GZ: DSB-D213.692/0001-DSB/2018 vom 16.11.2018

[Anmerkung Bearbeiter: Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen können aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein. Offenkundige Rechtschreib-, Grammatik- und Satzzeichenfehler wurden korrigiert.]

B E S C H E I D

S P R U C H

Die Datenschutzbehörde entscheidet im amtswegigen Prüfverfahren gegen die Allergie-Tagesklinik D*** GmbH (Verantwortliche) wegen Verletzungen von Pflichten nach der DSGVO wie folgt:

1. Die Verantwortliche hat gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten verstoßen.

2. Die Verantwortliche verpflichtet betroffene Personen mit dem Formular „Einwilligungserklärung zur Datenverarbeitung – Datenschutz-Gesetz“ (abrufbar unter http://www.allergie-tagesklinik***.at/wp-content/uploads/2018/08/ALTK***-DSGVO-Informationsblatt-mit-Einwilligung-20180502_2*5*.pdf) zu einer gesetzwidrigen Einwilligung, indem

    a) die Einwilligungserklärung Tatbestände erfasst, die keiner Einwilligung unterliegen, jedoch den Anschein erwecken, dass hierfür eine Einwilligung zu erteilen ist, und

    b) der Einwilligungserklärung nicht mit hinreichender Klarheit zu entnehmen ist, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage ist.

3. Die Verantwortliche hat gegen die Informationspflichten verstoßen, indem sie im „Informationsblatt zum Datenschutz“ bzw. auf ihrer Website unter http://www.allergie-tagesklinik***.at/datenschutz/

    a) nicht deutlich unterscheidet, ob die Informationen nach Art. 13 oder nach Art. 14 DSGVO erteilt werden;

    b) den Namen und die Kontaktdaten eines nicht bestellten Datenschutzbeauftragten angibt;

c) die Rechtsgrundlagen für die Verarbeitung unvollständig anführt;

d) in Bezug auf Art. 6 Abs. 1 lit. f DSGVO nicht anführt, worin die berechtigten Interessen, die von der Verantwortlichen verfolgt werden, beruhen;

e) in Bezug auf die Einwilligung nicht anführt, dass diese jederzeit widerrufen werden kann, ohne dass dadurch die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.

4. Die Verantwortliche hat gegen die Pflicht zur Prüfung der Notwendigkeit einer Durchführung von Datenschutz-Folgenabschätzungen betreffend die Verarbeitungstätigkeiten

   a) Patientenakten (Adress-, Rechnungs- und Meldedaten)

   b) Abrechnung (Abrechnung mit der Sozialversicherung)

   c) Befundanforderung/Befundübermittlung (Übermittlung und Offenlegung),

   d) Untersuchung von Proben (Untersuchung und Versand von Proben [Blut, Sekret etc.]),

   e) Verwaltung von Rezepten (Speicherung, welche Rezepte Patienten benötigen),

   f) Hausapotheke (Betrieb, Verwaltung, Abrechnung und Organisation der Hausapotheke),

   alle näher beschrieben unter II.B. im Verzeichnis der Verarbeitungstätigkeiten der Verantwortlichen, verstoßen, indem sie in unzutreffender Weise davon ausging, dass jedenfalls keine Datenschutz-Folgenabschätzungen durchzuführen sind.

5. Der Verantwortlichen wird aufgetragen, innerhalb einer Frist von acht Wochen bei sonstiger Exekution

   a) einen Datenschutzbeauftragten im Sinne der Art. 37 ff DSGVO zu bestellen und der Datenschutzbehörde zu melden;

   b) das Formular „Einwilligungserklärung zur Datenverarbeitung – Datenschutz-Gesetz“ sowie das „Informationsblatt zum Datenschutz“ bzw. die Information auf der Website http://www.allergie-tagesklinik***.at/datenschutz/ unter

Berücksichtigung der Spruchpunkte 2 und 3 dieses Bescheides rechtskonform zu gestalten; und

c) für die in Spruchpunkt 4 angegebenen Datenverarbeitungen jeweils zu prüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist und der Datenschutzbehörde diesbezüglich Meldung zu erstatten.

