OGH Beschluss vom 28.1.2011, 6 Ob 255/10h – *Datenschutzrechtlicher Dienstleister*

Dienstleister iS des § 4 Z 5 DSG sind natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie Daten (nur) zur Herstellung eines ihnen aufgetragenen Werkes verwenden. Damit sind primär Dienstleister erfasst, die Dienstleistungen iS des § 153 GewO erbringen, also Gewerbetreibende, die zur Ausübung eines Gewerbes der Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik berechtigt sind.

Leitsatz verfasst von Dr. *Clemens Thiele*, LL.M.

Der Oberste Gerichtshof hat als Revisionsgericht durch den Senatspräsidenten des Obersten Gerichtshofs Hon.-Prof. Dr. Pimmer als Vorsitzenden und durch die Hofräte des Obersten Gerichtshofs Dr. Schramm, Dr. Gitschthaler, Univ.-Prof. Dr. Kodek und Dr. Nowotny als weitere Richter in der Rechtssache der klagenden Partei E*****, vertreten durch Dr. Christian Leskoschek, Rechtsanwalt in Wien als Verfahrenshelfer, gegen die beklagte Partei U***** AG, *****, vertreten durch Fellner Wratzfeld & Partner Rechtsanwälte GmbH in Wien, wegen 343.787,84 EUR sA, Feststellung (Streitwert 3.000 EUR) und Löschung (Streitwert 3.000 EUR), über die außerordentliche Revision der klagenden Partei gegen das Urteil des Oberlandesgerichts Wien als Berufungsgericht vom 30. Juni 2010, GZ 4 R 351/09f-24, den

Beschluss

gefasst: Die außerordentliche Revision wird gemäß § 508a Abs 2 ZPO mangels der Voraussetzungen des § 502 Abs 1 ZPO zurückgewiesen (§ 510 Abs 3 ZPO).

Begründung:

1. Das Berufungsgericht hat sich mit der Beweisrüge des Klägers zur Negativfeststellung betreffend die Vornahme der Eintragung in die Warnliste auseinandergesetzt und nachvollziehbare Überlegungen angestellt, sodass die Entscheidung darüber mit Revision nicht mehr angefochten werden kann (RIS-Justiz RS0043268 [T4]; RS0043371 [T21]). Soweit der Kläger unterstellt, die Eintragung in die Warnliste sei von der Beklagten vorgenommen worden, geht die Rechtsrüge nicht vom festgestellten Sachverhalt aus und ist daher insoweit nicht gesetzmäßig ausgeführt (RIS-Justiz RS0043312 [T12]).

2.1. Soweit der Kläger aus der Verwendung des Begriffs „Dienstleister“ durch die Beklagte in der Klagebeantwortung ableitet, diese hafte iSd § 33 Abs 1 DSG, weil sie als Dienstleisterin Daten schuldhaft verwendet habe, ist ihm die Begriffsbestimmung des § 4 Z 5 DSG entgegenzuhalten. Danach sind Dienstleister natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie Daten (nur) zur Herstellung eines ihnen aufgetragenen Werkes verwenden. Damit sind primär Dienstleister erfasst, die Dienstleistungen iSd § 153 GewO erbringen, also Gewerbetreibende, die zur Ausübung eines Gewerbes der Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik berechtigt sind (*Dohr/Pollirer/Weiss*, DSG^2 § 4 Anm 6). Der Begriff „Verwendung“ erfasst dabei sowohl das Verarbeiten als auch das Übermitteln von Daten iSd § 4 Z 8 DSG. § 4 Z 12 DSG definiert das Übermitteln von Daten als die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister.

2.2. Ein ausdrückliches (§ 266 ZPO) oder schlüssiges (§ 267 ZPO) Zugeständnis der Beklagten, sie habe ihr vom Auftraggeber zur Herstellung eines aufgetragenen Werkes überlassene Daten in diesem Sinne als Dienstleister verwendet (§ 4 Z 5 DSG), ist dem Prozessvorbringen der Beklagten auch nicht ansatzweise zu entnehmen.
2.3. Im Übrigen würde die Missachtung eines Tatsachengeständnisses lediglich einen Mangel des Verfahrens erster Instanz begründen (RIS-Justiz RS0040118). Unterbleibt eine entsprechende Rüge im Berufungsverfahren, kann ein solcher Mangel in dritter Instanz nicht mehr bekämpft werden (RIS-Justiz RS0043111). Vor allem aber übersieht der Kläger, dass er im Verfahren erster Instanz kein Vorbringen in diese Richtung erstattet hat. Aus diesem Grund stellt das Fehlen entsprechender Feststellungen auch keine (sekundäre) Mangelhaftigkeit des Verfahrens dar (vgl *E. Kodek* in *Rechberger*, ZPO[3] § 496 Rz 4).
3. Zusammenfassend bringt der Kläger somit keine Rechtsfragen der in § 502 Abs 1 ZPO geforderten Bedeutung zur Darstellung, sodass die Revision spruchgemäß zurückzuweisen war.

