January 2022

Report of the independent interdisciplinary council on employee data protection

Establishment of the Council by the Federal Ministry of Labour and Social Affairs

The Federal Ministry of Labour and Social Affairs established the interdisciplinary council on employee data protection in fulfilment of its mandate set out in the coalition agreement of the 19th legislative period to examine whether stand-alone legislation should be enacted on employee data protection to protect the personal rights of employees at the workplace and establish legal certainty for employers, (coalition agreement for the 19th legislative period between the CDU, CSU and SPD of 7 February 2018, lines 6086 ff.).

The council took up work in June 2020 under the leadership of former Federal Minister of Justice Professor Herta Däubler-Gmelin. In regular meetings, the council's members discussed the data protection requirements of the rapid technology-driven transformation of the world of work. Discussions focused on the legal issues of employee data protection, while at the same time considering ethical, economic and technological perspectives.

The members of the council come from the fields of employment and organisational psychology, supervisory authorities, operational practice, ethics, computer science and law. The topics for discussion ranged from the limits of supervision and monitoring of employees to the question of the permissible extent of obtaining information about applicants to the use of "people analytics software" in the area of human resources.

The consultations, which were mainly virtual due to the pandemic, included a wide range of external expertise. The German Trade Union Confederation (DGB - Deutscher Gewerkschaftsbund) and the Confederation of German Employers' Associations (DBA - Bundesvereinigung der Deutschen Arbeitgeberverbände) made the most important contributions to the discussion. Representatives of the Data Protection Conference (Datenschutzkonferenz) and the Data Ethics Commission (Datenethikkommission) were also consulted. Internal and external data protection officers, works councils and entrepreneurs reported on real-world practical experience in companies. The council also received input from experts in the field of technology, such as Professor Katharina Zweig from the TU Kaiserslautern and Professor Hannes Federrath from the University of Hamburg and from the field of civil society, such as Matthias Spielkamp, co-founder and executive director of AlgorithmWatch.

The council's discussions and work took place without being influenced by third parties.

After finishing its work, the council for employee data protection presented the following theses and recommendations on moving forward with employee data protection to the Federal Minister of Labour and Social Affairs, Hubertus Heil in 17 January 2022.

Theses and Recommendations from the Commission of Experts at the Federal Ministry of Labour and Social Affairs on Moving Forward with Employee Data Protection

I. Digital technologies are changing the world of work

For some years now, the increasing use of digital technologies in companies and administrations has been changing the world of work in profound ways. This process will accelerate in the coming years.

Data-based applications are now a part of the everyday working lives of most employees. The dynamic development of new information and communication technologies means that companies and administrations are producing more and more detailed data sets. There are also new possibilities for linking and evaluating these sets, which means they offer opportunities for a more efficient and people-oriented organisation of work. These data sets also make it possible to increase the intensity of workloads and facilitate intensive oversight and monitoring. This goes all the way up to and includes knowing everything about employees. This can bring clear advantages for both sides, both employees and employers: Digital technologies make it possible to organise work in a way that is simpler and less stressful, as well as more efficient and cost-effective. However, digital transformation also entails considerable risks for employees, especially with regard to their personal rights: Having fine-grained control of operational processes often produces correspondingly detailed data sets related to individual employees. This increases the risk of ever more comprehensive transparency and monitoring of employee performance and behaviour. It is necessary to prevent employers from knowing everything about their employees.

New algorithm-based decision support systems also make analyses and predictions based on the collected data possible. Real or supposed information about the behaviour or personal characteristics of employees can be derived from this.

In the application phase, this can be used to determine the suitability or potential performance of applicants and to identify (supposed) deficits. During employment relationships, the performance of the tasks assigned can be assessed in detail. Such systems and procedures can help people make more informed decisions, but there is the danger of reinforcing existing prejudices and causing new discrimination that is not transparent.