Rechtsgrundlagen: § 22 Abs. 1 Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 idgF; Art. 6, Art. 7 Abs. 4, Art. 9, Art. 12, Art. 13, Art. 14, Art. 35, Art. 37, Art. 57 Abs. 1 lit. h, Art. 58 Abs. 1 lit. b und Abs. 2 lit. d Datenschutz-Grundverordnung (DSGVO), ABl. Nr. L119 vom 04.05.2016, S.1; Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl. II Nr. 108/2018; Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018.

B E G R Ü N D U N G

A. Verfahrensgang

1. Die Datenschutzbehörde hat die (verpflichtenden) Eingaben der Verantwortlichen vom 18. Juni und vom 22. Juni 2018 nach Art. 33 DSGVO (Sicherheitsverletzungen) zum Anlass genommen, ein amtswegiges Prüfverfahren einzuleiten, da in den Meldungen der Verletzung der Datensicherheit jeweils lediglich ein „Datenschutz-Koordinator“ benannt wurde. Die Datenschutzbehörde ersuchte danach, dazu Stellung zu nehmen und forderte insbesondere auf,

— das Verzeichnis der Verarbeitungstätigkeiten anher zu übermitteln;

— die an die Patienten auszuhändigenden Datenschutzerklärungen anher zu übermitteln;

— bekanntzugeben, ob bzw. unter welchen Umständen Daten nicht direkt bei der betroffenen Person ermittelt werden;

— die Gründe zu nennen, warum kein Datenschutzbeauftragter benannt wurde;

— die von der Verantwortlichen durchgeführten Datenschutz-Folgenabschätzungen (DSFA) anher zu übermitteln, oder die Gründe bekannt zu geben, warum DSFA aus Sicht der Verantwortlichen unterbleiben durfte(n);

— die Gründe zu nennen, warum ein Hinweis auf Cookies unterbleiben dürfte bzw. ein Opt-Out nicht vorzusehen war;

— soweit keine DSFA vorzunehmen war, bekannt zu geben, welche Datensicherheitsmaßnahmen bestehen und welche Datenminimierungsmaßnahmen ergriffen wurden bzw. werden;

— soweit sich dies nicht aus dem Verzeichnis ergibt, die Speicherdauer der Daten bekannt zu geben und mitzuteilen, ob eine Speicherung in Cloud-Diensten oder auf Servern im EWR oder in Drittländern stattfindet;

— Auftragsverarbeiter und Übermittlungsempfänger bekannt zu geben;

— die gemäß § 30 Abs. 3 DSG und die gemäß § 9 Verwaltungsstrafgesetz 1991 (VStG) bestellte Person bekannt zu geben.

2. Mit Eingabe vom 13. August 2018 führte für die Verantwortliche aus:

„Sehr geehrter Frau V***,
sehr geehrter Herr Mag. G***,

bezugnehmend auf Ihr Schreiben vom 16.Juli 2018 darf ich wie folgt Stellung nehmen:

