopt more specific provisions to ensure the protection of rights and freedoms with regard to the processing of personal employee data (para 1), insofar as these are appropriate to ensure specific measures to protect human dignity and the legitimate interests of the fundamental rights of the affected person (para 2). The German legislator has enacted Section 26 BDSG in this sense.[23]

b. Opening clause in Art. 6 (2) GDPR

For employee data protection in the public sector, there is a further opening clause in Art. 6 (2) GDPR, which the legislator has not yet made use of.[24]

c. Opening clauses for the KUG

The German legislator has also not utilised possible opening clauses that exist for the Kunsturhebergesetz, as no notification has been made to the Commission that could justify retention in accordance with Article 85 (3) or Article 88 (3) GDPR,[25] meaning that the Art Copyright Act does not apply to the right to one's own image in the employment relationship so far.

d. ECJ judgement from 30 March 2023

However, uncertainties regarding the legality of the German regulation in Section 26 BDSG were raised by the ruling of the ECJ on 30 March 2023, which had to decide on a question referred for a preliminary ruling regarding the state data protection regulation Section 23 HDSIG (Hessian Data Protection and Freedom of Information Act).[26] It argued that Section 23 (1) sentence 1 HDSIG violates the prohibition of repetition under EU law, according to which national regulations must necessarily 'distinct from the general rules of that regulation'.[27]

The purpose of this provision is to prevent member states from undermining the interpretation of EU law through their own case law.[28]

---

[23] BT-Drs 18/11325, 96 (governmental proposal); Krause, 'Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0' (n 10) 58; Brink (n 22) 87.

[24] Alexander Roßnagel 'DS-GVO Art. 6 II' in Spiros Simitis and other (eds), *Datenschutzrecht DSGVO mit BDSG* (2nd edn, Nomos 2019) para 33.

[25] Klein (n 13) 181; Behrang Raji, 'Auswirkungen der DS-GVO auf nationales Fotorecht, Das KUG im Zahnradmodell der DS-GVO' (2019) 9 ZD 61, 65.

[26] Case C – 34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer* [2023] EU:C:2023:270.

[27] ibid 61, 74, 81.

[28] Robert Selk, 'DS-GVO Art 88' in Eugen Ehrmann and Martin Selmayr (eds), *Datenschutzgrundverodnung* (3rd edn, C.H. Beck 2024) para 60; Markus Wünschelbaum, 'Tabula rasa im Beschäftigtendatenschutz? – EuGH setzt neue Maßstäbe: Rechtsfolgen und Handlungsoptionen' (2023) 9 NZA 542.

However, Section 23 (1) sentence 1 HDSIG is almost identical in wording to Section 26 (1) sentence 1 BDSG, meaning that a breach of Union law in the state law provision must consequently also lead to the inapplicability of Section 26 (1) sentence 1 BDSG.[29] Therefore, the provisions of the GDPR must be applied. In the case of Section 26 (1) sentence 1 BDSG, this is Article 6 (1) GDPR.[30]

It remains unclear to what extent the other authorisation provisions of Section 26 BDSG fulfil the requirements of EU law. In the German literature, there are opinions that assume conformity with EU law[31] as well as those that argue contrary to this.[32] However, Section 26 BDSG remains applicable until further notice, except for paragraph 1 sentence 1.[33]

3. Preliminary result

Consequently, the assessment of the permissibility of the processing of image data of employees under German law is still mainly based on Section 26 BDSG whereby the basic principles of the GDPR must be observed even when applying German law.[34] However, in cases where Section 26 (1) sentence 1 BDSG was applied, Art. 6 GDPR must now be used. Also if employees' personal data is processed for purposes outside the context of the employment relationship, Section 26 BDSG does not apply, but instead those of the General Data Protection Regulation.[35]

C. Legitimacy of the processing of employee images

I. Scope of application

Section 26 BDSG has a broad scope of application. Firstly, within the personal scope of application in accordance with Section 26 (8) BDSG also temporary workers, trainees, applicants and persons whose employment relationship has ended are covered, in addition to 'traditional' employees.[36] In terms of time, it even includes pre-contractual

[29] Daniel Sandvoß and Hans-Hermann Schild, 'Neue Entwicklungen des Beschäftigtendatenschutzes im Lichte der Rechtsprechung des EuGH vom 30.3.2023' (2023) 23 NJOZ 1056, 1057; Peter Wedde, 'Neues zum Rechtsrahmen für den Beschäftigtendatenschutz' (2024) AuR 197.

[30] Case C – 34/21 (n 26) paras 18 ff.

[31] Markus Wünschelbaum, 'Kommt ein souveränes Beschäftigtendatenschutzgesetz?' (2023) 26 MMR 548; Wedde (n 29).

[32] Sandvoß and Schild (n 29) 1058.

[33] See also Wünschelbaum, 'Tabula rasa im Beschäftigtendatenschutz?' (n 28).

[34] Martin Franzen, 'Datenschutz-Grundverordnung und Arbeitsrecht' (2017) 10 EuZA 313, 346; Michael Kort, 'Die Zukunft des deutschen Beschäftigtendatenschutzes, Erfüllung der Vorgaben der DS-GVO' (2016) 6 ZD 555, 556.

[35] Johannes Klausch and Jan Felix Grabenschröer, 'Zukünftige Erlaubnistatbestände der Verarbeitung von Beschäftigtendaten' (2018) 6 (3) PinG 135, 139; Wybitul (n 14) 415.

