CLARA-ANN GORDON
LUISA EGLI

DATENSCHUTZ IN DER UNTERNEHMENSNACHFOLGE

Datenschutzrechtliche Herausforderungen bei Verkauf und Übernahme von KMUs

Wer ein Unternehmen übergibt oder übernimmt, denkt zuerst an Bewertung, Steuern und Vertragsgestaltung – selten an Datenschutz. Dabei erfolgt bei jeder Nachfolge auch eine Handänderung etlicher Personendaten. Treuhänderinnen und Treuhänder sind davon gleich doppelt betroffen: sowohl bei der Beratung als auch bei der Veräusserung der eigenen Unternehmen.

1. EINLEITUNG

Die Unternehmensnachfolge steht in der Schweiz hoch im Kurs: Tausende von KMUs werden in den nächsten Jahren an neue Eigentümerschaften übergehen – aus Altersgründen, aus familiären Überlegungen oder weil sich eine strategische Opportunität ergibt.

Was dabei häufig übersehen wird: Mit dem Unternehmen werden auch grosse Mengen an Personendaten übergeben. Mitarbeiterlisten, Kundendossiers, Aktienbücher – all diese Informationen gelangen im Zuge der Transaktion in neue Hände. Das stellt datenschutzrechtliche Anforderungen, die einer sorgfältigen Planung bedürfen.

Treuhänderinnen und Treuhänder sind im Zusammenhang mit der Unternehmensnachfolge gleich doppelt gefordert: einerseits in der Beratung ihrer Kundschaft und andererseits bei einer möglichen Veräusserung des eigenen Unternehmens.

2. RECHTSGRUNDLAGEN

Seit dem 1. September 2023 gilt in der Schweiz das revidierte Datenschutzgesetz (DSG), wobei die vorangehende Debatte namentlich von der Befürchtung eines unverhältnismässigen administrativen Mehraufwands für KMUs geprägt war [1]. Zu den wichtigsten Neuerungen zählen der Wegfall des Schutzes juristischer Personen, erweiterte Informations- und Auskunftspflichten, eine Meldepflicht bei Datenschutzverletzungen sowie Sanktionen von bis zu CHF 250 000 gegen fehlbare Führungspersonen [2].

Die Datenschutz-Grundverordnung (DSGVO) der EU hat für die Schweiz nur eine indirekte bzw. extraterritoriale Wirkung [3]. Das revidierte DSG wurde jedoch stark an die DSGVO angelehnt, um das Datenschutzniveau anzugleichen und den wichtigen Angemessenheitsbeschluss zu erhalten [4].

Das DSG statuiert mehrere Bearbeitungsgrundsätze, die auch im Kontext der Unternehmensnachfolge zu beachten sind:

→ Personendaten müssen rechtmässig und nach Treu und Glauben bearbeitet werden (Art. 6 Abs. 1 und 2 DSG).

→ Der Grundsatz der Zweckbindung verlangt, dass die Bearbeitung nur zu einem für die betroffene Person erkennbaren Zweck erfolgt (Art. 6 Abs. 3 DSG).

→ Die Verhältnismässigkeit gebietet, dass nur diejenigen Daten bearbeitet werden, die für den verfolgten Zweck erforderlich sind (Art. 6 Abs. 2 DSG), was insbesondere den Grundsatz der Datenminimierung einschliesst.

→ Personendaten müssen sachlich richtig sein (Art. 6 Abs. 5 DSG), und ihre Sicherheit ist durch geeignete technische und organisatorische Massnahmen zu gewährleisten (Art. 8 DSG) [5].



CLARA-ANN GORDON,
FÜRSPRECHERIN,
LL.M., PARTNERIN,
BÄR & KARRER



LUISA EGLI,
RECHTSANWÄLTIN,
LL.M., ASSOCIATE,
NIEDERER KRAFT FREY

Anders als im EU-Recht, das von einem Verbot mit Erlaubnisvorbehalt ausgeht, ist die Datenbearbeitung durch Private nach dem DSG grundsätzlich erlaubt. Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn gegen die Bearbeitungsgrundsätze verstossen wird, weil die betroffene Person beispielsweise nicht hinreichend informiert wird, oder die Bearbeitung gegen ihren ausdrücklichen Willen erfolgt (Art. 30 Abs. 2 DSG). Eine solche Verletzung ist widerrechtlich, sofern sie nicht durch Einwilligung, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (Art. 31 Abs. 1 DSG) [6]. Diese Rechtfertigungsgründe spielen bei der Unternehmensnachfolge eine zentrale Rolle, da die Weitergabe von Personendaten im Rahmen einer Due Diligence regelmässig einer solchen Rechtfertigung bedarf [7].