a) Ad Verzeichnis Verarbeitungstätigkeiten: im Anhang
b) Ad Patienten-Datenschutzerklärung: im Anhang
c) Ad Umstände: Daten werden immer direkt von der betroffenen Person ermittelt bzw. immer in Anwesenheit der Person ermittelt (wenn der/die Patient/in kein Deutsch spricht und eine/n Dolmetscher/in dabei hat oder zu jung ist und eine/n Erziehungsberechtigte/r dabei hat)
d) Ad Datenschutzbeauftragter: wir haben die Informationen (u.a. der Ärztekammer und WKO) vor dem 25.Mai 2018 so verstanden, dass Ärzte aufgrund der Kerntätigkeit keinen Datenschutzbeauftragten verpflichtend benötigen, aber freiwillig einen nehmen können. Mittlerweile lesen wir auf https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-datenschutzbeauftragter-faq.html#11 und http://www.aekwien.at/datenschutzgrundverordnung, dass wir wegen unserer Mitarbeiteranzahl wohl eher einen nehmen müssen. Wie ist hier die aktuelle Empfehlung des DSB? Benötigen wir verpflichtend einen? Wenn ja, werden wir dies klarerweise umgehend ändern. Bitte um Ihre Rückmeldung.
e) Ad DSFA: es erfolgte keine schriftliche Datenschutz-Folgeabschätzung, da dies laut http://www.aekwien.at/datenschutzgrundverordnung für die ärztliche Patientenverwaltung nicht nötig wäre (die betroffenen Datenverarbeitungen entsprechen den ausgenommenen Datenverarbeitungen gem §1 DSFA-AV, DSFA-A12). Nichtsdestotrotz gibt es eine für die Allergie-Tagesklinik erstellte „IT-Richtlinie" sowie „Risikobewertung", die den konkreten Fall (Befundübermittlung) auch benennt.
f) Ad Cookies: Wir haben einen Verweis auf Cookies auf unserer Impressum-Seite unter http://www.allergie-tagesklinik***.at/impressum/ bzw einen Hinweis-Text zum Datenschutz auf unserer Startseite unter „Hinweise für Patienten". Es wurde nun aber noch zusätzlich ein Cookie-Hinweis-Banner auf der Startseite gesetzt, per heute.
g) Ad Datensicherheitsmaßnahmen: im Anhang
h) Ad Speicherdauer: siehe Verarbeitungsverzeichnis im Anhang

i) Ad Auftragsverarbeiter: im Anhang
j) Ad ernannte Person: Die Geschäftsführerin hat Frau Dr. Flora L*** inne.

Um die Anhänge zu öffnen, bitte hier klicken sowie Vorname, Nachname und E-Mail Adresse eingeben.

Bei Fragen bin ich auch unter 06**/*9*8*7*6 erreichbar.

Lieber Gruß

Walter Ä***

Mag. Walter Josef Ä***
Datenschutz

Allergie-Tagesklinik D***
P***-Gasse 13*, A-**** D***
T: +43 (***) *44*4*23 - 5*
F: +43 (***) *44*4*23 - 3*
M: +43 (6**) *7**22*01
E-Mail: w.ae***@allergie-tagesklinik***.at
Web: www.allergie-tagesklinik***.at
Landesgericht R***, FN *4*7*2*j

B. Verfahrensgegenstand

Gegenstand der Datenschutzüberprüfung ist, ob bzw. inwiefern die Verpflichtungen der DSGVO durch die Verantwortliche eingehalten werden. Der Maßstab der Prüfung bezieht sich auf die von der Behörde vermuteten Datenschutzverletzungen und auf die Tatsachen, die durch die Überprüfung hervorgekommen sind.

C. Sachverhaltsfeststellungen

1. Die Verantwortliche ist eine GmbH mit Sitz in D***. Ihr Geschäftszweck ist die Diagnostik und Therapie von allergischen Erkrankungen, insbesondere von Kindern und Familien.

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***.at/wp-content/uploads/2018/08/ALTK***-DSGVO-Informationsblatt-mit-Einwilligung-20180502_2*5*.pdf abgerufen und heruntergeladen werden kann und folgenden Inhalt aufweist (Format nicht 1:1 wiedergegeben):

Einwilligungserklärung zur Datenverarbeitung – Datenschutz-Gesetz

Die Allergie-Tagesklinik D*** GmbH (im Folgenden Allergie-Tagesklinik D***) ist zur Verschwiegenheit verpflichtet, hat personenbezogene Daten, die ihr bei ihrer Tätigkeit bekannt werden, vertraulich zu behandeln, gemäß Datenschutz zu wahren und Dritten nur solche Informationen weiterzugeben, die zur Bearbeitung notwendig sind. Der unverschlüsselte Versand von personenbezogenen Daten (siehe Informationsblatt zum Datenschutz auf den Seiten 2 und 3) ist gemäß Europäischer Datenschutzgrundverordnung nicht erlaubt, da der Schutz und die Integrität der Daten nicht gewährleistet werden können.