[36] Fuhlrott and Remy (n 2) 612; Michael Kort, 'Der Beschäftigtendatenschutz gem. § 26 BDSG-neu, Ist die Ausfüllung der Öffnungsklausel des Art 88 DS-GVO geglückt?' (2017) 7 ZD 319, 323.

relationships in addition to the period of employment and after its termination.[37]

II. Authorisations

Pursuant to Section 26 BDSG, the processing of personal employee data is generally prohibited unless there is a legal authorisation (so-called prohibition with reservation of permission).[38] A distinction must be made between statutory authorisation (Section 26 (1), (3) BDSG, Art 6 (1) (b) and (f) GDPR) and processing on the basis of consent or collective agreements (Section 26 (4) BDSG).[39]

1. Statutory authorisation

In the case of statutory authorisation, the law initially differentiates between a general clause, processing for the detection of criminal offences and the processing of special categories of personal data.

a. Processing under the general clause

Previously, Section 26 (1) 1 BDSG regulated the processing of personal data of employees for the purposes of the employment relationship. Even though this provision is no longer applicable following the judgement of the ECJ,[40] data processing remains permitted based on Article 6 (1) GDPR. Pursuant to Article 6 (1) (b) GDPR processing shall be lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. The term 'necessity' in this context refers to what is 'absolutely necessary' within the scope of the contractual relationship.[41]

However, Article 6 (1) (f) extends the scope that processing shall be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which requires protection of personal data. In this case, the conflicting fundamental rights positions, for example the employee's right to

[37] Peter Gola and others, 'Was wird aus dem Beschäftigtendatenschutz? – Die DS-GVO, das DS-AnpUG und § 26 BDSG-neu' (2017) 41 DuD 244, 245; Michael Kort, 'Beschäftigtendatenschutz gemäß dem BDSG 2018 (unter Einbeziehung neuerer Rechtsprechung)' in Martina Benecke (ed), *Unternehmen 4.0 Arbeitsrechtlicher Strukturwandel durch Digitalisierung* (Nomos 2018) 101.

[38] Rüdiger Linck, '§153 Beschäftigtendatenschutz' in Günter Schaub, *Arbeitsrechts-Handbuch – Systematische Darstellung und Nachschlagewerk für die Praxis* (20th edn, C.H.Beck 2023) para 5; Harald Stelljes, 'Stärkung des Beschäftigtendatenschutzes durch die Datenschutz-Grundverordnung – Viel Lärm um Nichts?' (2016) 40 DuD 787, 788.

[39] Dagmar Gesmann-Nuissl 'Rechtliche Herausforderungen in der Arbeitswelt 4.0 im Mittelstand anhand von zwei Beispielen' in Christian Bosse and Klaus J Zink (eds), *Arbeit 4.0 im Mittelstand Chancen und Herausforderungen des digitalen Wandels für KMU* (Springer Gabler 2019) 47 f; von Walter (n 6) 101.

[40] Case C – 34/21 (n 26).

[41] Sandvoß and Schild (n 29) 1058; Horst Heberlein, 'DS-GVO Art 6' in Eugen Ehrmann and Martin Selmayr (eds), *Datenschutzgrundverodnung* (3rd edn, C.H. Beck 2024) para 25.

one's own image, and the employer's interests in data processing must be balanced.[42] In conclusion, processing that was previously permitted under Section 26 (1) sentence 1 BDSG is now generally permitted under Article 6 (1) (b) and (f) GDPR. However, the extensive case law of the German courts on Section 26 (1) sentence 1 BDSG is not applicable, as the ECJ has sovereignty over the interpretation of Union law.[43]

When assessing the permissibility it must be taken into account that different requirements have to be applied for in the individual periods of employment due to the different accessibility of the data and the employees' need for protection.

aa. Before the employment relationship is established

The processing of image data prior to the establishment of the employment relationship may become relevant, for example, in the context of application documents in which the applicant has attached a photo, as well as in the application process in general[44] or if the employer obtains information about the applicant on social networks.[45] In all three cases, the processing is generally considered proportionate. While the employee is largely free to decide whether to use photos in the application process, the employer is generally entitled to collect information from publicly accessible sources, including social networks, insofar as the information is publicly accessible.[46] However, such applicant data may only be used up to the time of the decision on the employment of the applicant and must be deleted as soon as no further legal disputes are to be expected.[47]

bb. During the employment relationship

In the employment relationship, for example, photos on employee ID cards are generally considered necessary as they serve to authenticate the individual, treat the employee's data with care and are only made accessible to a limited group of recipients.[48] In contrast, the publication of employee photos in a promotional film, in the employee profile on the company's website and in social networks is not necessary and is therefore subject to the requirement of consent.[49] Public dissemination constitutes a serious infringement of the

[42] Case C – 275/06 *Promusicae* [2008] EU:C:2008:54 para 66; Case C – 597/19 *Mircom International* [2021] ECLI:EU:C:2021:492 para 112.

[43] Case C – 135/15 *Griechenland/Nikiforidis* [2016] EU:C:2016:774 para 28; Sandvoß and Schild (n 29) 1059 f.

[44] Reiserer and others (n 15) 1504.

[45] Martin Franzen 'BDSG § 26' in Rudi-Müller-Glöge and others (eds), *Erfurter Kommentar zum Arbeitsrecht* (24th edn, C.H.Beck 2024) para 19; Ralf Selig, *Arbeitnehmerdatenschutz – Das Datenschutzrecht im Spannungsfeld zwischen Mitarbeiterkontrolle und Arbeitnehmerinteressen* (Logos 2011) 118.

[46] Riesenhuber (n 2) 99, 101; Franzen, 'BDSG § 26' (n 45) 19.

[47] Franzen, 'BDSG § 26' (n 45) 20; Peter Gola and Stephan Pötters, 'BDSG § 26' in Peter Gola and Dirk Heckmann (eds), *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz* (3rd edn, C.H.Beck 2022) para 186.

[48] Riesenhuber (n 2) 159.

