DSGVO-Anforderungen an Einwilligung, Datenschutzinformation, Datenschutz-Folgenabschätzung und Bestellung von Datenschutzbeauftragten

Art 6, 9, 13, 14, 32, 35 DSGVO; DSFA-V, DSFA-AV

DSB 16. 11. 2018, D213.692/0001-DSB/2018

2019/241

1. Eine Allergie-Tagesklinik, deren Kerntätigkeit in der Diagnostik und Behandlung von Allergien – sohin in der Verarbeitung von Gesundheitsdaten nach Art 9 Abs 1 DSGVO – liegt, die ua siebzehn Ärzte beschäftigt und Gesundheitsdaten von Gesetzes wegen teilweise mindestens zehn Jahren zu speichern hat (§ 51 ÄrzteG), muss verpflichtend einen Datenschutzbeauftragten bestellen.

2. Von einer allfälligen Verpflichtung zur verschlüsselten Übermittlung kann nicht mit einer Einwilligungserklärung von betroffenen Personen abgegangen werden. Die Frage, ob eine Übermittlung in verschlüsselter oder unverschlüsselter Form erfolgt, ist eine der Datensicherheitsmaßnahmen nach Art 32 DSGVO und somit allein von der Verantwortlichen zu beurteilen.

3. Die Heranziehung von Auftragsverarbeitern ist einer Einwilligung von Betroffenen nicht zugänglich, weshalb eine diesbezügliche Einwilligung auch nicht rechtswirksam erteilt werden kann.

4. Eine „unwiderrufliche" Einwilligung widerspricht jedenfalls der DSGVO.

5. In der erteilten Information über die Datenverarbeitung („Datenschutzerklärung") ist strukturell zu unterscheiden, ob diese nach Art 13 oder Art 14 DSGVO erteilt wird, weiters darf dort kein Datenschutzbeauftragter genannt werden, wenn keiner bestellt wurde.

6. In der Datenschutzerklärung sind die einschlägigen Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten anzuführen und, wenn eine Verarbeitung auf der Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten beruht, die berechtigten Interessen, die von dem Verantwortlichen oder dem Dritten verfolgt werden, anzuführen.

7. Wird in der Datenschutzerklärung die Einwilligung als Rechtsgrundlage der Datenverarbeitung angeführt, muss darauf hingewiesen werden, dass ein Recht auf jederzeitigen Widerruf der Einwilligung besteht, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.

8. Der Ausnahmetatbestand des § 1 iVm DSFA-A12 nach der Anlage zur DSFA-AV, der von der Durchführung einer Datenschutz-Folgenabschätzung befreit, trifft nur dann zu, wenn die Datenverarbeitung von einem einzelnen Arzt geführt wird.

9. Die DSFA-AV und die DSFA-V enthalten keine abschließenden Aufzählungen, sondern führen nur Verarbeitungsvorgänge an, die jedenfalls einer oder keiner DSFA unterliegen. Ist ein Verarbeitungsvorgang nicht durch eine der beiden Verord-

nungen gedeckt, so trifft den Verantwortlichen die Pflicht, im Einzelfall zu prüfen, ob eine DSFA erforderlich ist oder nicht. Als Hilfestellung können hierzu die Leitlinien der Art-29-Datenschutzgruppe zur Datenschutz-Folgenabschätzung herangezogen werden.

1. Die Verantwortliche ist eine GmbH, ihr Geschäftszweck ist die Diagnostik und Therapie von allergischen Erkrankungen. Sie beschäftigt zum Zeitpunkt der Entscheidung drei Management-Mitarbeiter, siebzehn Ärzte, zwölf Büro- und Labormitarbeiter sowie zwei Ernährungsberater. Dabei werden regelmäßig und umfassend besondere Kategorien von Daten nach Art 9 DSGVO (Gesundheitsdaten) verarbeitet.