II. Balancing the interests of employees and employers fairly

The council believes that it is becoming increasingly important to have balanced regulations in this tense space between employees' interests and personal rights that are protected by human dignity and fundamental rights and employers' fundamental rights and interests. This is necessary to ensure there is binding protection for employees through effective data protection laws and to fairly balance the competing interests even as the digital transformation of the world of work continues to evolve dynamically. Employers' agreements with works councils can play a special role here.*

In meeting this challenge, it is essential to protect the fundamental personal rights of employees, in particular their fundamental right to informational self-determination. Clear regulations with legal certainty are necessary for effective data protection, so that employees are aware of their personal rights and can assert their rights, and so that employers can see what their obligations under data protection law are.

The council also notes that when processing employee data employers also have legitimate rights and interests protected by fundamental rights. The fun-

* Theses and recommendations concerning works councils (Betriebsräte) also apply to staff councils (Personalräte), staff representatives (Mitarbeitervertretungen) and spokespersons' committees (Sprecherausschüsse).

damental rights of employees and employers must therefore be appropriately balanced. When dealing with employee data, employers and employees should be able to have legal certainty when assessing which decisions and measures are permissible and which are not when processing employee data. This should be accomplished by means of a nationwide, legally binding and reliable set of rules.

III. Guaranteeing fundamental rights and freedoms through national, European and international employee data protection law

The fundamental right to informational self-determination was recognised by the Federal Constitutional Court in its landmark 1983 census ruling as a continuation of the protection of personal rights with regard to the risks of increasing data processing. This is the legal foundation of employee data protection in Germany as part of the protection of personal rights inalienably linked to human dignity. The aspect of employee data protection is legally activated by the fundamental right to informational self-determination. The state is obliged to uphold all fundamental rights, including in the context of the employment relationship with a private employer.

At European level, the regulations of the Charter of Fundamental Rights of the European Union (CFR) and the General Data Protection Regulation (GDPR) define the standard: Article 7 CFR guarantees respect for private life. Article 8 CFR guarantees the fundamental protection of personal data, establishing the fundamental right to data protection in the EU, which is also protected by Article 16 of the Treaty on the Functioning of the European Union (TFEU). The central EU legal framework in this regard is the GDPR. It also applies to employee data protection, but itself contains only rudimentary regulations tailored to this area. The flexibility clause in Article 88 of the GDPR leaves it up to the member states to create "more specific rules" for data protection in the context of employment through legislation and collective agreements. At the international level, Article 8 of the European Convention on Human Rights (ECHR) emphasises the value of the protection of personal rights as a "right to respect for private and family life". This also impacts legal relationships between private individuals.

With Section 26 of the Federal Data Protection Act (BDSG), the lawmakers availed themselves of the possibility for more specific regulations opened up by European law. However, Section 26 of the BDSG often does not allow for definitive statements on the permissibility of concrete processing of employee data in individual cases. It is essentially limited to general-clause type regulations. However, data protection is indispensable as an instrument for safeguarding human dignity, fundamental rights and freedoms. It provides legal certainty and thus effective data protection in the employment context, especially in the digital age. Lawmakers expressly reserved the right to further-reaching regulations on employee data protection at the time (BT-Drs. 18/11325, p. 97).

Employers' legitimate interests in processing employee data have their legal basis in particular in the guarantee of entrepreneurial freedom, in the protection of their legal interests,– and in particular protection of their property–, as well as in their obligations under occupational health and safety law. It is primarily up to lawmakers to assess the situation and strike a fair balance between employees' interests and personal rights that are protected by human dignity and other fundamental rights and employers' fundamental rights and interests. When regulations are more specific, labour courts will no longer have to decide individual case arguments concerning legally binding clarification of the question of which data processing is necessary in employment relationships and for which specific purposes and under which conditions.

IV. Guiding principles for specific regulations on employee data protection

The council believes that the following principles should guide lawmakers in filling out the framework for action under constitutional and EU law in its adaptation and future-oriented improvement of existing employee data protection law in light of the transformation of the world of work:

- reasonable balancing of the fundamental rights of both sides with particular attention to the protection of the human dignity of employees,
- effective protection of fundamental rights and legal certainty for all parties involved,
- a neutral stance towards technology and openness to technology in the regulations due to the dynamic pace of technological change,
- transparency for affected employees and works councils about the equipment and programmes used by employers in processing employee data,
- a guarantee of effective law enforcement.
- When moving forward with employee data protection law, a sense of proportion should be maintained in all measures following a risk assessment.