[49] ArbG Lübeck Case 1 Ca 538/19, 20 June 2019, BeckRS 2019, 36456 para 23; Franzen, 'BDSG § 26' (n 45) 33.

employee's general right of personality, which is not outweighed by the employer's interests in presenting its workforce or wanting to convey a personal impression to customers.[50] Exceptions are rare, for example in the case of important company events such as company celebrations or if publication is expressly the subject of the contract, for example in the case of a professional model.[51]

cc. After termination of the employment relationship

Personal data of employees may also be processed after termination of the employment relationship.[52] This is particularly relevant in the case of video recordings permitted under Section 26 (1) sentence 2 BDSG, which may constitute evidence for any legal disputes.[53] However, for many other personal data, in particular personal portraits, the purpose of the processing of this data or the necessity will cease to apply upon termination of the employment relationship.[54]

b. Processing for the detection of criminal offences

Section 26 (1) sentence 2 BDSG places much stricter requirements than Section 26 (1) sentence 1 BDSG and Article 6 (1) (f) GDPR on the permissibility of processing employees' personal data.[55] Processing data is permitted if (1) there are factual indications that justify the suspicion of a criminal offence by the data subject, (2) the processing is necessary for detection and (3) no interests of the data subject prevail. Consequently, vague indications or preventive surveillance measures, administrative offences or breaches of contract do not fall within the scope of application.[56] If the requirements of Section 26 (1) sentence 2 BDSG are not met, data processing may still be justified under Article 6 lit (f) GDPR. Section 26 (1) sentence 2 BDSG does not have a preclusive effect in this respect.[57]

In particular, video surveillance of non-public areas is covered by the authorisation requirement of Section 26 (1) sentence 2 BDSG.[58] The 'concept of necessity' also requires the conflicting fundamental rights positions to be weighed up in the context of the

[50] See also Assmuss and Winzer (n 4) 511.

[51] ibid 509, 511; Julian Fischer, 'Datenschutzrechtliche Stolperfallen im Arbeitsverhältnis und nach dessen Beendigung, Ein Leitfaden für Arbeitgeber nach der EU-Datenschutzgrundverordnung' (2018) 35 NZA 8, 11.

[52] Heberlein (n 41) 24.

[53] BAG Case 2 AZR 133/18 (n 9) 33; Katja Chadna-Hoppe, 'Beweisverwertung bei digitaler Überwachung am Arbeitsplatz unter Geltung des BDSG 2018 und der DS-GVO – Der gläserne Arbeitnehmer?' (2018) 35 NZA 614, 618.

[54] Fuhlrott and Remy (n 2) 613; von Walter (n 6) 27.

[55] Benkert, 'Beschäftigtendatenschutz in der DS-GVO-Welt' (2018) 15 NJW-Spezial 562.

[56] Klausch and Grabenschröer (n 35) 137; Michael Kort, 'Die Bedeutung der neuen arbeitsgerichtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes' (2018) 35 NZA 1097, 1099.

[57] Chadna-Hoppe (n 53) 617; Kort, 'Die Bedeutung der neuen arbeitsgerichtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes' (n 56) 1098.

[58] von Walter (n 6).

'principle of proportionality'.[59] The intensity of the surveillance is determined by the number of people being monitored, in particular the number of unsuspected third parties, the intensity of the interference, the duration, the reason for and type of surveillance, as well as the seriousness of the offence and the extent of the existing or imminent damage.[60] The more intensive the monitoring, the more important the employer's interests have to be.

In the case of overt video surveillance, it must first be taken into account that this is permissible in a large number of cases in publicly accessible areas in accordance with Section 4 BDSG and is to be assessed less strictly in the context of the proportionality test. In these cases, video surveillance often even serves to protect employees, such as in banks or petrol stations.[61] However, it must also be taken into account that the person concerned is often under increased psychological pressure to behave inconspicuously as a result of the surveillance, which directs their overall behaviour and thus constitutes a serious infringement of their general right of personality.[62] This is particularly the case in areas that are not publicly accessible. However, video surveillance is prohibited in the highly personal living areas of employees, such as changing rooms or showers (see Section 201a StGB, German Criminal Code).[63]

In the case of concealed video surveillance, the person concerned does not even have the opportunity to decide on the processing of their personal data themselves, which is why such an infringement is particularly severe.[64] Case law therefore requires the concrete suspicion of a criminal offence and the exploitation of less extensive instruments for clarification, so that concealed video surveillance is practically the only remaining instrument.[65] It is therefore only permissible in those exceptional cases.[66]

c. Processing of special categories of personal data

Section 26 (3) sentence 1 BDSG provides a more specific legal authorisation for the processing of special categories of personal data. According to Article 9 GDPR, this includes, for example, data revealing racial or ethnic origin or data of a genetic or

[59] BAG Case 2 AZR 681/16, 27 July 2017, BAGE 159, 389 para 30; Wybitul (n 14) 416.

[60] Riesenhuber (n 2) 137; Michael Kort, 'Neuer Beschäftigtendatenschutz und Industrie 4.0, Grenzen einer „Rundumüberwachung" angesichts der Rechtsprechung, der DSGVO und des BDSG nF' (2018) 71 RdA 24, 25.

[61] Riesenhuber (n 2) 148.

[62] BAG Case 1 ABR 46/15, 25 April 2017, BAGE 159, 49 para 20; Riesenhuber (n 2) 144.

[63] Isabell Conrad and Christina Treeger '§ 34 Recht des Datenschutzes' in Astrid Auer-Reinsdorff and Isabell Conrad (eds), *Handbuch IT- und Datenschutzrecht* (3rd edn, C.H. Beck 2019) para 283.

[64] BAG Case 2 AZR 681/16 (n 59) 23; von Strobl-Albeg (n 4) 41.

[65] BAG Case 2 AZR 51/02, 27 March 2003, BAGE 105, 356; BAG Case 2 AZR 395/15, 20 October 2016, BAGE 157, 69 para 22.