*2. Die Verantwortliche verwendet das Formular „Einwilligungserklärung zur Datenverarbeitung – Datenschutz-Gesetz", welches unter http://www.allergie-tagesklinik*** abgerufen und heruntergeladen werden kann und [Anm: im Kern] folgenden Inhalt aufweist:*

*„× Ich bin ausdrücklich damit einverstanden, dass personenbezogene Daten (insb Informationen über meinen Zustand bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf, meine Befunde sowie Informationen über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten) verarbeitet, gespeichert und in unverschlüsselter Form an die und von den dementsprechend relevanten Dritten geschickt werden. Die Zustimmung über den unverschlüsselten Versand kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Ich stimme weiters unwiderruflich zu, dass die Allergie-Tagesklinik D*** jederzeit andere Unternehmen und/oder Personen zur Durchführung der vereinbarten Dienstleistung heranziehen darf. Dies betrifft auch die Verarbeitung inkl Speicherung von personenbezogenen Daten. Ich nehme zur Kenntnis, dass durch die Übermittlung der Daten (unberechtigte) Dritte Kenntnis über die Informationen erhalten können und diese Daten verändert werden können. Mir ist bewusst, dass dies zur Offenlegung meines Gesundheitszustands führen kann. Mir ist bewusst, dass die Allergie-Tagesklinik D*** keinerlei Haftung für die korrekte und vollständige Übermittlung der Daten übernehmen kann."*

*3. Die Verantwortliche stellt unter http://www.allergie-tagesklinik***.at/datenschutz/ folgende Informationen zum Datenschutz zur Verfügung:*

„Datenschutzinformationen

(...)

Wer ist für die Datenverarbeitung verantwortlich und an wen können Sie sich wenden?

*Allergie-Tagesklinik D*** GmbH*
Datenschutzbeauftragter: bestellt

(...)

Für welche Zwecke und auf welcher Rechtsgrundlage werden die Daten verarbeitet?

*Die Allergie-Tagesklinik D*** verarbeitet Ihre personenbezogenen Daten im Einklang mit den Bestimmungen der DSGVO und dem Datenschutz-Anpassungsgesetz 2018:*

– zur Erfüllung von vertraglichen Pflichten (Art 5 Abs 1 b DSGVO)

Dokumentationspflicht gem § 51 ÄrzteG sowie die Erfassung sämtlicher Leistungen einschließlich automationsunterstützt erstellter und archivierter Textdokumente in diesen Angelegenheiten, etc

– zur Erfüllung rechtlicher Verpflichtungen (Art 6 Abs 1 c DSGVO)

Eine Verarbeitung personenbezogener Daten kann zum Zweck der Erfüllung unterschiedlicher gesetzlicher Verpflichtungen (Ärztegesetz, etc) oder aus steuer- sowie unternehmensrechtlichen Vorgaben erforderlich sein.

– im Rahmen Ihrer Einwilligung (Art 6 Abs 1 a DSGVO)

*Wenn Sie der Allergie-Tagesklinik D*** eine Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten erteilt haben, erfolgt eine Verarbeitung zu gemäß den in der Zustimmungserklärung festgelegten Zwecken und im darin vereinbarten Umfang. Eine erteilte Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.*

– zur Wahrung berechtigter Interessen (Art 6 Abs 1 f DSGVO).

(...)

4. Im Verzeichnis der Verarbeitungstätigkeiten der Verantwortlichen werden unter Punkt II.B. insgesamt neun Verarbeitungen angeführt: Patientenakte, Abrechnung, Befundanforderung/Befundübermittlung, Untersuchung von Proben, Organisation von Konsilien, Verwaltung von Rezepten, Hausapotheke, ELGA und Information an eigene Patienten.

Die Verantwortliche hat für keine dieser Verarbeitungstätigkeiten eine Datenschutz-Folgenabschätzung durchgeführt.

Aus den Entscheidungsgründen:

Zu Spruchpunkt 1 (verpflichtende Bestellung eines Datenschutzbeauftragten):

Verantwortliche benennen auf jeden Fall einen Datenschutzbeauftragten, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem Art 9 DSGVO besteht (Art 37 Abs 1 lit c DSGVO). (...)