Darüber hinaus dürfen auch berufliche, gesetzliche oder vertragliche Geheimhaltungspflichten sowie die arbeitsrechtlichen Regelungen zur Bearbeitung von Personendaten (Art. 328*b* OR) nicht übersehen werden [8].

3. SHARE DEAL ODER ASSET DEAL?

Die gewählte Transaktionsstruktur hat einen Einfluss auf die datenschutzrechtlich relevanten Fragen. Daher ist vorab kurz auf die verschiedenen Transaktionsstrukturen einzugehen.

→ Bei einem *Share Deal* erwirbt eine Käuferin ein Unternehmen durch den Kauf der Anteile an dieser Gesellschaft (i. d. R. Aktien oder Stammanteile) [9]. Entscheidend ist, dass es dabei zu keinem Parteiwechsel kommt, da die Zielgesellschaft als Vertragspartei unverändert bestehen bleibt und die Daten ihr weiterhin allein zugeordnet sind [10].

→ Bei einem *Asset Deal* erwirbt die Käuferin das Unternehmen oder einen Teil davon durch Übernahme der dazugehörigen Aktiven, Passiven und Vertragsverhältnisse [11], worunter neben Immaterialgüterrechten, Immobilien oder Maschinen auch Kunden- und Mitarbeiterdaten fallen können. Anders als beim Share Deal kommt es dabei zu einem Parteiwechsel bei den Arbeitsverhältnissen und übrigen Verträgen, wodurch auch die Daten der Zielgesellschaft samt bisherigen Bearbeitungsgrundlagen auf die Käuferin übergehen. Dies ist bei der Beurteilung der erforderlichen Schutzmassnahmen zu berücksichtigen [12].

Bei KMUs erfolgt die Nachfolge nicht selten in Form eines Share Deal, da eine Übertragung sämtlicher Anteile administrativ einfacher ist als die Übertragung des gesamten Geschäfts. Asset Deals werden i. d. R. gewählt, wenn lediglich bestimmte Aktiven oder Passiven übernommen werden sollen [13].

4. WELCHE PERSONENDATEN WERDEN BEARBEITET?

Eine Transaktion umfasst verschiedene datenschutzrechtlich relevante Vorgänge, insbesondere die Datenweitergabe an Drittpersonen wie potenzielle Käuferinnen oder deren Berater [14]. In der Regel gibt die Zielgesellschaft dabei Personendaten an die potenzielle Erwerberin bekannt, was als Datenbearbeitung zu qualifizieren ist [15]. Relevant sind insbesondere Mitarbeiterdaten, Kundendaten, Lieferantendaten, Daten von Geschäftspartnerinnen oder -partnern und Marketingkontakten sowie Daten über Inhaberinnen oder Inhaber des Unternehmens [16].

5. DATENSCHUTZ ENTLANG DER TRANSAKTIONSPHASEN

Je nach Transaktionsphase stellen sich unterschiedliche datenschutzrechtliche Fragen – von der Vorbereitung und Due Diligence über Vertragsabschluss und Vollzug bis hin zur Integration oder einem allfälligen Abbruch der Transaktion.

5.1 Vorbereitung und Due Diligence. Die erste Phase der Transaktion umfasst die Anbahnung und Vorbereitung, wobei die Due Diligence durch die Käuferseite das entscheidende Element darstellt [17].

Gegenstand eines Unternehmenskaufs ist wirtschaftlich stets das Unternehmen selbst, weshalb sich eine umsichtige Käuferin im Vorfeld ein umfassendes Bild von dessen Verhältnissen verschaffen will (siehe Kapitel 6) [18]. Die dafür entscheidenden Daten werden regelmässig in einem zugangsbeschränkten virtuellen Datenraum zur Verfügung gestellt [19]. Solche Daten darf der Verkäufer der Käuferin nur unter den erläuterten Voraussetzungen des DSG offenlegen, wobei die Offenlegung in einem virtuellen Datenraum datenschutzrechtlich als Übermittlung zwischen zwei oder mehreren Verantwortlichen gilt [20].

In der Praxis wird zur Minimierung von Datenschutzrisiken eine stufenweise Offenlegung praktiziert [21]. Dafür sind zunächst die im Rahmen der Due Diligence offenzulegenden Unterlagen zusammenzutragen und zu ermitteln [22]. Da Treuhänderinnen und Treuhänder bei KMUs regelmässig sowohl über die operativen Datenbestände als auch über die persönlichen Verhältnisse von Gesellschafterinnen und Gesellschaftern informiert sind, kommt ihnen bei der Vorprüfung und Aufbereitung des Datenraums eine zentrale Rolle zu.