[66] Gola and others (n 37) 246; Selig (n 45) 134f; Wünschelbaum, 'Kommt ein souveränes Beschäftigtendatenschutzgesetz?' (n 31) 549.

biometric nature that enables the identification of an employee. This generally does not include photographs according to Recital 51 sentence 3 GDPR, however, they can be categorised as biometric data if they are processed using special technical means. This may apply, for example, to photos of identity cards,[67] which often have to be presented to the employer to establish the employment relationship. Information on racial or ethnic origin may also emerge from photographs or video recordings.[68] In principle, it should be noted that such recordings are only to be classified as special categories of data if a special type of analysis is carried out, which is becoming increasingly possible through facial recognition technologies.[69] Nevertheless, if the image can be categorised as special categories of personal data, a proportionality test must also be carried out in accordance with Section 26 (3) sentence 1 BDSG, although the processing has to comply with stricter requirements.[70]

2. Processing on the basis of consent

In accordance with Section 26 (2) BDSG, personal data can also be processed on the basis of the employee's consent. However, the validity of consent is subject to a number of requirements in terms of voluntariness, form and certain information obligations.[71]

a. Voluntariness

The criteria of the voluntary nature of the declaration of consent required in Article 4 (11) GDPR is of particular importance due to the pressure that arises in relation to the submission of such a declaration as a result of the dependent relationship between the employee and the employer (see p. 3).[72] When assessing voluntariness, this relationship of dependency and the circumstances under which the consent was given are therefore taken into account in Section 26 (2) sentence 1 BDSG. These circumstances include the type of data processed, the intensity of the interference, the amount of data processed and the timing of the declaration of consent.[73] Consent prior to the establishment of the employment relationship is generally subject to higher requirements because the affected person is often under increased pressure with regard to the signing of an employment

[67] Marion Albers and Raoul-Darius Veit, 'DS-GVO Art. 9' in Amadeus Wolff, Stefan Brink and Antje v Ungern-Sternberg (eds), *Beck´scher Online Kommentar Datenschutzrecht* (48th edn, C.H.Beck 2024) para 43.

[68] Klein (n 13) 27; Eike Michael Frenzel, 'DS-GVO Art. 9' in Boris P Paal and Daniel A Pauly (eds), *Datenschutzgrundverordnung, Bundesdatenschutzgesetz* (3rd edn, C.H.Beck 2021) para 10.

[69] Klein (n 13) 249 ff; Stephan Schindler and Katharina Wentland, 'Videoüberwachung – quo vadis?' (2018) 8 ZD-aktuell 06057.

[70] Nebel (n 6) 523; Kort, 'Beschäftigtendatenschutz gemäß dem BDSG 2018' (n 37) 101 f.

[71] Tim Wybitul '§ 96 Beschäftigtendatenschutz' in Heinrich Kiel and others (eds), *Münchener Handbuch zum Arbeitsrecht Band 1: Individualarbeitsrecht I* (6th edn, C.H.Beck 2024) para 123.

[72] Conrad and Treeger (n 63) 338; Kort, 'Beschäftigtendatenschutz gemäß dem BDSG 2018' (n 37) 95.

[73] Riesenhuber (n 2) 47; Susanne Dehmel and Gesa Diekmann, 'I, Robot, Mr. Know-it-all? Datenschutz und Industrie 4.0' (2016) 4 (4) PinG 141, 143.

contract.[74]

In this context, the prohibition of tying under Article 7 (4) and Recital 43 sentence 2 GDPR needs to be considered. According to this, the employer may not restrict the signing and fulfilment of the employment contract to the employer's consent to data processing unless this is necessary for the fulfilment of the contract.[75]

However, the relationship of dependency between employee and employer can also be significantly less extensive in certain cases.[76] Section 26 (2) sentence 2 BDSG mentions two constellations in which a voluntary declaration of consent is regularly given. Firstly, if this results in a legal or economic advantage for the employee, and secondly, if the employer and employee pursue the same interests. The explanatory memorandum to the law cites a number of standard examples for these cases. According to this, the publication of a photo on the intranet is considered to be in the same interest.[77] Irrespective of this, it must be taken into account that the specific circumstances have to be weighed up in each individual case.[78]

b. Form

With regard to the required form, Section 26 (2) sentence 3 BDSG demands that consent is given in written or electronic form, unless there are specific circumstances that allow this requirement to be waived. However, the concept of electronic evidence is to be understood more broadly than that of Section 126a BGB (German civil code), so that a declaration of consent in an email is also sufficient to fulfil the formal requirements.[79] By dispensing with the originally exclusive written requirement, the legislator has declared circumstances such as exclusively electronic applications or consent for employees working from home to be the rule and thus made an important adjustment to digitalisation.[80]

As a further requirement, consent must relate to a specific use case in accordance with the principle of specificity and must not be generalised, which is also stated in Article 4 (11) GDPR.[81]

---

[74] BT-Drs 18/11325, 97 (governmental proposal); Conrad and Treeger (n 63) 339.

[75] Martin Franzen, 'VO (EU) 2016/679 Art. 5' in Martin Franzen and others (eds), *Kommentar zum Europäischen Arbeitsrecht* (5th edn, C.H.Beck 2024) para 9; Klausch and Grabenschröer (n 35) 139; Linck (n 38) 13.

[76] Tobias Gräber and Christine Nolden, 'BDSG § 26' in Boris P Paal and Daniel A Pauly, *Datenschutzgrundverordnung, Bundesdatenschutzgesetz* (3rd edn, C.H.Beck 2021) para 27.

[77] BT-Drs 18/11325, 97 (governmental proposal).

[78] Klausch and Grabenschröer (n 35) 139; von Walter (n 6) 122.

