

MEMORANDUM

An: Mag Thomas Kirchner /
Wirtschaftskammer Österreich

Von: Felix Hörlsberger / DORDA
Rechtsanwälte GmbH

Betreff: DSGVO - Datenschutzbeauftragter

Datum: 19.04.2018

Unser Zeichen:
WKO-DETEKT; FH

Sehr geehrter Herr Mag Kirchner,

Sie hatten uns gebeten, dazu Stellung zu nehmen, ob ein typisches Mitgliedsunternehmen der Berufsdetektive Datenschutzbeauftragten zu bestellen hat. Dazu dürfen wir – soweit man dies in dieser Allgemeinheit tun kann – folgendes festhalten:

1. Ein Datenschutzbeauftragter ist nach Art 37 Datenschutzgrundverordnung (DSGVO) zu bestellen, wenn "die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreiche Verarbeitung besonderer Kategorien von Daten" besteht.
2. Besondere Kategorien von Daten umfasst jedenfalls auch Kundendaten, sowie Daten von Personen, die Zielobjekt einer Überwachung, eines Personenschutzauftrags oder einer Tätigkeit in einem Kaufhaus sind, sodass sich die Frage stellt, ob Berufsdetektive grundsätzlich einen Datenschutzbeauftragten zu bestellen haben.
 - 3.1 Als Auslegungshilfe für diese Frage kann die Leitlinie in Bezug auf Datenschutzbeauftragte der Art 29 Datenschutzgruppe vom 13.12.2016 idF 5.4.2017 dienen.
 - 3.1.1 Punkte 2.1.3 dieser Leitlinie nennt als Beispiele für die umfangreiche Verarbeitung (soweit hier relevant)
 - die Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines Krankenhauses

- die Verarbeitung von Reisedaten durch öffentliche Verkehrsmittel / Nachverfolgung von Netzkarten¹
- die Verarbeitung von Geolokalisierungsdaten (in bestimmten Fällen)
- die Verarbeitung von Kundendaten im gewöhnlichen Geschäftsbetrieb eines Versicherungsunternehmens oder einer Bank

3.1.2 Als Beispiele, wenn keine umfangreiche Verarbeitung vorliegen soll werden in der Leitlinie genannt:

- die Verarbeitung von Patientendaten durch einen einzelnen Arzt
- die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten durch einen einzelnen Rechtsanwalt

3.1.3. Interessanterweise stellt die Art 29 Datenschutzgruppe daher offensichtlich gerade auf die Unternehmensgröße des Verantwortlichen ab (arg: einzelner Arzt vs Krankenhaus bzw einzelner Rechtsanwalt vs Großkanzlei). Dies ist wohl praxisnahe und idR sinnvoll, hat aber keine eindeutige Grundlage in der DSGVO. UE sprechen dennoch gute Gründe dafür, diese Auslegungshilfe zu Rate zu ziehen, zumal die Art 29 Datenschutzgruppe ja gerade Auslegungshilfen für die Rechtsunterworfenen erstellen soll.

3.2 Auf Basis dieser Auslegungshilfe und unter Berücksichtigung, dass laut Ihren Angaben ein typischer Berufsdetektiv rund 100 Kundenaufträge im Jahr abwickelt, während die Kundenzahl bei einem einzelnen Arzt oder Rechtsanwalt deutlich höher liegt, wird man für ein typisches **Mitgliedsunternehmen der Berufsdetektive mit rund 100 Kundenaufträgen im Jahr mit besonderen Kategorien von Daten (sensiblen Daten bzw strafrechtlich relevanten Daten) und keinem bzw nur im Innendienst tätigen Mitarbeitern wohl auch keinen Datenschutzbeauftragten** bestellen muss.

3.3 Umgekehrt empfehlen wir jedoch, **bei (deutlicher) Überschreitung der 100 Kundenaufträge mit besonderen Kategorien von Daten (sensiblen Daten bzw strafrechtlich relevanten Daten) im Jahr und/oder wenn das Mitgliedsunternehmen der Berufsdetektive Mitarbeiter, die im Außendienst tätig sind (also etwa selbst Recherchen vor Ort oder Beschattungen vornehmen) beschäftigt, einen Datenschutzbeauftragten** zu benennen.

4. Wenn freiwillig (in den Fällen des Punktes 3.2 oben) oder verpflichtend ein Datenschutzbeauftragter bestellt wird, bedingt dies eine Reihe von Folgethemen (Organisation, Ressourcen, Stellung im Unternehmen, etc). In diesem Zusammenhang wurden wir gebeten, festzuhalten, ob der Datenschutzbeauftragte auch Entscheidungen im Unternehmen treffen kann.

¹ Wenn auch in anderen Worten

4.1 Dazu ist festzuhalten, dass die Aufgaben des Datenschutzbeauftragten nach Art 39 DSGVO folgendes umfassen:

Aufgaben des Datenschutzbeauftragten

1. Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) **Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten**, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) **Überwachung der Einhaltung dieser Verordnung**, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten **einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen**;

c) **Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz- Folgenabschätzung** und Überwachung ihrer Durchführung gemäß Artikel [35](#);

d) **Zusammenarbeit mit der Aufsichtsbehörde**;

e) **Tätigkeit als Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel [36](#), und gegebenenfalls Beratung zu allen sonstigen Fragen.

2. Der **Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung**, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

4.2 Keine dieser Aufgaben umfasst die "Entscheidung", sondern immer nur die Beratung, Überwachung, Stellungnahme etc. Daraus ist zu schließen, dass Verantwortliche und Auftragsverarbeiter grundsätzlich (zumindest) zwei Personen benötigen, die sich im Datenschutzrecht auskennen:

- denjenigen, der alles vorbereitet und dann entscheidet und
- den Datenschutzbeauftragten, der dabei berät, kontrolliert und Verbesserungsvorschläge unterbreitet.

4.3 Diese Auslegung findet sich übrigens auch in Punkt 3.5 der oben genannten Leitlinie, welche unter Berufung auf Art 38 Abs 6 DSGVO festhält, dass der Datenschutzbeauftragte zwar auch "andere Aufgaben und Pflichten wahrnehmen" kann, jedoch keine die "zu einem Interessenskonflikt führen" könnten. Ergänzt wird, dass als Faustregel Funktionen im leitenden Management, wie des Unternehmensleiters, Leiter des operativen Geschäfts, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung oder Leiter der IT-Abteilung einem Interessenskonflikt unterliegen werden. Dies gilt "auch für hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen".

4.4 Dies führt dazu, dass der Datenschutzbeauftragte auch nicht verantwortlicher Beauftragter iSd § 9 VStG für Datenschutzangelegenheiten sein kann, weil er dafür Entscheidungskompetenzen benötigt, die gerade zu dem genannten Interessenskonflikt führend würden.