In terms of new forms of employment that have arisen in the course of the digital transformation of the world of work, the council recommends making adjustments in line with European law within the framework of the possibility to specify details of employee data protection opened up by Article 88 GDPR.

V. Instruments for moving forward with employee data protection law

The central elements of employee data protection with legal certainty that is effective need to be laid down in law. Insofar as, due to their need for interpretation, the existing regulations in the current version of Section 26 of the BDSG offer insufficient protection against intrusive data processing in the digital world of work, balanced, detailed legal regulations are required for all parties involved. Sub-legal regulations such as legal ordinances and collective agreements, but also new types of instruments can also be an integral part of effective employee data protection with legal certainty. Also recommended are further specific data protection law instruments including the development of codes of conduct within the meaning of Article 40 f. GDPR or certification according to Article 42 f. GDPR.

When moving forward with employee data protection, all instruments available to state and private actors, including self-regulation should therefore be considered:

- the instrument of legal regulation as the state's most fundamental option for action is essential. The line between data processing that is legally permissible and that which is not can be defined in a way that is recognisably binding for all parties involved.
- Sub-legal instruments can, on the basis of appropriate legal authorisations, help to make the line between what is legally permissible and impermissible clearer in concrete individual cases, which is important for practice.

VI. Substantive and procedural elements to make applicable law more specific

Justifications for processing employee data include legal grounds of authorisation, consent and collective agreements.

1. Specifics regarding necessity in the case of statutory processing authorisation

Regarding the legal grounds set forth in the GDPR and the BDSG that are linked to the criterion of necessity, the council considers it useful to provide specifics regarding the protection of employees' personal rights both through substantive legal delineation and through procedural elements.

Over decades, a rich body of case law has developed concerning employers' rights to collect data ("right to ask") during the application phase, including recruitment tests and recruitment examinations. In order to achieve the highest possible degree of effectiveness and legal certainty as well as uniformity in employee data protection, the council recommends that relevant case constellations that can be standardised be transferred into statutory law, insofar as appropriate in view of the diversity and dynamics of case practice.

In terms of employment relationships, it is not feasible for lawmakers to include every conceivable case constellation in a concrete situation. Nevertheless, where possible and appropriate, the balancing of interests should be carried out by lawmakers themselves within the framework of new, specific, normatively clear regulations. The council also recommends creating a legal framework for parameters for the assessment of necessity that are oriented in particular on Article 5 GDPR and that take into account, above all, the type, scope, intensity and circumstances of the processing of employee data.

The guiding principle of transparency in control and surveillance measures must also prove itself effective in preventing and detecting criminal acts. The majority of the council believes that covert measures should only be possible in exceptional situations as an ultima ratio for the detection of criminal acts. They should not be used for other serious breaches of duty. A minority of the council, however, considers covert measures to be permissible in exceptional situations as an ultima ratio for the prevention and detection of serious breaches of duty. Another minority rejects covert measures completely. In any case, the council recommends that the legal situation be clarified.

If covert measures are taken, the review of their legality must be ensured ex ante through the involvement of actors from inside or outside companies. Furthermore, it must be guaranteed ex post that the process is transparent and those affected are informed.

Regarding the special case of the comparison of employee data with lists of terrorists and sanctions lists without grounds, the majority of the council considers such comparisons to be permissible only if a specific legal basis is established. A minority of the council considers the existing legal regulations for the legitimisation of such comparisons to be sufficient, however.

2. Requirements for consent as an expression of data sovereignty in employment relationships

Consent is an expression of the right to informational self-determination. Being able to freely dispose of one's own data as one sees fit is thus an aspect of the data sovereignty of every individual. The GDPR regulates the conditions under which consent can constitute an effective legal basis.