[79] BT-Drs 19/11181, 19 (decision recommendation by the Committee on Home Affairs and Integration); Gregor Thüsing and Sebastian Rombey, 'Die „schriftlich oder elektronisch" erteilte Einwilligung des Beschäftigten nach dem neuen Formerfordernis in § 26 II 3 BDSG' (2019) 36 NZA 1399, 1401.

[80] Riesenhuber (n 2) 45; Franz Düwell and Stefan Brink, 'Beschäftigtendatenschutz nach der Umsetzung der Datenschutz-Grundverordnung: Viele Änderungen und wenig Neues' (2017) 34 NZA 1081, 1084 f.

[81] Linck (n 38) 15; Conrad and Treeger (n 63) 340.

c. Duty to provide information and right of withdrawal

According to Section 26 (2) sentence 4 BDSG, the employer is also obliged to inform the employee in text form about the purpose of the data processing and their right to withdraw consent in accordance with Article 7 (3) GDPR.

This right of withdrawal entitles the affected person to withdraw their consent at any time without giving reasons.[82] According to Article 7 (3) 2 GDPR, the revocation is effective for the future. However, as Article 17 (1) (b) GDPR clarifies, the processing of personal data may still be permitted by the statutory permissions. This provision is essential, for example, if the publication of an image is part of the fulfilment of a contract for which the affected person has been paid, as is usually the case with a modeling contract.[83]

d. Relevance of processing on the basis of consent

In connection with the legal uncertainties in contractual relationships resulting from the possibility of withdrawal and the high requirements for voluntariness and its provability, the question arises to what extent processing on the basis of consent is used in practice at all. The widely held view that processing on the basis of consent is less relevant in practice due to these circumstances[84] must be contradicted. Even if the permissibility of the processing of personal data often already results from the statutory authorisation, processing on the basis of consent is indispensable as soon as employee images are published, for example on the company's website or on social media.[85]

3. Collective agreements

According to Section 26 (4) BDSG, collective agreements constitute a further element of authorisation. The purpose of this provision is to enable adaptation to the specific characteristics of different companies. [86] As Section 26 (4) sentence 2 BDSG also clarifies, the principles of Article 88 (2) GDPR must be observed, in particular the legitimate interests and fundamental rights of the affected persons must be protected.[87] The interests of the parties concerned must be balanced, as is also the case with the other statutory authorisation possibilities. This can be ensured, for example, in works

[82] Assmuss and Winzer (n 3) 510; Karin Spelge, 'Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO)' (2016) 40 DuD 775, 781.

[83] Fischer (n 51) 11; Philip Uecker, 'Die Einwilligung im Datenschutzrecht und ihre Alternativen, Mögliche Lösungen für Unternehmen und Vereine' (2019) 9 ZD 248, 250.

[84] Dehmel and Diekmann (n 73) 142 f.; Klausch and Grabenschröer (n 35) 139; see also Data Protection Working Party, 'Opinion 2/2017 on data processing at work' (WP 249, 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=45631> accessed 24 July 2024.

[85] Regarding the requirement of consent in these cases see also Assmuss and Winzer (n 3) 509; Fuhlrott and Remy (n 2) 612.

[86] BT-Drs 18/11325, 98 (governmental proposal); Nebel (n 6) 523.

[87] Franzen, 'BDSG § 26' (n 45) 48; Wybitul (n 14) 413.

agreements through the works council's duty to co-operate.[88] The regulation in collective agreements is particularly suitable for the video surveillance of employees.[89]

4. Interim result

Summarising, it can be said that there are many ways to regulate the interests of employers and employees in the various periods of employment with the statutory authorisation, consent and the possibility of regulation in collective agreements.

III. Compliance with the principles of Art. 5 GDPR

When weighing up the interests of the individual circumstances, certain principles for the processing of personal data must also be taken into account (see Section 26 (5) BDSG), which are listed in Article 5 GDPR. Some of these principles, which can be problematic in the employment relationship, are highlighted below as examples.

1. Principle of transparency

The principle of transparency is enshrined in Article 5 (1) (a) GDPR. Accordingly, the data subject must be informed about the purpose of the processing of their personal data and their rights.[90] In the employment context, problems may arise in particular with concealed video surveillance as well as the use of artificial intelligence, but these can be solved by the employer informing the works council about the scope of the use so that they can check compliance with the principles.[91]

2. Principle of purpose limitation

One of the most important principles of European data protection law is the principle of purpose limitation, which is set out in Art. 5 (1) (b) GDPR.[92] The purpose of data processing must be established and clearly defined at the time of processing. Further processing for other purposes, known as a 'change of purpose', requires a separate legal basis (Recital 50 GDPR sentence 2) or must still be compatible with the original regulatory purpose (Recital 50 GDPR sentence 1). This becomes relevant in the context of the protection of the right to one's own image in the case of so-called ‘chance finds’. These occur when another offence, for example one of another employee, is uncovered as a

[88] Reiserer and others (n 15) 1505; von Walter (n 6) 133.

[89] Kort, ‘Die Bedeutung der neuen arbeitsgerichtlichen Rechtsprechung für das Verständnis des neuen Beschäftigtendatenschutzes’ (n 56) 1102; von Walter (n 6) 142.

[90] Stelljes (n 38) 790; Joachim Schrey, ‘General conditions for data processing in companies under the GDPR’ in Daniel Rücker and Tobias Kugler (eds) *New European General Data Protection Regulation, A Practitioner´s Guide* (C.H.Beck 2018) para 606.

[91] Dehmel and Diekmann (n 73); Matthias Lachenmann, ‘Neue Anforderungen an die Videoüberwachung, Kritische Betrachtung der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG-neu’ (2017) 7 ZD 407.