Nähere Anhaltspunkte dazu, was unter einer „umfangreichen Datenverarbeitung" zu verstehen ist, finden sich in den *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"*, WP 248 Rev01 (abrufbar unter https://www.dsb.gv.at/documents/22758/112500/Leitlinien+zur+Datenschutz-Folgenabschaetzung-wp248-rev-01_de.pdf/2246301e-ffbb-4a03-bf23-797fee89174e), auf S 11:

Demnach sind folgende Kriterien zu berücksichtigen:

Im Hinblick darauf, dass

a) die Kerntätigkeit der Verantwortlichen in der Diagnostik und Behandlung von Allergien – sohin in der Verarbeitung von Gesundheitsdaten nach Art 9 Abs 1 DSGVO – liegt,

b) sie zwölf Büro- bzw Labormitarbeiter, siebzehn Ärzte und zwei Ernährungsberater beschäftigt und

c) Gesundheitsdaten von Gesetzes wegen teilweise mindestens zehn Jahren zu speichern sind (§ 51 ÄrzteG),

hätte die Verantwortliche daher zu dem Schluss kommen müssen, dass – unter Berücksichtigung der genannten Kriterien – sehr wohl eine umfangreiche Verarbeitung besonderer Kategorien von Daten nach Art 9 DSGVO besteht und deswegen verpflichtend ein Datenschutzbeauftragter bestellt werden hätte müssen.

Zu Spruchpunkt 2 (unzulässige Einwilligung):

Die von den betroffenen Personen abverlangte Einwilligung stellt sich als unzulässig heraus.

Zunächst ist der Einwilligung nicht mit der erforderlichen Klarheit zu entnehmen, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage darstellt. In der bereitgestellten Information nach Art 13 DSGVO wird als Rechtsgrundlage zwar die Einwilligung genannt, es werden jedoch auch andere Rechtsgrundlagen, wie bspw die Erfüllung rechtlicher Verpflichtungen oder die Wahrung berechtigter Interessen angeführt.

Die Verantwortliche bindet die Einwilligung zur Datenverarbeitung an eine Zustimmung zur unverschlüsselten Übermittlung von Daten, weil sie vermeint, die DSGVO statuiere eine – auch mittelbar aus den einschlägigen Regelungen nicht ableitbare – Verpflichtung, Daten verschlüsselt zu übermitteln.

Von einer allfälligen Verpflichtung zur verschlüsselten Übermittlung kann aber nicht mit einer Einwilligungserklärung von betroffenen Personen abgegangen werden. Die Frage, ob eine Übermittlung in verschlüsselter oder unverschlüsselter Form erfolgt, ist nämlich eine der Datensicherheitsmaßnahmen nach Art 32 DSGVO und somit allein von der Verantwortlichen zu beurteilen. Eine Einwilligung iSd Art 6 Abs 1 lit a bzw Art 9 Abs 2 lit a DSGVO ist schon deshalb nicht statthaft, weil die Einwilligung hier nicht dazu dient, um eine Rechtsgrundlage für die Datenverarbeitung zu schaffen, sondern um von – gegebenenfalls erforderlichen – Datensicherheitsmaßnahmen zum Nachteil von Betroffenen abweichen zu können.

In der Einwilligungserklärung wird weiters ausgeführt, dass der Betroffene „unwiderruflich" zustimmt, „dass die Allergie-Tagesklinik D*** jederzeit andere Unternehmen und/oder Personen zur Durchführung der vereinbarten Dienstleistung heranziehen darf. Diese Passage kann nur so verstanden werden, dass der Heranziehung von Auftragsverarbeitern zugestimmt wird, wofür sich die einschlägigen Regelungen in Art 28 DSGVO finden. Die Entscheidung, ob ein Auftragsverarbeiter herangezogen wird, obliegt ebenfalls allein der Verantwortlichen. Folglich ist die Heranziehung von Auftragsverarbeitern einer Einwilligung von Betroffenen nicht zugänglich, weshalb eine diesbezügliche Einwilligung auch nicht rechtswirksam erteilt werden kann.

Abschließend ist darauf hinzuweisen, dass eine „unwiderrufliche" Einwilligung jedenfalls der DSGVO widerspricht, folglich nicht verlangt werden kann (vgl dazu Art 7 Abs 3 DSGVO) und eine allfällige Einwilligung in diesem Punkt auch nicht verbindlich wäre (Art 7 Abs 2 DSGVO).