According to the GDPR, consent is generally equal in rank to other permissions. That consent be voluntary is of key importance in this regard. The majority of the council believes that because of the fundamentally hierarchical nature of employment relationships, it can usually only be assumed that consent is voluntary if special conditions are met, for example, if the employees are pursuing their own interests or interests similar to their employer's by giving their consent.

During the application process, it cannot be assumed that the consent of applicants is voluntary as a rule. In order to create more legal certainty in that situation, it makes sense to supplement the regulations on voluntary consent already set out in Section 26 (2) sentence 1 BDSG. In order to increase legal certainty for both sides, standard examples of the admissibility or inadmissibility of consent should be formulated for both application procedures and employment relationships. The majority of the council also believes it would be reasonable to supplement the existing law by clarifying that gaining an economic advantage must not necessarily mean "buying" consent, so that employee data does not become a "commodity" that can be purchased.

3. Conditions for company-level agreements as appropriate regulatory instruments

Parties on the company level can actively address employment data-related fields of action and conclude company-level agreements to achieve a fair balance of interests. However, the majority of the council believes that increased use of company-level agreements can only lead to more effective employee data protection if accompanying regulations in the Works Constitution Act (Betriebsverfassungsgesetz) enable the works councils to better fulfil their task of protecting the personal rights of employees. However, a minority of the council favours stronger use of company-level agreements in general as appropriate regulatory instruments and also encourages incentives for employers.

4. Data protection requirements for the use of artificial intelligence in employment relationships

Artificial intelligence represents the next stage of a digital transformation driven by technological progress. It therefore deserves to be considered in its own right. For the council, artificial intelligence means not only self-learning systems, but also algorithmic systems whose function and effect can only be understood by experts due to their high level of complexity.

The council strongly recommends that the use of artificial intelligence in the context of employment be regulated by law. Lawmakers should be guided by the seven data protection requirements for the use of AI formulated by the Hambach Declaration of the Data Protection Conference (DSK). They contain important ideas on the regulation of the use of AI in employment relationships. Legal developments at the European level must also be monitored.

VII. Specific rights of data subjects in the employment context

1. Specifics regarding the rights of data subjects

Litigation before the courts and discussions in the relevant literature are evidence that there is considerable uncertainty and ambiguity concerning the rights of data subjects and the obligations of controllers under the GDPR. How to deal with data subjects' rights should be specified in the context of specific legal foundations for typical processing situations in employment relationships. Employees' right of access to information is to be seen as an essential means of establishing transparency, provided that it is not asserted in an inappropriate context.

2. Regulation of prohibitions on the submission of facts and use of evidence

There was considerable debate in the council over legal standardisation of a prohibition on the use of unlawfully processed employee data in legal proceedings, particularly with reference to fundamental procedural rights. The majority of council members believe that employee data protection in companies with works councils should be made more effective by explicitly opening up the possibility for the parties in the company to include effective prohibitions on the use of data in company-level agreements. A majority of the council also favours legal standardisation stating criteria for judicial review of a prohibition on the submission of facts and use of evidence with regard to the protection of employee data. A minority of the council rejects such regulations as inappropriate interference in the free judicial assessment of evidence.

VIII. Additional regulations in works constitution law in the interest of employee data protection

Works councils play a central role in employee data protection: works constitution law gives them the role of protecting and promoting the rights of employees, also their personal rights. To fulfil this role even when digital technologies are increasingly transforming the world of work, a majority of the council members believe that additional regulations in the Works Constitution Act (Betriebsverfassungsgesetz) are needed. This may include the expansion of the rights of works councils to participate in decision-making related to employee data protection and the facilitation of the involvement of external experts. However, a minority of the council rejects an expansion of the rights of works councils to participate in decision-making and, in particular, the extension of that participation to the appointment of data protection officers, considering that that does not fit the system and is an obstacle to the objectives of data protection.

IX. Improving law enforcement

The majority of the council sees a need to bolster possibilities for legal enforcement, advocating improvements in the legal position of works councils and trade unions within the framework of judicial legal protections. A minority of the council sees no need for regulation in this regard, however.

