TECH LAW BRIEFING

Processing of employees' geo-data in Germany

It is a known fact that digitalization reaches every part of life and society, and in particular the world of employment. This leads to enormous amounts of employees' personal data being collected and processed by the employer. In particular, the use of smart (mobile) devices offers new possibilities of accessing and analysing such data by employers because very often location data ("geo-data") of the user based on internet queries or location based services are collected and automatically transmitted by smart devices. As such data allows the employer to draw his conclusions about the behaviour and social relationships of his employee, the employee's right to informational self-determination[1] may easily be affected. Thus, the employee needs to be protected from the unlawful creation of data profiles.

According to German Law the collection of geo-data by a provider of telecommunication services requires, if such data is not anonymized, the consent of the data-subject.[2] Independent of the question whether the employer can be considered as telecommunication services' provider, which may be the case when he provides his employee with the smart device and/or the technical infrastructure to use it, the validity of the employee's consent may be doubted. On the one hand, such consent must base on an informed decision which presupposes a – in most cases missing – thorough technical clarification about any personal data affecting services. In addition, the consent can be revoked at any time. On the other hand, in consideration of the structural imbalance between employer and employee the voluntariness of an employee's consent may often be questionable as it cannot be ruled out that the employee feels himself forced to consent to the data processing and therefore does not dare to deactivate the collection and transmission of geo-data on his smart device. The assessment of the voluntary nature of the employee´s consent, the dependency of the employee in the employment relationship and the circumstances under which the consent was granted must be taken into account when examining the validity of the consent. Voluntariness can exist in particular if a legal or economic advantage is achieved for the employee or if employer and employee pursue similar interests.[3] However, this has to be examined closely and, ideally, documented. If consent by the employee is deemed necessary the employer is further required to provide proof of the consent. Consent must therefore be given in writing or electronically, unless a different form is appropriate in exceptional circumstances.[4]

In default of consent the collection and processing of geo-data may be legitimized by the general permissive rule of employees' data protection law.[5] According to this, personal data of an employee may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. This requires a comprehensive weighing of interests of both parties with due regard to the purposes of the specific data processing. In respect of geo-data the rule is that employees must not be located in their protected area of life, e.g. in break, sanitary and private rooms or during permitted private use of company vehicles, and must usually not be permanently observed during their working time.[6] Any collection of geo-data outside of working hours has to be omitted. An exception may only apply if there are clearly documented indications that the employee has committed a criminal offense in the context of the employment.[7] Hence, processing and analysing employees' geo-data are limited to specific information needs of the employer for either controlling or organizational purposes, i.e. for the coordination of working processes or, in specific cases, for invoicing the client. Even in that case the storage of geo-data should always be realized in anonymous form to avoid the creation of employees' data profiles. A German court recently denied a general need for surveillance of permitted private use of company vehicles for the protection of employees.[8] The decision further states that the collection of geo-data without cause is not necessary for the operational use of company vehicles for employment related purposes. In fact, the interests of the employer, such as control of private use or protection from theft, could be encountered by less intrusive measures (like a driver´s logbook, a GPS-tracker that is manually activated in case of theft).[9]

Furthermore, the employee has to be informed about the collection and processing of his personal geo-data and the purposes of such activities, if he is not already aware of these facts anyway.[10] The consequence of lacking transparency is the employer's obligation to delete any personal data referring to such employee, and the risk of a punishment fine up to EUR 20 million or 4 % of the employer's worldwide annual turnover for an administrative offence.[11]

[1] Art. 2 (1) Grundgesetz ("GG" - Basic Law for the Federal Republic of Germany).
[2] Sec. 98 Telekommunikationsgesetz ("TKG" – Telecommunications Law).
[3] Sec. 26 (2) 1, 2 Bundesdatenschutzgesetz ("BDSG" – Federal Data Protection Act).
[4] Sec. 26 (2) 3 BDSG.
[5] Art. 88 GDPR, sec. 26 (1) BDSG.
[6] DPA North Rhine-Westphalia, 24. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: *"GPS (to determine the position of vehicles) must not be used for a seamless behavior and performance monitoring of employees."*
[7] Cf. § 26 (1) 2 BDSG.
[8] Administrative Court of Lüneburg, partial judgement of 19.3.2019 – 4 A 12/19.
[9] Cf. DPA Rhineland-Palatine on GPS-tracking, https://www.datenschutz.rlp.de/de/themenfelder-themen/gps-ortung/
[10] Art. 13 (4) GDPR.
[11] Art. 83 (5) GDPR.

