MeToo bis Dieselgate – Kein Datenschutz ist Tatenschutz!

EINFÜHRUNG

Das Beispiel VW & Diesel, ein kurzer Blick in die Presse: *„Die Untersuchung und Prüfung erstreckte sich auf alle (…) Mitglieder des Vorstands der drei Gesellschaften. Dafür wurden über 65 Petabyte Daten gesichert und insgesamt mehr als 480 Millionen Dokumente in Datenräume überführt. Davon wurden rund 1,6 Millionen Dateien als relevant identifiziert, gesichtet und überprüft sowie über 1.550 Interviews und Vernehmungen geführt. Zudem wurden staatsanwaltschaftliche Ermittlungsakten, Berichte des US-Monitors sowie behördliche und gerichtliche Verfahren weltweit ausgewertet und berücksichtigt.“*

COMPLIANCE VS. DATENSCHUTZ – REKORDBUßGELDER NACH DSGVO

Es geht sicher auch eine Nummer kleiner. Gleichwohl wirft dieses jüngste Beispiel der umfangreichsten internen Untersuchung der deutschen Wirtschaftsgeschichte ein Schlaglicht vor allem auf den **Datenschutz**. Compliance und Ermittlungspflichten auf der einen Seite, ein Dickicht europäischer und nationaler Vorschriften aus dem Datenschutz auf der anderen. Und für den Fall eines Verstoßes? Hier drohen nicht nur Beweis- bzw. „Sachvortragsverwertungsverbote“ – so zuletzt das BAG –, sondern vor allem drastische Haftungsrisiken, letzteres vor allem im Zeitalter von sich immer weiter übertreffenden **datenschutzrechtlichen Rekordbußgeldern**. Die Summe von EUR 1,12 Mio., die die Deutsche Bahn in den 2000er Jahre im Zuge interner „Rasterfahndungen“ zu zahlen hatte, liefert spätestens seit der Einführung der DSGVO keine ernsthafte Referenz mehr, denn hier ist ein Bußgeldrahmen bis zu EUR 20 Mio. oder 4 Prozent des Jahresumsatzes vorgesehen, von dem die Behörden zuletzt auch rege Gebrauch machten.

BAG: „DATENSCHUTZ KEIN TATENSCHUTZ“

Und dennoch gilt: Auch wenn der Datenschutz zahlreiche formale Verfahrensvorgaben (bspw. generelle und punktuelle Informations- und Aufklärungspflichten) und inhaltliche Maßstäbe (bspw. zu Voraussetzungen und Inhalt einzelner Ermittlungsmaßnahmen) setzt, bleiben **wirksame Ermittlungen** weiter möglich. Hierzu ganz eindringlich das BAG vor ein paar Jahren (BAG vom 23.08.2018 – 2 AZR 133/18): Hier war – nach Feststellung entsprechender Inventurdifferenzen – eine Unterschlagung seitens eines Mitarbeiters lediglich aufgrund der Auswertung von Videoaufnahmen nachweisbar. Problem: Es standen u.a. Verstöße gegen datenschutzrechtliche Löschpflichten im Raum. Das BAG allerdings: *„Der rechtmäßig gefilmte Vorsatztäter ist in Bezug auf die Aufdeckung und Verfolgung seiner materiell-rechtlich noch verfolgbaren Tat nicht schutzwürdig. Er wird dies auch nicht durch bloßen Zeitablauf.“* Oder kurz und prägnant in den Leitsätzen: **„Datenschutz ist kein Tatenschutz“** (vgl. BAG a.a.O.). Ob sich der EuGH einer derartigen Sichtweise allerdings anschließen würde, bleibt – vorsichtig ausgedrückt – unklar.

EIN BLICK IN DIE PRAXIS: WELCHE MAßNAHMEN SIND NOTWENDIG?

Gleichwohl sind der rechtliche Rahmen und entsprechende Maßnahmepakete zentral. Diese beginnen bei **generellen Vorgaben** bspw. zu allgemeinen „Compliance-Informationen“ (ob als Infoschreiben, in Arbeitsverträgen und Betriebsvereinbarungen), aber auch andere – nicht auf den ersten Blick mit diesem Thema in Verbindung zu bringende Aspekte – können wesentlich sein. Hier ist insbesondere das **Verbot der E-Mail-Privatnutzung** zu nennen, denn dieses – soweit immer noch unklar zwischen Datenschutzbehörden (Tendenz ja) und Gerichten (Tendenz nein) – kann jedenfalls zur Anwendbarkeit der schärferen telekommunikationsrechtlichen Standards (heute TTDSG, früher TKG) führen, was – infolge der Verknüpfung mit einer möglichen Straftat gem. § 201 StGB – internen Ermittlungen gänzlich entgegenstehen oder diese jedenfalls erheblich ausbremsen kann. Und hier einmal ehrlich: In Zeiten von WhatsApp & Co ist der praktische Nutzen privater E-Mail-Korrespondenz doch recht begrenzt und sollte gegenüber Mitarbeiterinnen und Mitarbeitern bzw. deren Vertretungen entsprechend gut zu erklären sein.