Deshalb benötigt die Allergie-Tagesklinik D*** eine ausdrückliche und schriftliche Zustimmung aller Patienten und Patientinnen, um personenbezogene Daten zukünftig zu verarbeiten und unverschlüsselt zu senden und zu empfangen (Befundversand per E-Mail, telefonische Befundauskunft, etc.).

Bitte deshalb folgende ausdrückliche und schriftliche Zustimmung in Blockbuchstaben ausfüllen und unterschreiben. Pro Person – auch für Kinder – muss eine eigene Zustimmung ausgefüllt werden.

Abgeschlossen zwischen der Allergie-Tagesklinik D*** einerseits, und andererseits:

VORNAME Patient/Patientin

NACHNAME Patient/Patientin

GEBURTSDATUM (Tag, Monat, Jahr) **Telefon**

E-MAILADRESSE Patient/Patientin **Geschlecht**

× 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 Gesundheitszustandes 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, welche jenen entsprechen, die auch auf den Seiten 2 und 3 der Einwilligungserklärung abgedruckt sind:

„Datenschutzinformationen

*Der Datenschutz ist der Allergie-Tagesklinik D*** GmbH (im Folgenden Allergie-Tagesklinik D***) ein wichtiges Anliegen. Die Allergie-Tagesklinik D*** versichert Ihnen daher, dass Ihre persönlichen Daten unter Beachtung des Grundsatzes von Treu und Glauben und nur zu den nachstehend angeführten Zwecken verarbeitet werden. Die Allergie-Tagesklinik D*** bestätigt Ihnen außerdem, dass geeignete technische und organisatorische Maßnahmen getroffen wurden, um Ihre Daten zu schützen und Pflichten nach der Europäischen Datenschutzgrundverordnung (DSGVO) zu erfüllen. Im Sinne der Art.13 ff DSGVO möchte die Allergie-Tagesklinik D*** Ihnen außerdem nachstehende Informationen über die Verarbeitung Ihrer personenbezogenen Daten und über Ihre damit im Zusammenhang stehenden Rechte und Pflichten erteilen.*

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

*Allergie-Tagesklinik D*** GmbH*
*P***-Gasse 13**
***** D*****

Datenschutzbeauftragter: bestellt

Kontaktdaten des Ansprechpartners:
*Mag. Walter Josef Ä****
*w.ae***@allergie-tagesklinik***.at*

Welche Daten werden verarbeitet und aus welchen Quellen stammen diese Daten?

*Die Allergie-Tagesklinik D*** verarbeitet die personenbezogenen Daten, die die Allergie-Tagesklinik D*** im Rahmen der Geschäftsbeziehung von Ihnen erhält. Zudem verarbeitet die Allergie-Tagesklinik D*** Daten, die die Allergie-Tagesklinik D*** von Dritten (GKK, Auskunftgeber, Schuldnerverzeichnisse, etc.) und aus öffentlich zugänglichen Quellen (Firmenbuch, Medien, etc.) zulässigerweise erhalten hat.*