Zu Spruchpunkt 3 (Verstoß gegen die Informationspflichten):

In der erteilten Information wird strukturell nicht unterschieden, ob diese nach Art 13 oder Art 14 DSGVO erteilt wird. Diese Unterscheidung ist jedoch insofern von Bedeutung, als nach Art 14 DSGVO auch Informationen zu erteilen sind, die Art 13 DSGVO nicht abdeckt. So ist etwa nach Art 14 Abs 1 lit d die Information zu erteilen, welche Kategorien personenbezogener Daten verarbeitet werden; ebenso ist – anders als in Art 13 – auch die Information über die Herkunft der Daten zu erteilen (Art 14 Abs 2 lit f DSGVO).

Wie festgestellt, hätte die Verantwortliche einen Datenschutzbeauftragten bestellen müssen. In der erteilten Information wird W*** als Datenschutzbeauftragter genannt, obwohl er nicht als solcher bestellt wurde. Damit wird der fälschliche Eindruck erweckt, dass die Verantwortliche einen Datenschutzbeauftragten, der über sämtliche Garantien des Art 38 DSGVO verfügt, bestellt hat.

In der Datenschutzerklärung werden als Rechtsgrundlage nur „Art 5 Abs 1b" (gemeint wohl: Art 6 Abs 1 lit b) und Art 6 Abs 1 lit a, lit c und lit f DSGVO angeführt. Da die Verantwortliche aber unstrittig besondere Kategorien personenbezogener Daten nach Art 9 DSGVO (nämlich Gesundheitsdaten) verarbeitet, richtet sich die Rechtsgrundlage der Verarbeitung *dieser* Daten *ausschließlich* nach Art 9 Abs 2 DSGVO. Es ist daher Aufgabe der Verantwortlichen, zu prüfen, ob angesichts ihres Tätigkeitsfelds Art 6 DSGVO als Rechtsgrundlage für Datenverarbeitungen überhaupt einschlägig ist.

Gem Art 13 Abs 1 lit d sowie Art 14 Abs 2 lit b DSGVO hat ein Verantwortlicher, wenn die Datenverarbeitung auf Art 6 Abs 1 lit f DSGVO („Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten") beruht, die berechtigten Interessen, die von dem Verantwortlichen oder dem Dritten verfolgt werden, anzuführen.

In der Datenschutzerklärung wird die Einwilligung als eine Rechtsgrundlage der Datenverarbeitung angeführt, ohne jedoch – wie von Art 13 Abs 2 lit c bzw Art 14 Abs 2 lit d DSGVO gefordert – darauf hinzuweisen, dass ein Recht auf jederzeitigen Widerruf der Einwilligung besteht, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.

Zu Spruchpunkt 4 (Verstoß gegen die Pflicht zur Prüfung, ob eine Datenschutz-Folgenabschätzung erforderlich ist):

Die Verantwortliche führt aus, dass die Datenverarbeitung, welche in ihrem Verarbeitungsverzeichnis unter II.B. „Patientenverwaltung" firmiert, nicht einer „schriftlichen" Datenschutz-Folgenabschätzung (DSFA) zu unterziehen gewesen wäre, da der Ausnahmetatbestand des § 1 iVm DSFA-A12 nach der Anlage zur DSFA-AV zutreffe.

Dazu ist auszuführen, dass die Verantwortliche schon aus den Erläut (abrufbar auf der Website der

DSB) hätte feststellen müssen, dass die Patientenverwaltung – begrenzt auf den Gegenstand der Verwaltung der Datensätze, die üblicherweise auch bei einer Kundenverwaltung anfallen – nur dann nicht einer DSFA zu unterziehen ist, wenn sie von einem einzelnen Arzt geführt wird.

Für die Verarbeitungstätigkeiten Patientenakten; Abrechnung mit der Sozialversicherung; Befundanforderung/Befundübermittlung; Untersuchung und Versand von Proben; Verwaltung von Rezepten und Hausapotheke werden sämtliche der Verantwortlichen bekannten Gesundheitsdaten verwaltet, offengelegt und übermittelt. Somit geht schon aus dem Wortlaut des Art 35 Abs 2 lit b DSGVO klar hervor, dass in diesen Fällen die Prüfung der Notwendigkeit einer DSFA erforderlich gewesen wäre.