[92] Franzen, ‘VO (EU) 2016/679 Art. 5’ (n 75) 5.

result of permitted concealed video surveillance of an employee.[93] A change of purpose is justified in this context in accordance with Section 26 (1) sentence 2 BDSG, as long as the misconduct discovered would itself have justified such surveillance, i.e. it is a criminal offence or other serious breach of duty that is proportionate to the violation of the right to one's own image.[94]

3. Principle of data minimisation

It is also important to observe the principle of data minimisation, which arises from Article 5 (1) (c) GDPR. According to this, the processing of personal data should be 'adequate in relation to the purposes for which it is processed and limited to what is necessary'. In the employment relationship, for example, the group of uninvolved persons monitored should be kept as small as possible in the case of permitted video surveillance and, if possible, the data should be anonymised.[95]

4. Interim result

It can be seen that the principles of transparency, purpose formation and data minimisation are fundamental to the consideration of the employee's right to their own image. They consequently require comprehensive consideration when weighing up interests.

IV. Co-determination right of the works council

In order to ensure even more comprehensive protection of the employee's right to one's own picture, the works council has a right of co-determination in accordance with Section 87 (1) no. 6 BetrVG (German Works Constitution Act) with regard to 'the introduction and use of technical equipment' if this is 'intended to monitor the behaviour or performance of employees'. According to the case law of the Federal Labour Court, an intention to process data by the employer is not required. Instead, the only condition is that the technical equipment is objectively suitable for monitoring behaviour or performance.[96] With regard to the protection of the right to one's own image, this right of co-determination of the works council is mainly relevant in the case of video surveillance of employees, but also when working with assistance systems or biometric access systems.[97] These new technologies are making co-determination rights increasingly relevant, which

[93] Chadna-Hoppe (n 53) 618; Kort, 'Neuer Beschäftigtendatenschutz und Industrie 4.0' (n 60) 27.

[94] LAG Hamm Case 11 Sa 858/16 (n 5) 95; Venetis and Oberwetter (n 5) 1053.

[95] See also Peter Schantz, 'DS-GVO Art. 5' in Amadeus Wolff, Stefan Brink and Antje v Ungern-Sternberg (eds), *Beck´scher Online Kommentar Datenschutzrecht* (48th edn, C.H.Beck 2024) para 25.1; Selig (n 45) 134.

[96] BAG 1 Case ABR 43/81, 6 December 1983, BAGE 44, 285; BAG Case 1 ABR 7/03, 27 January 2004, BAGE 109, 235.

[97] Riesenhuber (n 2) 201.

can lead to negotiation processes between employers and works councils slowing down a company's technical progress.[98] Many representatives in the literature as well as companies and employers' associations are therefore calling for the co-determination law to be adapted so that only those cases in which the employer intends to monitor are subject to approval.[99] It remains to be seen to what extent this is possible, taking into account the protection of employee data privacy.[100]

V. Applicability of the principles to new technologies

As already shown, the use of new assistive devices such as smart glasses or even artificial intelligence, biometric access systems or the exchange of information using video conferencing is constantly increasing.[101] The question therefore arises whether the authorisation provisions of Section 26 BDSG are suitable for integrating these technologies. This is analysed in more detail below using the example of smart glasses.

Smart glasses are glasses that provide users with information about their surroundings. For example, they can show the employee information about work steps or stock levels and are used by employers to improve operational processes.[102] However, they can consistently collect image data and thus create movement profiles and behavioural patterns of the employees who are wearing them and those who are in the area surrounding the data glasses.[103] It is questionable whether the authorisation conditions guarantee a comprehensive balance of interests.

Processing on the basis of consent seems rather unsuitable as a legal basis, as the purpose of wanting to improve operational processes cannot be considered voluntary due to the relationship of dependency between employer and employee. It would also create legal uncertainties for the employer due to the freedom to withdraw consent.[104] However, the permissibility can be based on Article 6 (1) (f) GDPR. The collection of personal data therefore has to be necessary for the purposes of the legitimate interests pursued by the controller or by a third party, which requires the conflicting fundamental

[98] Thomas Kania 'BetrVG § 87' in Rudi Müller-Glöge and others (eds), *Erfurter Kommentar zum Arbeitsrecht* (24th edn, C.H.Beck 2024) para 57; Johannes Schipp, 'Industrie 4.0 und Mitbestimmung bei technischen Innovationen' (2016) ArbRB 177, 179.

[99] Federal Ministry of Labour and Social Affairs (n 14) 147; Gerrit Hornung and Kai Hofmann 'Datenschutz als Herausforderung der Arbeit in der Industrie 4.0' in Hartmut Hirsch-Kreinsen and others (eds), *Digitalisierung industrieller Arbeit, Die Vision Industrie 4.0 und ihre sozialen Herausforderungen* (2nd edn, Nomos 2018) 238.

[100] Federal Ministry of Labour and Social Affairs (n 14) 148.

[101] Krause, 'Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0' (n 10); Roßnagel (n 10).

[102] Krause, *Expertise Digitalisierung und Beschäftigtendatenschutz* (n 3) 14 f; Dehmel and Diekmann (n 73) 142.

[103] Klebe (n 13) 82; Klein (n 13) 254.