The council also unanimously recommends increasing the enforcement powers of the supervisory authorities and the independence of company data protection officers.

X. Data protection supervisory authorities as guarantors of effective employee data protection with legal certainty

The council believes that monitoring by data protection supervisory authorities contributes significantly to effective employee data protection with legal certainty.

The council recommends staff increases at the supervisory authorities in order to avoid violations of employee data protection from the outset or to detect them at an early stage. This increase should make it easier for the supervisory authorities to also provide advice that is complementary and supportive.

XI. Establishing an employee data protection commission and a permanent secretariat at the AK Beschäftigtendatenschutz (employee data protection working group) of the Data Protection Conference (DSK)

To supplement stand-alone legislation on employee data protection, the council proposes the creation of two new bodies to monitor and support ongoing technical developments and other relevant developments in the area of employee data protection and to make abstract regulations more specific so that they can be put to use in practice:

- a permanent employee data protection commission at the Federal Ministry of Labour and Social Affairs and
- a permanent secretariat at the Arbeitskreis Beschäftigtendatenschutz (employee data protection working group) of the conference of independent data protection supervisory authorities of the federation and the Länder (Data Protection Conference (DSK)).

The participation of the social partners from business and labour and the independence of the data protection supervisory authorities must be ensured.

In addition to advising those who make laws and ordinances, these bodies may also be tasked with looking at other instruments. These include, for example, supporting best practice approaches, publishing model documents and self-audits for regular stocktaking of the level of data protection. Regarding processing systems in the context of employment, this may also include providing assessment criteria for selection and for use in compliance with data protection. These instruments may also include assistance for development in accordance with the principle of data protection by design and by default (Article 25 GDPR). The special needs of small and medium-sized enterprises must be taken into account.

XII. Recommendations for companies without works councils and recommendations for new forms of employment

In order to effectively implement and enforce employee data protection in companies without works councils, the council proposes that recommendations for action be drawn up for those responsible under data protection law. This could be done, for example, by the employee data protection commission to be created at the Federal Ministry of Labour and Social Affairs. Lawmakers are called upon to establish specific regulations on employee data protection regarding data-based business models and new forms of employment, for example in the platform economy, and to ensure their implementation.

Members of the Council

As of 17 January 2022

Professor Herta Däubler-Gmelin (Chair)
Lawyer, former Federal Minister of Justice

Photo: Klant/BMAS

Professor
Beate Beermann (Dir.)
Vice-President of the Federal Institute for Occupational Safety and Health (BAuA)

Photo: Klant/BMAS

Professor Dr Anne Riechert
Professor of Data Protection Law and Information Processing Law at the Frankfurt University of Applied Sciences

Photo: Klant/BMAS

Marit Hansen
Commissioner for Data Protection for the Land Schleswig-Holstein, holds a degree in computer science

Photo: Klant/BMAS

Benedikt Rüdesheim, LL.M.
Lawyer with dka Rechtsanwälte

Photo: Klant/BMAS

Professor Ulrich Kelber
Federal Commissioner for Data Protection and Freedom of Information

Photo: Klant/BMAS

Professor Judith Simon
Professor of Ethics in Information Technology at the University of Hamburg

Photo: UHH_Nicolai

Thomas Koczelnik
Chair of the Group Works Council of the Deutsche Post DHL Group

Photo: Klant/BMAS

Professor Jürgen Taeger (also Professor h. c.)
Of Counsel at DLA Piper LLP; previously Professor of Civil Law, Commercial and Economic Law and Legal Informatics at the Carl von Ossietzky University Oldenburg

Photo: private

Professor Rüdiger Krause
Holder of the Chair of Civil Law and Labour Law at the Georg-August University of Göttingen

Photo: Klant/BMAS

Professor Peter Wedde
Professor of Labour Law and Information Society Law at the Frankfurt University of Applied Sciences

Photo: Klant/BMAS

01/2022

www.denkfabrik-bmas.de