Es ist darauf zu achten, die Offenlegung während der Due Diligence auf das Erforderliche und Gerechtfertigte zu beschränken.

In der Vorbereitungsphase besteht das Risiko einer zu weitreichenden Weitergabe von Personendaten, sei es weil Käuferinnen ohne eigentlichen Kaufwillen lediglich an den Informationen interessiert sind, sei es weil das Unternehmen aus Fahrlässigkeit oder zur Erzielung eines höheren Verkaufspreises mehr Personendaten offenlegt, als erforderlich sind. Dies birgt die Gefahr, dass die potenzielle Käuferin beim Scheitern der Verhandlungen die betreffende Kundschaft oder entsprechende Mitarbeitende abzuwerben versucht.

Ausserdem stellt sich das Problem der Zweckänderung, da die betreffenden Daten ursprünglich für einen anderen Zweck erhoben wurden und nun im Rahmen der Due Diligence zweckfremd bearbeitet werden. Grundsätzlich muss die Zielgesellschaft die betroffenen Personen daher vorab über den neuen Zweck sowie die Empfängerin informieren. Die Einholung von Einwilligungen ist praktisch nicht möglich, da eine generelle, im Vorfeld erteilte Einwilligung regel-

Tabelle: **DATENSCHUTZ-DUE-DILIGENCE**

Ebenen	Aufnahme des Ist-Zustands
Datenebene	Insbesondere Übersicht über Art und Umfang der bearbeiteten Personendaten sowie Datenflüsse und IT-Landschaft
Organisationsebene	Zuständigkeiten, Datenschutzbeauftragte und Prozesse für Datenschutzverletzungen und Betroffenenanfragen, Massnahmen zur Datensicherheit, Datenschutz-Folgeabschätzungen
Dokumentenebene	Insbesondere (externe) Datenschutzerklärungen, (interne) Datenschutzreglemente, Datenaufbewahrungsreglemente, abgeschlossene Auftragsdatenbearbeitungsverträge (Data Processing Agreements), Data Sharing Agreements, Intragroup Data Transfer Agreements und EU-Standardvertragsklauseln

mässig an der fehlenden Freiwilligkeit, dem jederzeitigen Widerspruchsrecht sowie der mangelnden Konkretisierung ihres Gegenstands scheitert [23].

Es sind daher insbesondere folgende Massnahmen zu treffen [24]:

→ Personendaten sind weitgehend zu anonymisieren, pseudonymisieren oder zu aggregieren; es genügt i. d. R., Musterverträge statt detaillierter Einzelunterlagen vorzulegen.

→ Der Empfängerkreis ist einzugrenzen und der Zugang zum Datenraum bzw. auf bestimmte besonders sensitive Daten auf einen streng begrenzten Personenkreis einzuschränken (sog. Clean Room).

→ Es empfiehlt sich der Abschluss von Geheimhaltungsvereinbarungen (NDAs) sowie Auftragsdatenbearbeitungs- und Datenaustauschverträgen mit Datenraumbetreibern und potenziellen Käuferinnen.

→ Bei Käuferinnen oder Datenraumbetreibern ausserhalb des EWR sind die nötigen Massnahmen für die grenzüberschreitende Bekanntgabe zu treffen, z. B. EU-Standardvertragsklauseln in der vom schweizerischen Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) genehmigten Fassung.

→ Erwerberinnen sollten sich schliesslich verpflichten, Informationen bei Verhandlungsabbruch zu vernichten.

5.2 Vertragsabschluss und Vollzug. In einer zweiten Phase, die Zustandekommen und Vollzug des Kaufvertrags umfasst, ist die Käuferin bis zum Vollzug gleichermassen formell als Drittperson anzusehen. Ihr dürfen die Daten der Unternehmung nicht ohne Weiteres offenbart werden [25]. Auch hier besteht das Risiko, dass gegen das Zweckbindungsgebot verstossen wird oder generelle Datenschutzverletzungen auftreten.

Je nach Ergebnis der Due Diligence sollten im Kaufvertrag insbesondere Datenschutz-Gewährleistungen und Zusicherungen des Verkäufers, Schadloshaltungen sowie vor Vollzug zu implementierende Massnahmen betreffend den Datenschutz verankert werden [26].

Nach dem Erwerb sind die übernommenen Datenbestände auf Zweckvereinbarkeit zu prüfen, der Zugriff auf tatsächlich zugriffsberechtigte Mitarbeitende zu beschränken und die Betroffenen bei rechtlicher Unsicherheit über die neue Datenbearbeitung zu informieren beziehungsweise um Zustimmung zu ersuchen.