Anmerkung[*]

I. Das Problem

Das Erstgericht ist zur Negativfeststellung gelangt, dass nicht festgestellt werden konnte, dass die Vornahme der Eintragung in die Warnliste von der Beklagten erfolgt war. Den Hintergrund dürfte eine Bonitätsbeurteilung bilden, die eine Schadenersatzforderung des Klägers nach sich gezogen hatte. Die erste und zweite Instanz wiesen die Klage ab.
Aufgrund einer außerordentlichen Revision hatte sich der OGH – soweit ersichtlich – erstmals zum Begriff des Dienstleisters iS des § 4 Z 5 DSG Stellung zu nehmen.

II. Die Entscheidung des Gerichts

Der OGH lehnte eine Haftung der Beklagten nach § 33 Abs 1 DSG für die behaupteten Schäden ab, bestätigte die Klagsabweisung durch die Vorinstanzen und übernahm in seinem Zurückweisungsbeschluss den von der Datenschutzlehre[1] entwickelten Begriff des „Dienstleisters“. Im Übrigen hielt das Höchstgericht differenzierend fest, dass in diesem Zusammenhang der Begriff „Verwendung“ sowohl das Verarbeiten als auch das Übermitteln von Daten iSd § 4 Z 8 DSG erfassen würde.

III. Kritische Würdigung und Ausblick

Mit dem vorliegenden Zurückweisungsbeschluss übernimmt das zivile Höchstgericht den datenschutzrechtlichen Begriff des „Dienstleisters“ nach § 4 Z 5 DSG, der auf Art 2 lit e Datenschutz-Richtlinie (DSRL)[2] beruht. Demnach ist ein „Auftragsverarbeiter“ jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Daher sind Dienstleister natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie Daten (nur) zur Herstellung eines ihnen aufgetragenen Werkes verwenden. Damit sind primär

---

* RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), Anwalt.Thiele@eurolawyer.at; Näheres unter http://www.eurolawyer.at.
1 *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 3/45 ff; *Dohr/Weiss/Pollirer/Knyrim*, DSG[2] § 4 Anm 6.
2 RL 95/46/EG, ABl L 281, 31.