Zu den personenbezogenen Daten zählen Ihre persönlichen Stammdaten (Name, Adresse, Kontaktdaten, Geburtstag und -ort, Staatsangehörigkeit, gesetzl. Vertreter/Vertreterin, etc.), Legitimationsdaten (Ausweisdaten, etc.), Authentifikationsdaten, Vertragsdaten (Vertrags-/Rechtsbeziehungen, etc.), Patienteninformationen/Patientinneninformationen (Vorgeschichte von Erkrankungen, Diagnosen, Krankheitsverlauf, Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten, Terminvereinbarungen, etc.), Vertragsabrechnungs- und Zahlungsdaten (Sozialversicherungs-, Bankverbindungsdaten, etc.), Planungs- und Kontrolldaten, offengelegte Informationen (von Dritten, z.B. von öffentlichen Verzeichnissen), Bewertungsdaten, Kommunikationsinhalt, Kommunikationsmetadaten, Lebenslaufdaten, Daten zum persönlichen Leben, Informationen zu früheren Beschäftigungsverhältnissen, Informationen über religiöse oder philosophische Ansichten, Gesundheit (Untersuchung von Proben, etc.), sexuelle Orientierung, ethnische Herkunft, etc., Mitarbeiterdaten sowie Daten, die zur Erfüllung gesetzlicher und regulatorischer Aufgaben erforderlich sind.

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 1b DSGVO)*

Dokumentationspflicht gem. & 51 Ärztegesetz sowie die Erfassung sämtlicher Leistungen einschließlich automationsunterstützt erstellter und archivierter Textdokumente in diesen Angelegenheiten, etc.

- *zur Erfüllung rechtlicher Verpflichtungen (Art 6 Abs 1c 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 1a 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 1f DSGVO).*

Wer erhält Ihre Daten?

*Innerhalb der Allergie-Tagesklinik D*** erhalten diejenigen Stellen bzw. Mitarbeiter/Mitarbeiterinnen Ihre Daten, die diese zur Erfüllung der vertraglichen, gesetzlichen und aufsichtsrechtlichen Pflichten sowie berechtigten Interessen benötigen. Darüber hinaus erhalten von der Allergie-Tagesklinik D*** beauftragte Auftragsverarbeiter (IT-Dienstleister, Backofficedienstleister, etc.) Ihre Daten, sofern diese die Daten zur Erfüllung ihrer jeweiligen Leistung benötigen. Sämtliche Auftragsverarbeiter sind vertraglich entsprechend dazu verpflichtet, Ihre Daten vertraulich zu behandeln und nur im Rahmen der Leistungserbringung zu verarbeiten.*

Wie lange werden Ihre Daten gespeichert?

*Die Allergie-Tagesklinik D*** verarbeitet Ihre personenbezogenen Daten, soweit erforderlich, für die Dauer der gesamten Geschäftsbeziehung (von der Anbahnung, Abwicklung bis zur Beendigung eines Vertrags) sowie darüber hinaus gemäß den gesetzlichen Aufbewahrungs- und Dokumentationspflichten.*

Zudem sind bei der Speicherdauer die gesetzlichen Verjährungsfristen, die z.B. nach dem Allgemeinen Bürgerlichen Gesetzbuch in bestimmen Fällen bis zu 30 Jahre betragen können, zu berücksichtigen.

Welche Datenschutzrechte stehen Ihnen zu?

*Die Allergie-Tagesklinik D*** weist Sie darauf hin, dass Sie im Sinne der DSGVO jederzeit das Recht auf Auskunft Ihrer gespeicherten Daten (Art 15 DSGVO), sowie unter bestimmten Voraussetzungen das Recht auf Löschung (Art 17 DSGVO), Einschränkung (Art 18 DSGVO), Berichtigung (Art 16 DSGVO), Datenminimierung und*

*Datenübertragbarkeit (Art 20 DSGVO) sowie Widerspruch (Art 21 DSGVO) haben. Zur Ausübung Ihrer Rechte wenden Sie sich bitte an den oben angeführten Verantwortlichen. Die Allergie-Tagesklinik D*** weist außerdem darauf hin, dass Ihnen ein Beschwerderecht bei der Aufsichtsbehörde (Österreichische Datenschutzbehörde) zusteht, sollten Sie der Annahme sein, dass eine Datenschutzverletzung vorliegt. Für Fragen und Auskünfte steht die Allergie-Tagesklinik D*** Ihnen selbstverständlich jederzeit zur Verfügung.*

Sind Sie zur Bereitstellung von Daten verpflichtet?