5.3 Faktische Übernahme und Integration. In der dritten Phase übernimmt die Käuferseite faktisch das Zielunternehmen. Zu beachten ist, dass das DSG kein explizites Konzernprivileg kennt; auch konzerninterne Datenweitergaben haben daher die Datenschutzgrundsätze einzuhalten [27]. Nach erfolgter Offenlegung der Transaktion sind die bestehenden Datenschutzerklärungen gegenüber Mitarbeitenden, Kundschaft und Lieferanten einzuhalten. Transition Service Agreements können einen störungsfreien Übergang sicherstellen; allenfalls sind Mitarbeitende, Kundschaft und Lieferanten aktiv über den Eigentümerwechsel zu informieren [28].

5.4 Transaktionsabbruch. Wird die Transaktion abgebrochen, ist sicherzustellen, dass die potenzielle Käuferin die im Rahmen der bisherigen Transaktionsstruktur zur Verfügung gestellten Daten unverzüglich zurückgibt bzw. löscht. Diese Pflicht ist bereits von Anfang an in der Geheimhaltungsvereinbarung festzuhalten.

6. DATENSCHUTZ-PRÜFPUNKTE

Eine Datenschutz-Due-Diligence beginnt mit der Aufnahme des Ist-Zustands auf drei Ebenen (vgl. *Tabelle*) [29].

Darüber hinaus ist festzustellen, inwiefern das Unternehmen den Datenschutz in der Vergangenheit eingehalten hat bzw. ob in der Vergangenheit Datenschutzverletzungen erfolgt sind. In diesem Zusammenhang ist relevant, ob das Unternehmen Ziel behördlicher Anfragen oder Untersuchungen im Zusammenhang mit der Einhaltung des Datenschutzes gewesen ist und allenfalls bereits entsprechende Sanktionen verhängt wurden.

Identifizierte Risiken sind zu klassifizieren: Behebbare Risiken – etwa fehlende Verträge oder Datenschutzerklärungen – lassen sich nachträglich implementieren. Nicht behebbare Risiken – etwa vergangene Datenschutzverstösse – rechtfertigen Kaufpreisanpassungen, Schadloshaltungsklauseln oder eine Versicherungslösung. Beim Share Deal ist besonders zu beachten, dass die Datenschutz-Compliance des Zielunternehmens miterworben wird; unent-

deckte Mängel können sich nach dem Vollzug als erhebliche Altlasten erweisen [30].

7. BESONDERHEITEN BEI TREUHAND-UNTERNEHMEN ALS ÜBERGABEOBJEKT

Wenn das zu übergebende Unternehmen selbst ein Treuhandbüro ist, gelten verschärfte Anforderungen. Treuhänderinnen und Treuhänder unterliegen dem Berufsgeheimnis und bearbeiten teilweise besonders schutzbedürftige Kundendaten. Es stellt sich insbesondere die Frage, ob Kundendaten ohne vorgängige Einwilligung der Kundschaft übertragen werden dürfen und wie mit laufenden Kundinnen und Kunden umzugehen ist, die der Übernahme widersprechen könnten.

In der Praxis empfiehlt sich eine frühzeitige Kommunikation mit der Kundschaft sowie eine sorgfältige Gestaltung der Übertragungsvereinbarungen zwischen abgebender und übernehmender Treuhandstelle.

8. PRAKTISCHE EMPFEHLUNGEN

Datenschutz ist in allen Phasen der Transaktion einzuhalten:
→ eine Datenschutz-Due-Diligence ist durchzuführen,
→ die Übernahme von Altrisiken ist zu vermeiden und
→ Compliance-Gewährleistungen/Zusicherungen sowie Schadloshaltungen sind im Kaufvertrag zu verhandeln.

Welche Punkte Treuhänderinnen und Treuhänder konkret berücksichtigen sollten, kann der *Infobox* entnommen werden.