Nach § 2 Abs 3 Z 1 DSFA-V unterliegt die umfangreiche Verarbeitung personenbezogener Daten gem Art 9 DSGVO jedenfalls dann einer DSFA, wenn zusätzlich zumindest ein weiteres Kriterium nach Abs 3 erfüllt ist (zur „umfangreichen Verarbeitung" s nochmals die bereits oben zitierten Leitlinien zur Datenschutz-Folgenabschätzung).

Dabei ist zu berücksichtigen, dass die DSFA-AV und die DSFA-V keine abschließenden Aufzählungen enthalten, sondern nur Verarbeitungsvorgänge anführen, die *jedenfalls* einer oder keiner DSFA unterliegen. Ist ein Verarbeitungsvorgang nicht durch eine der beiden Verordnungen gedeckt, so trifft den Verantwortlichen die Pflicht, im Einzelfall zu prüfen, ob eine DSFA erforderlich ist oder nicht. Als Hilfestellung können hierzu die bereits zitierten Leitlinien zur Datenschutz-Folgenabschätzung herangezogen werden.

Es ist daher Aufgabe der Verantwortlichen, unter Zugrundelegung des oben Ausgeführten, zu prüfen, ob die hier genannten Datenverarbeitungen einer DSFA zu unterziehen sind oder nicht.

Anmerkung:

Die vorliegende E ist die bisher umfangreichste der DSB zu den Pflichten, die ein Unternehmen nach der DSGVO trifft. Ausgelöst wurde die amtswegige Untersuchung durch zwei Meldungen von Sicherheitsverletzungen („Data Breach") an die DSB, in denen sich der unterfertigende Einmelder als Datenschutz-Koordinator des Unternehmens bezeichnete, während er in der Datenschutzinformation auf der Homepage des Unternehmens, einer Allergie-Tagesklinik, als Datenschutzbeauftragter genannt wurde. Dies veranlasste die DSB nachzufragen, ob ein Datenschutzbeauftragter bestellt ist oder nicht. Der Datenschutz-Koordinator antwortete, dass er sich aufgrund von Informationen der Ärztekammer und der Wirtschaftskammer aus dem Internet nicht sicher sei, ob ein Datenschutzbeauftragter zu bestellen sei, und bat die DSB um ihre Meinung dazu. Die DSB gab ihre Meinung in Form eines Bescheids ab, in dem sie die Verletzung der Pflicht zur Nichtbestellung eines Datenschutzbeauftragten feststellte und auftrug, einen solchen binnen acht Wochen bei sonstiger Exekution zu bestellen. Das Prüfverfahren, in dem sich die DSB auch mit den Texten der Einwilligung und der Datenschutzinformation auf der Webseite des Unternehmens sehr genau befasste, endete mit der Feststellung von insgesamt 14 DSGVO-Pflichtverletzungen in den oben angeführten Bereichen.

Die E zeigt, dass sich die DSB eine eigenständige, intensive Befassung nicht nur mit der DSGVO selbst, sondern auch mit den zugehörigen österr Verordnungen und den dazu gehörenden Gesetzesmaterialien sowie den Leitlinien der Art-29-Datenschutzgruppe bzw nunmehr des Europäischen Datenschutzausschusses erwartet und ebenso, dass aus dem Ergebnis dieser Befassung dann auch die entsprechenden Handlungen abgeleitet und umgesetzt werden. Die DSB hat auch klargestellt, dass sie den Unternehmen diese eingehende Befassung mit Datenschutzrecht nicht im Verfahren abnimmt.

Laut Jahresbericht 2018 der DSB ist ein Verwaltungsstrafverfahren gegen die Allergie-Tagesklinik anhängig.

Rainer Knyrim

RA Dr. *Rainer Knyrim* ist Rechtsanwalt und Partner der Knyrim Trieb Rechtsanwälte OG.