*Im Rahmen der Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung der Geschäftsbeziehung erforderlich sind und zu deren Erhebung die Allergie-Tagesklinik D*** gesetzlich verpflichtet ist.*

Gibt es eine automatisierte Entscheidungsfindung einschließlich Profiling?

*Die Allergie-Tagesklinik D*** nutzt keine automatisierten Entscheidungsfindungen nach Art 22 DSGVO zur Herbeiführung einer Entscheidung über die Begründung und Durchführung der Geschäftsbeziehung."*

4. Im Verzeichnis der Verarbeitungstätigkeiten der Verantwortlichen werden unter Punkt II.B. insgesamt neun Verarbeitungen angeführt:

- Patientenakte,
- Abrechnung (sowohl Sozialversicherung/Privat),
- 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.

<u>Beweiswürdigung</u>: Beweise wurden aufgenommen durch die Eingaben der Verantwortlichen samt Beilagen sowie aufgrund des Amtswissens der Behörde und amtswegigen Recherchen auf der Webseite der Verantwortlichen.

D. In rechtlicher Hinsicht folgt daraus:

1. Zur Zuständigkeit der Behörde:

Jeder Aufsichtsbehörde ist es gestattet, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen (Art. 57 Abs. 1 lit. h DSGVO).

Gemäß § 18 Abs. 1 DSG ist die Datenschutzbehörde als nationale Aufsichtsbehörde nach Art. 51 DSGVO eingerichtet und berechtigt, jederzeit und ohne Angabe von Gründen Verantwortliche zu überprüfen. Die Datenschutzbehörde hat aufgrund der Angaben der Verantwortlichen in (verpflichtenden) Meldungen der Verletzung der Datensicherheit nach Art. 33 DSGVO Anlass zur Annahme gehabt, dass die Verantwortliche umfassend besondere Kategorien von Daten verarbeitet und keinen Datenschutzbeauftragten bestellt hat. Mit Erledigung vom 16. Juli 2018 leitete die Datenschutzbehörde daher ein amtswegiges Prüfverfahren ein.

2. 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 gemäß Art. 9 DSGVO besteht (Art. 37 Abs. 1 lit. c DSGVO).

Die *Leitlinien zum Datenschutzbeauftragten der Art. 29-Datenschutzgruppe* (WP 243 rev.01, abrufbar u.a. unter https://www.dsb.gv.at/europaischer_datenschutzausschuss_edsa) nehmen zwar unter 2.1.3, Seite 9, in Fußnote 14 dazu Stellung, indem im Hinblick auf eine umfangreiche Datenverarbeitung „*die Verarbeitung personenbezogener Daten […] nicht als umfangreich gelten [sollte], wenn die Verarbeitung personenbezogene Daten von Patienten oder […] betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes […] erfolgt*“.

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 Rev.01 (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 Seite 11:

Demnach sind folgende Kriterien zu berücksichtigen:

a) Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;

b) verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;

c) Dauer oder Dauerhaftigkeit der Datenverarbeitung;

d) geografisches Ausmaß der Datenverarbeitung.

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 tlw. mindestens 10 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.

Es war folglich diese Pflichtverletzung spruchgemäß festzustellen.

3. Zu Spruchpunkt 2 (unzulässige Einwilligung):

3.1. Sofern die Datenverarbeitung auf der Einwilligung einer betroffenen Person beruht, ist besonders Rücksicht darauf zu nehmen, ob die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich sind (Art. 7 Abs. 4 DSGVO).

