

Datenschutzrechtliche Due Diligence: Teil I

Dr. Lukas Lezzi, Rechtsanwalt, Meyerlustenberger Lachenal AG (Zürich)

Dr. Christian Kunz, Rechtsanwalt, LL.M., Bär & Karrer AG (Zürich)

Jutta Sonja Oberlin, PwC (Zürich)

Es empfiehlt sich, abhängig von der allgemeinen datenschutzrechtlichen Risikoeexposition des Zielunternehmens und den Erwartungen der Klienten, eine im Einzelfall sinnvolle Auswahl von Fragen zu treffen und den Umfang der Prüfung im Due-Diligence-Bericht darzulegen. In der Regel müssen darin nicht alle resultierenden Erkenntnisse detailliert enthalten sein, sondern eine konzise Darstellung der identifizierten Red Flags einschliesslich Priorisierung und möglicher Lösungsansätze. Gestützt darauf können technische, organisatorische oder vertragliche Massnahmen getroffen werden. Zehn Themenblöcke helfen bei der systematischen Prüfung. Teil I enthält die ersten sechs.

Zu den Autoren

Dr. Lukas Lezzi, Rechtsanwalt, CIPP/E, hat Rechtswissenschaften studiert und im Finanzmarktrecht promoviert. Zurzeit arbeitet er als Associate bei Meyerlustenberger Lachenal AG in Zürich, hauptsächlich im Bereich des Finanzmarktrechts.

Dr. Christian Kunz, Rechtsanwalt, LL.M., hat sich auf interne Untersuchungen, grenzüberschreitende Verfahren, Datenschutzrecht und private M&A-Transaktionen spezialisiert. Er arbeitet als Senior Associate bei Bär & Karrer AG in Zürich.

Jutta Sonja Oberlin, CIPP/E, CIPM, arbeitet als Manager im Bereich Regulatory Compliance bei der PwC in Zürich. Zudem ist sie Mitglied der IAPP Leadership Community und engagiert sich in der Schweiz als Young Privacy Professional Lead.



Der Datenschutz hat in jüngerer Zeit auch im Rahmen von M&A-Transaktionen an Bedeutung gewonnen. Die Prüfung der datenschutzrechtlichen Compliance des Zielunternehmens gehört heute zum Standard einer sorgfältigen Due Diligence. Was müssen Personen, welche mit der Prüfung der datenschutzrechtlichen Compliance befasst sind, konkret beachten? Im Folgenden finden Sie eine Orientierungshilfe, mit der die wichtigsten Punkte systematisch abgefragt und geprüft werden können. Diese Orientie-

rungshilfe richtet sich nach dem Standard der europäischen Datenschutz-Grundverordnung (DSGVO) und des schweizerischen Datenschutzgesetzes (DSG).

Grobanalyse der Datenverarbeitungen

Zu Beginn ist das Unternehmensumfeld der Zielgesellschaft einschliesslich allfälliger Tochtergesellschaften zu prüfen, um die Funktion der einzelnen Gesellschaften innerhalb der Gruppe zu verstehen. Zu er-

mitteln ist etwa, ob eine Gesellschaft für die gesamte Gruppe zentrale Dienstleistungen wie z.B. HR oder Marketing erbringt. Dies erlaubt grob einzuschätzen, welche Gruppengesellschaft welche Art von Personendaten bearbeitet, ob von einer Gruppengesellschaft u.U. spezielle Kategorien von Daten bearbeitet werden und wie die internen und externen Datenflüsse aussehen (Data Mapping). Zudem lässt das Data Mapping erkennen, ob neben der DSGVO bzw. dem DSG lokales ausländisches Datenschutzrecht zur Anwendung kommt.

Prüfung Datenverarbeitungsvorgänge

Ausgehend vom bereits durchgeführten Data Mapping bezieht sich die Prüfung, soweit vorhanden, auf Verzeichnisse der Verarbeitungsvorgänge, durchgeführte Datenschutz-Assessments inkl. Templates, Projektpläne zum Stand der Umsetzung der rechtlichen Anforderungen des Datenschutzes und Prozessbeschreibungen.