[104] Reiserer and others (n 15) 1505 ff; von Walter (n 6) 126.

rights to be weighed up as part of a proportionality test.[105] Data glasses can be used to display helpful information to employees,[106] which can make their work easier and open up the possibility of organising production processes more effectively, resulting in an improvement in operational work processes. This purpose is permitted as such under the law, relates to the performance of the employment relationship and is promoted by the use of smart glasses, which is why they appear suitable for achieving the purpose.[107] Whether there is no equally suitable means that is less restrictive of the employee's personal rights ('necessity')[108] cannot be answered in general terms. Firstly, it should be noted that there are assistance systems that could provide the relevant information with the help of employee input. Nonetheless, this would not be equally suitable for facilitating their work and improving operational work processes, particularly in terms of the time required and the skills required for employees to recognise the problem in question. Furthermore, the employer's autonomy generally allows him to decide on the effectiveness of the measures.[109]

In the context of a detailed weighing up, the employee's right to their own image as an expression of the general right of personality (Article 2 (1) in conjunction with Article 1 (1) GG) must be taken into account.[110] The data glasses can record the entire environment of the employee wearing them.[111] This means that comprehensive movement profiles, behavioural patterns and communication with others can be recorded.[112] It should also be noted that employees who are simply in the area around the smart glasses are particularly affected,[113] as they cannot determine the extent to which their image is recorded and will often not even notice the process. In addition, data is collected throughout the entire working time and is therefore particularly intensive. On the employer's side, particularly economic interests are at stake, which are secured as utilisation and exploitation interests by the right of property and the basic right to carry on the business.[114]

In order to fulfil the interests of both parties, it is necessary to ensure that the employee's personal rights are protected while permitting the use of the smart glasses. To accomplish

[105] BT-Drs 18/11325 (governmental proposal); Bernd Grzeszick, 'GG Art .20' in Günter Düring and others (eds), *Grundgesetz Kommentar (*103th edn, C.H.Beck 2024) para 109 ff.

[106] Dehmel and Diekmann (n 73) 142; Klebe (n 13).

[107] On the concept of 'necessity' see BVerfG Case 2 BvL 45/92, 10 April 1997, BVerfGE 96, 10, 23; BVErfG Cases 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66 and 1 BvR 754/66, 16 March 1971, BVerfGE 30, 292, 316.

[108] BVerfG Case 1 BvL 14/60B, 14 December 1965, BVerfGE 19, 330, 337; Gesmann-Nuissl (n 39) 49 f.

[109] Nebel (n 6) 523.

[110] Düwell and Brink (n 80) 1084; Klausch and Grabenschröer (n 35) 136.

[111] Kai Hofmann, 'Smart Factory, Arbeitnehmerdatenschutz in der Industrie 4.0, Datenschutzrechtliche Besonderheiten und Herausforderungen' (2016) 6 ZD 12, 13; Reinhold Kopp and Karen Sokoll, 'Wearables am Arbeitsplatz – Einfallstore für Alltagsüberwachung?' (2015) 32 NZA 1352, 1354.

[112] Hofmann (n 111) 13; Klebe (n 13) 82.

[113] Kopp and Sokoll (n 111) 1354.

[114] Krause, 'Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0' (n 10) 54; Selig (n 45) 90.

this, video data should not be stored and personal data should not be accessible to the employer in real-time. If personal data needs to be evaluated for operational optimisation purposes, it has to be deleted immediately afterwards.[115] It is also essential that the data is anonymised,[116] that the employee has the option of switching off the smart glasses[117] and that the employer ensures that the data cannot be accessed by third parties.[118] Ensuring that employees are not monitored, but that the data is only analysed to optimise work, is therefore imperative.[119] The use of smart glasses in the employment relationship can therefore take into account the interests of both parties, if certain conditions are met. As the example of data glasses shows, the flexible balancing of interests made possible by the authorisation provisions of Section 26 BDSG and Article 6 (1) (f) GDPR can be used to find solutions that are in line with the interests of both parties, allowing new technologies to be integrated.

D. Conclusion and perspectives

The previous explanations have shown that Section 26 BDSG and Article 6 GDPR provide regulations that enable a comprehensive balancing of interests with regard to the permissibility of processing employee images from the period before the employment relationship is established until after it has ended. Although positive aspects of the regulation could be emphasised, there are also certain aspects that appear to be in need of improvement. However, there is currently an urgent need for action, particularly in view of the ECJ judgement from 2023, which leads to the inapplicability of Section 26 (1) 1 BDSG.

Nevertheless, it is worth mentioning that different types of authorisations ensure that both the interests of the employer and the right to one's own image of the employee are taken into account.[120] The respective weighting of interests in individual cases proves to be flexible and suitable for balancing interests in the context of new technologies.[121] Moreover, the legislator has made important adjustments to digitalisation by dispensing with the written requirement[122] or the specific prerequisite to be placed on the processing of special categories of personal data.[123] The risks of digitalisation have also been counteracted by the primacy of the General Data Protection Regulation and the resulting

[115] Gesmann-Nuissl (n 39) 50; Stelljes (n 38) 790.
[116] Dehmel and Diekmann (n 73) 144; Klebe (n 13) 82.
[117] Gesmann-Nuissl (n 39) 50.
[118] Kopp and Sokoll (n 111) 1355.
[119] Dehmel and Diekmann (n 73) 144; Hofmann (n 111) 17.
[120] Chadna-Hoppe (n 53) 617.
[121] ibid 619.
[122] Riesenhuber (n 2) 45; Düwell and Brink (n 80) 1084 f.
[123] Frenzel (n 68) 10; Schindler and Wentland (n 69).

inapplicability of the provisions of the Kunsturhebergesetz. This is significant because the provisions of the KUG do not appear to be able to cope with the risks of facial recognition software and increasingly advanced camera technology, as Section 23 (1) KUG permits the dissemination of images in exceptional cases, such as when the person concerned appears merely as an accessory to a landscape or other location (No. 2).[124]