Die Verantwortliche führt dazu in Ihrem Formular „Einwilligungserklärung zur Datenverarbeitung – Datenschutz-Gesetz“ aus:

> *„[…] Der unverschlüsselte Versand von personenbezogenen Daten (siehe Informationsblatt zum Datenschutz auf den Seiten 2 und 3) ist gemäß*

Europäischer Datenschutzgrundverordnung nicht erlaubt, da der Schutz und die Integrität der Daten nicht gewährleistet werden können.

*Deshalb benötigt die Allergie-Tagesklinik D*** eine ausdrückliche und schriftliche Zustimmung aller Patienten und Patientinnen, um personenbezogene Daten zukünftig zu verarbeiten und unverschlüsselt zu senden und zu empfangen (Befundversand per E-Mail, telefonische Befundauskunft, etc.).“*

Unter dem vom Betroffenen auszufüllenden Teil (mit Namen, Geburtsdatum und weiteren Kontaktdaten) findet sich, eingerandet und mit einem bereits vorangekreuzten Kästchen versehen, folgende Textpassage:

*„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 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 Gesundheitszustandes führen kann. Mir ist bewusst, dass die Allergie-Tagesklinik D*** keinerlei Haftung für die korrekte und vollständige Übermittlung der Daten übernehmen kann.“*

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

3.2.1. 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. Insofern ist unklar, für welche konkreten Datenverarbeitungen die Einwilligung die Rechtsgrundlage ist.

Die Einwilligungserklärung erweist sich daher in diesem Punkt als rechtswidrig (vgl. dazu auch den Bescheid der Datenschutzbehörde vom 31. Juli 2018, GZ DSB-D213.642/0002-DSB/2018; noch nicht veröffentlicht).

3.2.2. 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 alleine von der Verantwortlichen zu beurteilen. Eine Einwilligung im Sinne des 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.

Die abverlangte Einwilligung erweist sich auch aus diesem Grund als unzulässig.

3.2.3. 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. Dies betrifft auch die Verarbeitung inkl. Speicherung von personenbezogenen Daten.“

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 alleine der Verantwortlichen, die auch die Pflicht zur sorgfältigen Auswahl und zum Abschluss eines Vertrages mit bestimmtem Inhalt mit dem Auftragsverarbeiter trifft.

Folglich ist die Heranziehung von Auftragsverarbeitern einer Einwilligung von Betroffenen nicht zugänglich, weshalb eine diesbezügliche Einwilligung auch nicht rechtswirksam erteilt werden kann. Die Einwilligung erweist sich daher auch in diesem Punkt als rechtswidrig.

Abschließend ist darauf hinzuweisen, dass eine „unwiderrufliche“ Einwilligung jedenfalls der DSGVO der 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).

3.2.4. Die Einwilligungserklärung enthält auch die Passage, wonach Betroffene zur Kenntnis nehmen, „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 Gesundheitszustandes führen kann. Mir ist bewusst, dass die Allergie-Tagesklinik D*** keinerlei Haftung für die korrekte und vollständige Übermittlung der Daten übernehmen kann."

Auch hier werden wiederum Aspekte der Datensicherheit nach Art. 32 DSGVO angesprochen, von denen mittels Einwilligung zum Nachteil von Betroffenen nicht abgewichen werden kann. Es ist vielmehr die Pflicht eines Verantwortlichen adäquate Maßnahmen zu ergreifen, damit es nach allgemeinem Ermessen zu keiner Verletzung des Schutzes personenbezogener Daten kommt und folglich die Vorgaben der DSGVO eingehalten werden (Art. 24 DSGVO).

Folglich erweist sich auch dieser Teil der Einwilligungserklärung als unrechtmäßig.

4. Zu Spruchpunkt 3 (Verstoß gegen die Informationspflichten):

4.1. 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).