Apart from this, with respect to all geo-data processing activities potential works council's rights have to be taken into account. In general, the works council has a right of co-determination in matters relating to the rules of operation and the conduct of employees in the establishment[12] and, what is even more relevant for the processing of employees' personal data, as regards the introduction and use of technical devices designed to monitor the behaviour or performance of the employees.[13] These rights remain unaffected by the data protection law provisions,[14] and already apply when the technical devices are objectively suitable to control the employees' behaviour or performance so that the surveillance only depends on the employer's volition.[15] Against this background, the processing of employees' geo-data will usually require a so-called works agreement between the works council and the employer[16] containing specific regulations on the preconditions and the scope of such data processing which may then also serve as legitimisation for the collection and analysation of geo-data by the employer.

In conclusion, no matter of the statutory basis of the data processing the general principle of data reduction and data economy must always be kept in mind. This means that any data processing activities shall pursue the aim of collecting, processing and using as little personal data as possible.[17] Concerning geo-data this can be realised best by implementing IT-systems which locate themselves and transfer the self-collected geo-data only on request of an authority or the employer in the event that he has a specific reason to access and analyse such data, and which even enable the employee to deactivate geo-tracking services.[18] Beyond that, in order to grant transparency towards the employee the employer should implement appropriate technical means,[19] e.g. an indicator light on the device when a localisation is carried out. In any case, the most effective way to cope with data protection requirements is to implement technology that operates economically with regard to the collection and processing of personal data. This is why the principle privacy by design[20] evolves into the most effective instrument of data protection in the Industry 4.0. The recent court decision also shows that the collection of geo-data must be very carefully justified in the context of a data protection impact assessment.[21] Apart from this, it is possible that a statutory clarification comes to pass in the future. The German legislator has expressively reserved the right for a statutory regulation concerning the limitation of the localization of employees.[22]

Susanne Klein
Lawyer | LL.M. | Licensed Specialist
for Information Technology Law
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Frankfurt am Main

Peter Tzschentke
Lawyer
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Frankfurt am Main

[12] Sec. 87 No. 1 Betriebsverfassungsgesetz ("BetrVG" – Works Constitution Act).
[13] Sec. 87 No. 6 BetrVG.
[14] Sec. 26 (6) BDSG.
[15] Constant jurisdiction of the German Federal Labour Court since judgement of 9.9.1975, AP BetrVG 1972 Sec. 87 Überwachung No. 2.
[16] Sec. 77 BetrVG.
[17] Art. 5 (1) c GDPR.
[18] Hofmann, "Smart factory – Employees' data protection in Industry 4.0", in DSRITB 2015, 209 (220).
[19] § 26 (5) BDSG w. Art. 5 (1) lit. a GDPR.
[20] Art. 25 (1) GDPR.
[21] Art. 35 GDPR.
[22] BT-Drs. 18/11325, 97.

Imprint

This publication is issued by
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33 | D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich/VAT Reg. No.: DE811218811

For more information see:
https://www.beiten-burkhardt.com/en/imprint

EDITOR IN CHARGE
Dr Andreas Lober | Lawyer | Partner

© BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH.
All rights reserved 2020.

PLEASE NOTE
This publication cannot replace consultation with a trained legal professional.

If you no longer wish to receive this newsletter, you can unsubscribe at any time by e-mail (please send an e-mail with the heading “Unsubscribe” to newsletter@bblaw.com) or any other declaration made to BEITEN BURKHARDT.

YOUR CONTACTS

BERLIN
Luetzowplatz 10 | 10785 Berlin
Dr Matthias Schote
Tel.: +49 30 26471-280 | Matthias.Schote@bblaw.com

DUSSELDORF
Cecilienallee 7 | 40474 Dusseldorf
Mathias Zimmer-Goertz
Tel.: +49 211 518989-144 | Mathias.Zimmer-Goertz@bblaw.com

FRANKFURT AM MAIN
Mainzer Landstrasse 36 | 60325 Frankfurt am Main
Dr Andreas Lober
Tel.: +49 69 756095-582 | Andreas.Lober@bblaw.com

MUNICH
Ganghoferstrasse 33 | 80339 Munich
Dr Axel von Walter
Tel.: +49 89 35065-1321 | Axel.Walter@bblaw.com