Dienstleister erfasst, die Dienstleistungen iSd § 153 GewO erbringen, also Gewerbetreibende, die zur Ausübung eines Gewerbes der Dienstleistungen in der automatischen Datenverarbeitung und Informationstechnik berechtigt sind.[3]
Bemerkenswerterweise billigt das Höchstgericht auch die Auffassung, dass vom datenschutzrechtlichen Begriff der Dienstleistung, besser „Auftragsverarbeitung", auch der Fall umfasst ist, dass ein mit der Herstellung eines Werkes Betrauter (d.h. der Dienstleister) nicht nur vom Auftraggeber überlassene Daten verwenden darf, sondern zur Herstellung des Werkes auftragsgemäß auch Daten ermitteln muss. Die Datenverwendung wird dabei iS der europarechtlichen Terminologie nach Art 2 lit a DSRL verstanden. Daher sind Daten, die der Dienstleister aus eigenem ermittelt, um das Werk zu erstellen, vom Begriff der Auftragsverarbeitung umfasst.[4] Der Daten-Dienstleister ist daher zur Speicherung und Nutzung dieser Daten sowie zu ihrer Übermittlung und ihre Aufnahme in einen Report, der zur Vorlage und zur weiten Verbreitung bestimmt ist, berechtigt.[5] Die Erhebung, Aufbewahrung und Übermittlung der personenbezogenen Daten iS des § 4 Z 1 DSG durch die mit der Auftragsverarbeitung betraute Stelle sind daher zulässig.[6] Die DSG-Novelle 2010[7] hat insoweit eine sprachliche Klarstellung des Dienstleisterbegriff in § 4 Z 5 DSG für sog. Ermittlungsdienstleister gebracht, ohne eine inhaltliche Änderung der Rechtslage zu bewirken.[8]
Lediglich wenn beauftragte Dienstleister *auf Grund* von Rechtsvorschriften oder Verhaltensregeln über die Datenverwendung eigenverantwortlich zu entscheiden haben iS des § 4 Z 4 DSG, sind sie datenschutzrechtliche Auftraggeber. Daher ist z.B. ein mit der Lohnverrechnung beauftragter Steuerberater kein datenschutzrechtlicher Auftraggeber iS des DSG 2000, weil die gesetzliche Verankerung der Eigenverantwortlichkeit fehlt.[9] Dies steht nach einem Teil der Lehre[10] der ursprünglichen Intention des Gesetzgebers entgegen, Freiberufler als datenschutzrechtliche Auftraggeber zu qualifizieren, wenn sie als Dienstleister iS des DSG 2000 tätig werden.
Ausblick: Die vorliegende Entscheidung bietet Anlass, das Verhältnis zwischen Auftraggeber und Datendienstleister näher zu erörtern. Die datenschutzrechtliche Besonderheit besteht darin, dass ein Überlassen der personenbezogenen Daten vom Auftraggeber an den Dienstleister als interne Handlung eingestuft wird, die keine Zweckbindung, sondern lediglich die vertragliche Grundlage, insbesondere die Auftragsbindung, erfordert.[11]
§ 10 Abs 1 Satz 2 DSG verpflichtet den Auftraggeber iS des § 4 Z 4 DSG, mit dem Dienstleister eine Vereinbarung über die Auftragsdatenverarbeitung abzuschließen. § 11 Abs 2 DSG empfiehlt aus Beweissicherungsgründen die Schriftlichkeit. Ungeachtet einer Vereinbarung gelten die Pflichten des Dienstleisters bereits aufgrund des Gesetzes nach den z.T. detaillierten Bestimmungen des § 11 Abs 1 Z 1 bis 6 DSG.
Besonderes Augenmerk bei der Vertragsverfassung liegt auf einer Regelung der Herausgabe der überlassenen, aber auch der ermittelten Daten mit und ohne Personenbezug. Insoweit besteht nämlich die Gefahr des sog. „**Data-Lock-In**". Da der Dienstleister idR die Infrastruktur vorgibt und physisch über die Daten auf seinen Speichereinheiten verfügt, besteht für den Auftraggeber das Risiko einen einmal gewählten Anbieter nur schwer wechseln zu können. Aufgrund der Langfristigkeit der Auftragsdatenverarbeitung kann es auch zu Software- oder Datenformatüberalterungen kommen. Die Auswahl eines

---

3 *Jahnel*, Datenschutzrecht Rz 3/46.
4 Ebenso *Jahnel*, Datenschutzrecht Rz 3/47 mwN.
5 Vgl. EuGH 20.5.2003, C-465/00 – *Österreichischer Rundfunk*, Rz 64.
6 EuGH 16.12.2008, C-524/06 – *Huber*, Rz 47.
7 BGBl I 2009/133 in Kraft ab 01.01.2010.
8 Zutreffend bereits *Jahnel*, Datenschutzrecht Rz 3/48.
9 DSK 20.5.2005, K120.862/0011-DSK/2005, RIDA 0195281.
10 *Jahnel*, Datenschutzrecht Rz 3/50, 3/53.
11 Vgl. das ausführliche Prüfungsschema von *Knyrim*, Datenschutzrecht (2003), 201 ff.

Dienstleisters sollte daher gut überlegt und auf die Bedürfnisse angepasst sein, insbesondere welche Funktionen man in die Auftragsverarbeitung auslagern will. Im günstigsten Fall führt der Data-Lock-In lediglich dazu, dass nach der Entscheidung für einen Dienstleister eine Migration eigener Daten später sehr schwierig sein könnte. Nach der bisherigen Rsp[12] zu dieser Problematik besteht mangels ausdrücklicher Vereinbarung aus § 11 Abs 1 Z 5 DSG nämlich keine Verpflichtung des Dienstleisters, die vorhandenen Daten in einem ganz bestimmten, für den Auftraggeber am besten zu handhabenden Format zu übergeben. Diese noch zur alten, aber durch die DSG-Novelle 2010 insoweit unverändert gebliebenen Datenschutzrechtslage ergangene Entscheidung bedeutet einigen Beratungsaufwand, insbesondere im Bereich des IT-Outsourcings.