Nach der Rechtsprechung des EuGH (Urteil vom 1. Oktober 2015, C-201/14, noch zur Rechtslage nach der Richtlinie 95/46/EG, wobei diese Entscheidung auch für Art. 13 und 14 DSGVO Relevanz entfaltet) kommt den Informationspflichten eine wesentliche Bedeutung zu, weil der Umfang des Informationsrechts jedenfalls die Ausübung des Auskunftsrechts ermöglichen soll.

Abgesehen davon ist es aus Sicht der Betroffenen erforderlich, dass sie einer Erklärung klar und zweifelsfrei entnehmen können, welche Daten direkt bei ihnen erhoben werden und welche Daten gegebenenfalls aus anderen Quellen herangezogen werden (siehe dazu Art. 12 Abs. 1 DSGVO), woran sich aber unterschiedliche Informationspflichten knüpfen.

Indem in den Informationspflichten nicht klar zwischen den Informationspflichten nach Art. 13 und Art. 14 DSGVO unterschieden wird, hat die Verantwortliche gegen diese Pflichten sowie Art. 12 Abs. 1 DSGVO verstoßen.

4.2. Wie festgestellt, hätte die Verantwortliche einen Datenschutzbeauftragten bestellen müssen. In der erteilten Information wird Mag. Walter Josef Ä*** 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.

Dadurch hat die Verantwortliche gegen ihre Pflicht nach Art. 13 Abs. 1 lit. b sowie Art. 14 Abs. 1 lit. b iVm Art. 37 ff DSGVO verstoßen.

4.3. 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 Tätigkeitsfeldes Art. 6 DSGVO als Rechtsgrundlage für Datenverarbeitungen überhaupt einschlägig ist.

Indem die Verantwortliche es verabsäumt hat, in ihrer Datenschutzerklärung die einschlägigen Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten anzuführen, hat sie gegen ihre Pflicht nach Art. 13 Abs. 1 lit. c und Art. 14 Abs. 1 lit. c DSGVO verstoßen.

4.4. Gemäß 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.

Indem die Verantwortliche dieser Pflicht in ihrer Datenschutzerklärung nicht nachkommt, hat sie gegen die zitierten Bestimmungen der DSGVO verstoßen.

Anzumerken ist, dass diese Rechtsgrundlage ausschließlich für die Verarbeitung von Daten, die nicht unter Art. 9 DSGVO fallen, herangezogen werden kann.

4.5. 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.

Die Verantwortliche hat daher gegen die zitierten Bestimmungen verstoßen.

5. 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 erläuternden Bemerkungen (abrufbar auf der Website der Datenschutzbehörde) hätte feststellen müssen, dass die Patientenverwaltung – begrenzt auf den Gegenstand der Verwaltung der Datensätze, die üblicher Weise 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 (Adress-, Rechnungs- und Meldedaten)
- Abrechnung (Abrechnung mit der Sozialversicherung)
- Befundanforderung/Befundübermittlung (Übermittlung und Offenlegung),
- Untersuchung von Proben (Untersuchung und Versand von Proben [Blut, Sekret etc.]),
- Verwaltung von Rezepten (Speicherung, welche Rezepte Patienten benötigen),
- Hausapotheke (Betrieb, Verwaltung, Abrechnung und Organisation der 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 gemäß Art. 9 DSGVO jedenfalls dann einer DSFA, wenn zusätzlich zumindest ein weiteres Kriterium nach Abs. 3 erfüllt ist (zur „umfangreichen Verarbeitung“ siehe 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 hiezu 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.

Indem die Verantwortliche aber in unzutreffender Weise davon ausgegangen ist, dass sie jedenfalls keine DSFA durchzuführen hatte, hat sie gegen ihre Pflicht nach Art. 35 DSGVO verstoßen.

6. Zum Leistungsauftrag (Spruchpunkt 5):

Der Leistungsauftrag gründet sich auf Art. 58 Abs. 2 lit. d DSGVO. Eine Frist von acht Wochen scheint angemessen, um dem Leistungsauftrag zu entsprechen.