From Me Too to Dieselgate – No Data Protection is Protection of a Misdeed!

INTRODUCTION

Taking the example of VW & Diesel as depicted by the news media: *„The investigation and review took in all (…) members of the board of the three companies. To this end, 65 petabytes of data and a total of more than 480 million documents were transferred into data rooms. Of this, about 1.6 million files were identified as being relevant and then perused and examined, and more than 1,550 interviews and interrogations were conducted. Furthermore, the investigative files of public prosecutors, reports of the U.S. monitor and the administrative and court proceedings around the world were evaluated and taken into account.“*

COMPLIANCE VS. DATA PROTECTION– RECORD-BREAKING FINES UNDER THE GDPR

This can certainly be turned down a notch or two. At the same time, this recent example of the most comprehensive internal investigation in the history of German business casts a spotlight - in particular - on **data protection**. Compliance and the duties to investigate on the one hand, a thicket of European and national data protection regulations on the other. And if there is a violation? There is not only the threat of the inadmissibility of evidence and submitted facts – as most recently determined by the Federal Labor Court (BAG) – but also, and particularly in this day and age of ever increasing, **record-breaking fines under data protection law**, drastic liability exposure. The amount of EUR 1.12 MM which Deutsche Bahn had to pay in the early 2000's because of internal "dragnet operations" ceased to be a serious reference point by no later than the enactment of the GDPR, for these regulations call for a framework of fines of up to EUR 20 MM or 4 per cent of annual revenue, of which the authorities have made eager use.

BAG: „DATA PROTECTION IS NOT PROTECTION OF A MISDEED“

Nevertheless, the following applies: Even if data protection sets down numerous formal procedural requirements (such as general and selective duties to inform and disclose) and substantive standards (such as the requirements and content of individual investigative measures), **effective investigations** remain possible. This was noted quite emphatically by the BAG a few years ago (BAG judgment of August 23, 2018 – 2 AZR 133/18): In that case, the larceny by an employee could only be proven by evaluating video recordings after a difference in inventories was established. The problem: There was the issue of violations of the duties to delete the recordings under data protection law. The BAG ruled, however: *„The legally filmed perpetrator does not deserve protection with regard to the discovery and prosecution of his deed which can still be prosecuted under the law. He does not become worthy of protection merely due to the passage of time.“* To put it in a nutshell: **„Data protection is not protection of a misdeed“** (cf. BAG ibid). Whether or not the ECJ would concur, however, is unclear, to put it cautiously.

A LOOK INTO PRACTICAL APPLICATION: WHAT MEASURES ARE NECESSARY?

At the same time, the legal framework and appropriate sets of measures are of central significance. They commence with **general requirements** such as with respect to general compliance information (be this as an information bulletin, in employment contracts or in shop/company agreements), but other aspects, which one may not necessarily associate with this topic at first glance, may also be crucial. Of particular note is the **prohibition of the private use of email**, for this can result in the application of stricter standards under telecommunications law (currently the Telecommunications-Telemedia Data Protection Act (TTDSG), previously the Telecommunications Act (TKG)) – to the extent this is unclear between the data protection authorities (tending to yes) and the courts (tending to no), which would completely prevent internal investigations or at least slow them down considerably as a result of the link to a possible crime under Sec. 201 German Criminal Code (violation of privacy of spoken word). And to be honest: In this age of WhatsApp and other messaging tools, the practical use of personal email correspondence is pretty limited, so that this should be quite easy to explain to employees and their representatives.

Aside from this, the accompanying sets of measures necessary with a view to specific investigations can include the following aspects, depending on the scope, degree of suspicious conduct, resulting damage, etc.:

- Formal procedural requirements: They include in particular the **data protection impact assessment, involvement of the data protection officer, documentation measures, fulfillment of disclosure claims**, etc. And last, but not least, because business practice still gives this the cold shoulder: the specific **duties to inform** on the basis of the transparen-

cy requirements under Articles 13 and 14 of the GDPR; this has recently become a source of possible fines in connection with the topic of investigation compliance.

- Substantive requirements: Furthermore - and this is known to be a central issue- the substantive requirements under the GDPR/German DPA must be met under two primary aspects: The presence of **suspected misconduct** which must also be documented, that is, **"no fishing expeditions"** and – very briefly – reasonable measures equivalent to a "staircase system" of **ascending, intensifying investigative measures** with regard to the specific suspicion and the investigative objective.

Apart from this, the case law illustrates here that a mistake in business practice which gets called out is usually based on investigations which have been started despite inadequate elements of suspicion; a lot of players in business practice are a little premature here. One example: The merely **vague information** by a customer of comments made to customers about the employer that are detrimental to business does not justify the review of an email account even if this would be reasonable as such (Superior Labor Court of Hesse, judgment of September 21, 2018 – 10 Sa 601/18).

INVESTIGATION COMPLIANCE: „NO DATA PROTECTION IS PROTECTION FROM MISDEEDS"

In summary– From Me Too to the diesel scandal to whistleblower protection: It is impossible to imagine business practice in 2023 without internal investigations or without the legal framework in the sense of **Investigation Compliance**. The various regulatory levels – Europe and individual countries - as well as the various players – from the ECJ to the national labor courts and the data protection authorities- with their mostly differing views concerning the possible, secondary inadmissibility of submitted facts or the application of the TTDSG make this increasingly complex. The supplementing labor law rules such as the **two-week period for dismissals without notice** under Sec.626 (2) German Civil Code stand in an additionally tense relation to the requirements for conducting an investigation "by the book".

In the end, none of this is a help: A multitude of experiences from business practice has shown that the legal standards for investigative measures, whether large or small, are of central importance if one wants to avoid being defeated in litigation on the grounds of unfair dismissal with the employee who has been "caught out" and maybe also being exposed to damage claims and fines. Or, to paraphrase the BAG: "**No data protection is protection of a misdeed.**"

Please do not hesitate to contact us if you have questions concerning this topic. If you would like to be included in our mailing list of the subscribers to our free newsletter, please send us a brief **email** with your request.

CONTACT

Dr. Daniel Klösel
d.kloesel@justem.de

Dr. Sebastian Schulte
s.schulte@justem.de

www.justem.de