However, problems have arisen in particular since the ECJ ruling of 30 March 2023. Not only the applicability of Art. 6 GDPR alongside the applicability of Section 26 (1) sentence 2, (3), (4) BDSG, but specifically the concerns regarding the legality of Section 26 BDSG in its entirety under EU law have led to considerable legal uncertainty.[125]
In order to make employee data protection even more comprehensive and, above all, more legally certain, it is essential to create an independent Employee Data Protection Act.[126] Section 26 BDSG and Article 6 (1) GDPR are characterised by many undefined legal terms and, in particular, the abstract proportionality test leads to certain legal uncertainties.[127] Those entail particular risks for companies due to the fines, which can amount to up to 4% of a company's annual turnover depending on the severity of the violation in accordance with Art. 83 GDPR.[128] A separate law could specify these terms and it would be possible to stipulate certain criteria for the assessment. In addition, different requirements must be placed on the various phases of the employment relationship, which is why a separation of these phases appears appropriate in order to create individual balancing factors.[129] In the context of Section 26 BDSG (especially as a result of the inapplicability of Section 26 (1) sentence 1 BDSG) the General Data Protection Regulation must be referred to again and again. This could be simplified for legal practitioners by an independent Employee Data Protection Act. However, challenges arise for legislators due to the prohibition of repetition under EU law, according to which national regulations must necessarily 'distinct from the general rules of that regulation'.[130] In addition, the case law of the Federal Labour Court or the Higher Administrative Courts is often used because no specific statutory balancing factors are specified as part of the weighing process. A statutory structure would create more clarity for employers in this respect. An independent Employee Data Protection Act could include individual provisions for different types of personal data. As part of the regulations on the right to one's own image of employees, separate provisions could be created for publication, overt and concealed video surveillance or the use of artificial intelligence, for example, in addition to a division

[124] Klein (n 13) 253.
[125] Sandvoß and Schild (n 29) 1063; Wünschelbaum, 'Tabula rasa im Beschäftigtendatenschutz?' (n 28) 547.
[126] Krause, *Expertise Digitalisierung und Beschäftigtendatenschutz* (n 3) 5 ff; Körner (n 3) 1385; Brink (n 22).
[127] Körner (n 3) 1385.
[128] Kort, 'Datenschutz-Grundverordnung und Arbeitsrecht' (n 22) 90.
[129] See also Stelljes (n 38) 791.
[130] See also Wünschelbaum, 'Kommt ein souveränes Beschäftigtendatenschutzgesetz?' (n 31) 550.

into the various phases of the employment relationship.[131] In these provisions, it is then possible to take up individual criteria from case law, form concrete standards and also take into account elementary principles of the General Data Protection Regulation, such as the principles of transparency, purpose limitation and data minimisation.[132] In addition, a flexible general clause could be maintained to cover previously unknown technologies in the future.

In a nutshell, digitalisation poses a high potential risk to the protection of the right to one's own image in the employment relationship, in particular due to the relationship of dependency between the employee and the employer.[133] The General Data Protection Regulation and the associated Federal Data Protection Act have brought some changes to the German legal situation that guarantee the protection of the right to one's own image. Although Section 26 BDSG and Article 6 GDPR can be applied particularly flexibly, because of their abstract consideration in relation to the rapidly developing new technologies, an independent Employee Data Protection Act is now indispensable with regard to the legal certainty of the data subjects due to the wide variety of cases and a possible infringement of EU law by Section 26 BDSG.[134] It is therefore gratifying that the Federal Ministry of Labour and Social Affairs and the Federal Ministry of the Interior and Home Affairs announced the revision of the Employee Data Protection Law in a statement in April 2023.[135] Apart from single proposals in the key issues paper that have not yet been worked out in detail, there have been no concrete elaborations since then. Neither does the key issues paper contain any real innovations for employee data protection law.

Essentially, it aims to establish clear requirements, most of which have already been developed by case law, to form concrete categories of cases and to incorporate practical case studies. In terms of legal certainty, however, this appears to be a consistent and necessary solution. Even though a government draft was announced for the first half of

---

[131] See also Frank Schemmel, 'Neuer Anlauf Beschäftigtendatenschutzgesetz – was lange währt, wird endlich gut?' (2023) 13 ZD-Aktuell 01164; Federal Ministry of Labour and Social Affairs and the Federal Ministry of the Interior and Home Affairs, 'Vorschläge für einen modernen Beschäftigtendatenschutz Innovation ermöglichen – Persönlichkeitsrechte schützen – Rechtsklarheit schaffen' (12 April 2023) <https://www.denkfabrik-bmas.de/fileadmin/Downloads/Publikationen/Vorschlaege_fuer_einen_modernen_Beschaeftigtendatenschutz.pdf> acessed 24 July 2024.

[132] See also Wünschelbaum, 'Kommt ein souveränes Beschäftigtendatenschutzgesetz?' (n 31) 549; Federal Ministry of Labour and Social Affairs and the Federal Ministry of the Interior and Home Affairs, 'Vorschläge für einen modernen Beschäftigtendatenschutz: Innovation ermöglichen – Persönlichkeitsrechte schützen – Rechtsklarheit schaffen' (12 April 2023) <https://www.denkfabrik-bmas.de/fileadmin/Downloads/Publikationen/Vorschlaege_fuer_einen_modernen_Beschaeftigtendatenschutz.pdf> acessed 24 July 2024.

[133] Hornung and Hofmann (n 99) 235 f; Krause, 'Herausforderung Digitalisierung der Arbeitswelt und Arbeiten 4.0' (n 10).

[134] Chadna-Hoppe (n 53) 619; See also Körner (n 3) 1385.

[135] Federal Ministry of Labour and Social Affairs and the Federal Ministry of the Interior and Home Affairs, 'Vorschläge für einen modernen Beschäftigtendatenschutz Innovation ermöglichen – Persönlichkeitsrechte schützen – Rechtsklarheit schaffen' (12 April 2023) <https://www.denkfabrik-bmas.de/fileadmin/Downloads/Publikationen/Vorschlaege_fuer_einen_modernen_Beschaeftigtendatenschutz.pdf> acessed 24 July 2024.

the 20th legislative period (2021 – 2025), it will still take a long time before an Employee Data Protection Act comes into force.