Infobox: **PRAKTISCHE EMPFEHLUNGEN FÜR TREUHÄNDERINNEN UND TREUHÄNDER**

→ **Frühzeitig starten:** Datenschutz-Compliance ist keine reine Due-Diligence-Aufgabe, sondern beginnt mit der Entscheidung zur Nachfolge.
→ **Transaktionsstruktur beachten:** Share Deal und Asset Deal haben unterschiedliche datenschutzrechtliche Konsequenzen – insbesondere hinsichtlich Datentransfer, Rollenwechsel und Informationspflichten.
→ **Datenbestand prüfen:** Welche Personendaten sind vorhanden, wo liegen sie, wer hat Zugriff?
→ **Datenraum professionell gestalten:** Sicherheit, Zugriffsprotokollierung, Anonymisierung und das Need-to-know-Prinzip.
→ **NDA und Datenbearbeitungsvereinbarungen kombinieren:** Geheimhaltungsvereinbarungen sollten durch Data Processing Agreements und/oder Data Sharing Agreements ergänzt werden.
→ **Kaufvertrag absichern:** Datenschutzzusicherungen, Kaufpreisanpassungsmechanismen bei nicht behebbaren Risiken und Löschungsregelungen gehören in den Vertrag.
→ **Post-Closing berücksichtigen:** Zweckbindung bei der Datenintegration prüfen, Datenschutzerklärungen anpassen, Kundschaft und Mitarbeitende informieren.

9. FAZIT

Wer den Datenschutz bei der Unternehmensnachfolge vernachlässigt, setzt sich erheblichen Risiken aus, die sich unmittelbar auf Kaufpreis und Haftung auswirken können. Treuhänderinnen und Treuhänder sind doppelt gefordert: sowohl bei der Beratung ihrer Kundschaft als auch bei einer möglichen Veräusserung des eigenen Unternehmens. Wer Datenschutz von Beginn an als integralen Bestandteil des Nachfolgeprozesses begreift, schützt Organisation und Kundschaft vor vermeidbaren Risiken – und positioniert sich als kompetente Begleitung im heutigen Transaktionsumfeld. ■

Fussnoten: 1) Husi-Stämpfli S., Morand A.-S., Datenschutzrecht, 2. Aufl., Zürich/Genf 2024 (nachfolgend Husi-Stämpfli, Morand, N ...), N 13. **2)** Zum Ganzen Gordon C.-A., Lutz T., M&A und Datenschutz, in: Diem (Hrsg.), Mergers & Acquisitions XXII, Zürich/Basel/Genf 2021, S. 141 ff. (nachfolgend Gordon, Lutz, S. ...), S. 147. **3)** Husi-Stämpfli, Morand, N 20. **4)** Husi-Stämpfli, Morand, N 11. **5)** Vgl. auch Dal Molin L., Mattle K., Datenschutz in M&A-Transaktionen, in: Dal Molin, Wesiak-Schmidt (Hrsg.), Datenschutz im Unternehmen, Zürich/St. Gallen 2023 (nachfolgend Dal Molin, Mattle, § 9 N ...), § 9 N 12. **6)** Vgl. Husi-Stämpfli, Morand, N 293 ff. **7)** Vgl. Gordon, Lutz, S. 149 ff. **8)** Dal Molin, Mattle, § 9 N 14. **9)** Tschäni R., Diem H.-J., Wolf M., M&A Transaktionen nach Schweizer Recht, 2021 (nachfolgend Tschäni, Diem, Wolf, Rz. ...), Rz. 131 ff. **10)** Winkler M., Datenschutz bei M&A Transaktionen, GesKR 2018, S. 124 ff. (nachfolgend Winkler, S. ...), S. 127. **11)** Tschäni, Diem, Wolf, Rz. 194 ff. **12)** Winkler, S. 128. **13)** Tschäni, Diem, Wolf, Rz. 195. **14)** Gordon, Lutz, S. 149. **15)** Mathys R., Triebold O., Deals, Daten, Datenschutz, in: Olano (Hrsg.), Jurisprudenz und Musik, Liber amicorum für Felix H. Thomann zum 80. Geburtstag, Zürich 2016, 51 ff. (nachfolgend Mathys, Triebold, S. ...), S. 61 f. **16)** Vgl. Gordon, Lutz, S. 149. **17)** Winkler, S. 153 f. **18)** Winkler, S. 125. **19)** Winkler, S. 126. **20)** Vgl. Gordon, Lutz, S. 154 f. **21)** Winkler, S. 153 f. **22)** Gordon, Lutz, S. 157. **23)** Gordon, Lutz, S. 158 ff.; Mathys, Triebold, S. 63. **24)** Vgl. auch Dal Molin, Mattle, § 9 N 24 f. sowie 35 ff. **25)** Winkler, S. 125, 131. **26)** Vgl. Dal Molin, Mattle, § 9 N 71 ff. **27)** Winkler, S. 132. **28)** Gordon, Lutz, S. 161. **29)** Vgl. auch Dal Molin, Mattle, § 9 N 56 ff. **30)** Gordon, Lutz, S. 144; Mathys, Triebold, S. 55.