Bei der Entscheidung für einen Dienstleister stellt sich auch immer die Frage, wie allfällige Risiken gedeckt werden können. Wer haftet, bei Ausfällen? Was geschieht, wenn der Dienstleister insolvent wird oder von einem anderen Anbieter übernommen wird? Wem gehören dann welche Ressourcen zu welchen Bedingungen? Wie kann ein durchgängiger Betrieb weiter geleistet werden? Wie sehen die Haftungsbedingungen aus? Bei der Auftragsverarbeitung kommt somit dem Dienstleistervertag eine zentrale Bedeutung zu. Darin sollten vor allem Themen der IT-Sicherheit und der Datenschutz geregelt sein.

Im Zuge einer Auftragsdatenverarbeitung stellt sich regelmäßig die Frage nach der Richtigstellung und **Löschung personenbezogener Daten** Betroffener. Der Dienstleister darf gemäß den Vorgaben des Auftraggebers Daten richtig stellen oder löschen, sofern der Auftraggeber dazu berechtigt ist. Der Abschluss des Dienstleistervertrages entbindet den Auftraggeber aber nicht von seinen Pflichten als datenschutzrechtlich verantwortliche Stelle.[13] Er allein bleibt auch für Ansprüche der Betroffenen aktiv legitimiert.[14]

Sofern ein Löschen personenbezogener Daten erforderlich ist, reicht nach der Rsp[15] ein bloß „logisches Löschen“ nicht aus. Um das Löschungsgebot zu erfüllen, genügt es daher nicht, die Datenorganisation so zu verändern, dass ein „gezielter Zugriff“ auf die betreffenden Daten ausgeschlossen ist. Es muss zu einem unwiderruflichen Beseitigen der Daten kommen. Die von den Gerichten klar statuierte Löschungsverpflichtung löst bei Nichtbeachtung in den Fällen der §§ 27, 28 DSG, d.h. bei verspäteter Löschung oder Nichtlöschung, nach § 52 Abs 2a DSG[16] eine Verwaltungsstrafe in Höhe von bis Euro 500,-- aus. Es liegt daher im wirtschaftlichen Interesse von Unternehmen, aber auch öffentlich-rechtlichen Auftraggebern, einer Löschung bzw. Richtigstellung nach § 27 DSG oder einem Widerspruch nach § 28 DSG umgehend – jedenfalls innerhalb der Maximalfrist von acht Wochen – durch effektives und nachhaltiges Löschen nachzukommen.

Daran anknüpfend lässt sich folgende **Checkliste für die Auftragsverarbeitung** erstellen, die keineswegs Anspruch auf Vollständigkeit erhebt und keine individuelle, anwaltliche Beratung ersetzen kann:[17]

---

[12] OGH 15.4.2010, 6 Ob 40/10s – *Datenformat*, jusIT 2010/61, 136 (*Staudegger* und *Thiele*) = RdW 2010/530, 517; dazu *Schweiger*, Dienstleistungsvertrag bei Datenverarbeitung und Verpflichtung zur Rückgabe der Daten bei Beendigung des Vertrages, lex:itec 2010 H 4, 18.

[13] Zu den Pflichten des Auftraggebers statt vieler *Jahnel*, Datenschutzrecht, Rz 3/44 ff.

[14] Vgl. OGH 19.5.2010, 6 Ob 2/10b, jusIT 2010/70, 148 (*Kastelitz/Leiter*) = ZFR 2010/143, 226 (*Ennöckl*) = RdW 2010/739, 730 = RZ 2010/EÜ 170 = ZIK 2010/375, 239 = ÖBA 2010/1678, 853 = ecolex 2010/314, 857.

[15] OGH 15.4.2010, 6 Ob 41/10p, jusIT 2010/69, 146 (*Kastelitz/Leiter*) = RdW 2010/528, 516 = ecolex 2010/315, 858 = RZ 2010/EÜ 144 = ZIK 2010/374, 238; dazu *Thiele*, Löschen heißt Vernichten. OGH erstmals zum datenschutzrechtlichen Löschungsgebot, lex:itec 2010 H 4, 20.