Zudem sind punktuell mit Blick die konkrete Ermittlung begleitende Maßnahmenpakete erforderlich, die – je nach Ausmaß, Verdachtsmoment, Schadensfolge etc. – folgende Aspekte umfassen können:

- Formale Verfahrensvorgaben: Hierbei sind insbesondere die **Datenschutzfolgenabschätzung, Einbindung der Datenschutzbeauftragten, Dokumentationsmaßnahmen, Erfüllung von Auskunftsansprüchen** etc. zu nennen. Und last but not least, weil die Praxis dies noch immer jedenfalls etwas stiefmütterlich behandelt, die konkreten **Informationspflichten** auf Basis der daten-

schutzrechtlichen Transparenzvorgaben nach Art. 13, 14 DSGVO; dies stellt in jüngster Zeit eine Quelle möglicher Bußgelder im Zusammenhang mit dem Thema Investigation Compliance dar.

- Materielle Inhaltsvorgaben: Zudem, und dies ist bekanntlich ganz zentral, muss angesichts der materiellen Vorgaben nach DSGVO/BDSG vor allem zweierlei erfüllt sein: Das Vorliegen eines im Übrigen auch zu dokumentierenden **Verdachts**, d.h. **„keine Ermittlungen ins Blaue hinein“** sowie – in aller Kürze – angemessene Maßnahmen gleichzusetzen mit einem Treppenmodell **aufsteigend intensiver Ermittlungsmaßnahmen** mit Blick auf den konkreten Verdacht und Ermittlungszweck.

Hier zeigt übrigens die Rechtsprechung, dass ein „abgestrafter“ Fehler in der Praxis vor allem darin begründet liegt, Ermittlungen trotz unzureichenden Verdachtsmomenten zu beginnen; hier sind viele Akteure in der Praxis ein wenig vorschnell. Ein Beispiel: Lediglich **vage Hinweise** eines Kunden über geschäftsschädigende Äußerungen über den Arbeitgeber gegenüber Kunden rechtfertigt nicht die Auswertung des E-Mail Accounts, selbst wenn diese an sich angemessen wäre (LAG Hessen vom 21.09.2018 – 10 Sa 601/18).

INVESTIGATION-COMPLIANCE: „KEIN DATENSCHUTZ IST TATENSCHUTZ“

Kurzum – Von MeToo über Diesel bis hin zum Hinweisgeberschutz: Internal Investigations sind im Jahre 2023 aus der Praxis nicht mehr hinwegzudenken, die rechtlichen Rahmenbedingungen im Sinne einer **Investigation Compliance** auch nicht. Die verschiedenen Regelungsebenen – Europa und Nationalstaat – sowie die unterschiedlichen Akteure – von EuGH über die nationalen Arbeitsgerichte bis hin zu den Datenschutzbehörden – sowie ihre zumeist unterschiedlichen Auffassungen bspw. zu möglichen sekundärrechtlichen Sachvortragsverwertungsverboten oder der Anwendbarkeit des TTDSG machen die Sache zunehmend komplex. Die ergänzenden arbeitsrechtlichen Regelungen bspw. zur **Zwei-Wochen-Frist** für **fristlose Kündigungen** gem. § 626 Abs. 2 BGB stehen zusätzlich in einem Spannungsfeld zu den Vorgaben einer „sauberen“ Investigation.

Aber am Ende hilft alles nichts: Hier haben vielfältige Erfahrungen aus der Praxis gezeigt, dass die rechtlichen Standards bei Ermittlungsmaßnahmen – ob groß oder klein – von zentraler Bedeutung sind, will man vermeiden, den Kündigungsschutzprozess gegen den „überführten“ Täter bzw. die „überführte“ Täterin zu verlieren und obendrein noch Schadenersatzansprüchen und Bußgeldern ausgeliefert zu sein. Oder in Anlehnung an das BAG: „**Kein Datenschutz ist Tatenschutz.“**

Zögern Sie bitte nicht, uns bei Fragen zu diesem Thema anzusprechen. Falls Sie in den Verteiler unseres kostenlosen Kanzlei-Newsletters aufgenommen werden möchten, senden Sie uns zu diesem Zweck bitte eine kurze **Mail**.

KONTAKT

Dr. Daniel Klösel
d.kloesel@justem.de

Dr. Sebastian Schulte
s.schulte@justem.de

www.justem.de