[16] IdF DSG-Nov 2010 für eine Säumnis seit 1.1.2010.

[17] Die von der DSK bereit gestellten Vertragsmuster unter *https://www.dsk.gv.at/site/6208/default.aspx* (10.8.2011) nehmen auf die weitere Judikaturentwicklung keine Rücksicht, sind z.T. überholt und können lediglich als Ausgangs- oder Anhaltspunkte für eine konkrete Vertragsformulierung dienen; zum selben Befund gelangen *Knyrim/Haidinger*, Cloud Computing – trübe Aussichten für ein neues Geschäftsmodell? ecolex 2011, 562, 564 lSp.

Checkliste

- Technische Details der Zusammenarbeit ermitteln und formulieren
- Umfang der Verpflichtung des Dienstleisters abklären
  - Sorgfältige **Auswahl** des Dienstleisters, z.B. mittels
    - Vorlage des Sicherheitskonzepts,
    - ggf. Nachweis der Zertifizierung (z.B. ISO 9001:2000; Datenschutzsaudit Gütesiegel; EuroPriSe)
  - **Schriftliche Beauftragung** unter Festlegung von Gegenstand, Art und Umfang der Verpflichtungen sowie der Gestattung/Festlegung etwaiger **Subdienstleister**
  - Festlegung der **Kontrollrechte** des Auftraggebers
  - Verpflichtung der zuständigen Beschäftigten vor Aufnahme ihrer Tätigkeit auf das **Datengeheimnis** (Nachweis)
- **Datenrückgabeverpflichtung** formulieren
  - die Datenherausgabe festlegen (ratsam wegen dem Problem des Data-Lock-In)
  - **Datenformat**
  - **Kosten** der Herausgabe und deren Tragung
  - Zusicherung, dass keine proprietäre Software (z.B. SAP etc) zur Übernahme/Herausgabe der Daten notwendig ist, andernfalls eine Read-Only-Lizenzvereinbarung treffen
  - Datenübergabe auch in 10 Jahren noch gewährleisten (an jeweils technischen Standard anpassen, z.B. wenn ursprüngliche s Programm „ausgelaufen“ ist)
  - Recht des Auftraggebers, auch vor Vertragsende (oder in regelmäßigen Intervallen) eine Kopie der Daten zu bekommen
- Festlegung der technisch-organisatorischen Maßnahmen bzgl. **Löschung/Richtigstellung**
  - **Löschungsverpflichtung** formulieren
  - Festlegung des Zustands, in dem sich die Datenträger befinden müssen, um als gelöscht/entsorgt gelten zu können;
  - Schriftliche Bestätigung der Durchführung der Vernichtung unter Angabe des angewendeten technischen Verfahrens (Lösch-/Entsorgungsprotokoll).
  - **Kontrolle** der Einhaltung der technischen und organisatorischen Maßnahmen durch regelmäßige Überprüfung und **Dokumentation** des Ergebnisses.
  - Regelmäßige Überprüfung des Löschkonzepts, insb. der technischen und organisatorischen Maßnahmen anhand von Schutzbedarf und aktuellem Stand der Technik.
- **Technische Details** der Zusammenarbeit ermitteln und formulieren
- **Sonst Rechtliches**
  - Rechts- und Gerichtsstandswahl: Art 23 EuGVVO beachten
  - Zugriffsverfügbarkeit festlegen: z.B. 98 % Verfügbarkeit der Dienste bedeutet einen max. Ausfall für 7,3 Tage pro Jahr
  - Data Breach-Notification nach § 24 Abs 2a DSG
  - Weiterleitungspflicht nach § 26 Abs 10 DSG
  - Internationaler Datenverkehr: u.U. genehmigungspflichtig; Safe-Harbor-Regeln beachten; §§ 12, 13 DSG
  - Haftung gegenüber Dritten: insbes. Schadenersatz nach § 33 DSG

IV. Zusammenfassung

Die vorliegende Entscheidung des OGH zeigt einmal mehr, dass das DSG 2000 massiv in die Judikatur des zivilen Höchstgerichts Eingang gefunden hat. Mit einer routinemäßigen Selbstverständlichkeit übernimmt die Rsp die von der datenschutzrechlichen Lehre entwickelten Begriffe der „Verwendung“ und des „Dienstleisters“ nach § 4 Z 5 DSG und wendet ihn auf den zu beurteilenden Sachverhalt an.