Die relevanten Fragen lauten:

- Sind die zwingenden Informationen in den Verzeichnissen der Verarbeitungsvorgänge und Templates der Datenschutz-Assessments in der nötigen Granularität enthalten?
- Ist die Risikoevaluation in den durchgeführten Assessments verhältnismässig, nachvollziehbar und in den zu treffenden/ getroffenen Massnahmen zu erkennen?
- Welche Arten von Personendaten werden bearbeitet? Wenn Persönlichkeitsprofile erstellt oder spezielle Kategorien von Daten (nach DSG: besonders schützenswerte Personendaten) bearbeitet werden, sind die damit verbundenen weitergehenden Pflichten erfüllt?
- Sind die Rechtsgrundlagen für die jeweilige Datenverarbeitung vorhanden und entsprechend dokumentiert?
- Benötigen die Datenverarbeitungsprozesse eine Einwilligung der Betroffenen? Falls ja, werden diese rechtsgültig eingeholt, dokumentiert und die Betroffenenrechte gewährleistet? Wird auch der allfällige Rückzug einer Einwilligung dokumentiert?

- Hat das Zielunternehmen Datensammlungen, bei denen regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden oder Personendaten an Dritte bekannt gegeben werden, an den EDÖB gemeldet? Falls nein, ist ein gesetzlicher Ausnahmetatbestand erfüllt?

Red Flags:

- Lückenhafte bzw. nicht vorhandene Dokumentation.
- Nichtvorhandensein von «Grundlagendokumenten» bzw. gesetzlich vorgeschriebenen Dokumenten, wie z.B. dem Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).

Prüfung Organisation

Für die Due Diligence ist vom Zielunternehmen die Offenlegung aller vorhandenen datenschutzrechtlichen Dokumente zu verlangen. Dazu gehören namentlich die interne, externe und Arbeitnehmer-Datenschutzrichtlinie, die Archivierungspolicy, alle weiteren Weisungen zum Datenschutz-/ Risk-Management, IT/Cybersecurity, Change-Management, Organisationsreglemente, Organigramme, Code of Conduct, Auftragsverarbeitungsverträge und Berichte der internen oder externen Revision.

Red Flags:

- Die internen datenschutzrechtlichen Dokumente sind unvollständig.
- Sind die Berichte der internen und/oder externen Revision offensichtlich fehler- oder lückenhaft?

Datenschutz-Governance

Sodann ist zu eruieren, ob das Zielunternehmen den Datenschutz systematisch in die Prozesse integriert hat und klar geregelt ist, wer für die Einhaltung der gesetzlichen Vorgaben verantwortlich ist. Insbesondere sind regelmässig die Berichte der internen oder externen Revision zu konsultieren.

Die relevanten Fragen lauten:

- Sind Verantwortlichkeiten und Zuständigkeiten klar geregelt?



Achtung

Bei der Prüfung der Dokumente ist der Grösse, der Komplexität und der datenschutzrechtlichen Risikoexposition des Unternehmens sowie der Art und dem Zweck der Datenbearbeitungsaktivitäten Rechnung zu tragen. Fragestellung: Sind alle der Grösse, der Komplexität und der datenschutzrechtlichen Risikoexposition sowie der Art und dem Zweck der Datenbearbeitungsaktivitäten angemessenen Dokumente vorhanden?



Wichtig ist bei der Prüfung von Personendaten, dass die internen Weisungen Regeln für den Umgang mit Personendaten und Klassifizierungen der vom Unternehmen bearbeiteten Daten enthalten und dass für jede dieser Kategorien klare Handlungsanweisungen gemacht und Sicherheitsanforderungen definiert werden.

- Gibt es, falls notwendig, einen fachlich qualifizierten und unabhängigen Datenschutzbeauftragten mit entsprechendem Pflichtenheft und ist dieser beim EDÖB gemeldet und in der EU bei der zuständigen Aufsichtsbehörde registriert?
- Sind Prozesse zur Berücksichtigung des Datenschutzes bei neuen bzw. veränderten Datenverarbeitungsaktivitäten vorhanden? Ist sichergestellt, dass die internen Datenschutzverantwortlichen dabei frühzeitig involviert werden?
- Gibt es eine klare Weisung für den Umgang und die Durchführung von Datenschutz-Folgenabschätzungen gemäss Art. 35 DSGVO?
- Gibt es eine Liste mit den implementierten technischen und organisatorischen Massnahmen (TOMs)? Falls ja, sind die TOMs angemessen umgesetzt? Für diese Prüfung müssen IT- und IT-Security-Experten beigezogen werden.
- Sind Prozesse zur Einhaltung des Datenschutzes bei Outsourcing-Projekten vorhanden?
- Ist das Zielunternehmen verpflichtet, einen EU-Vertreter zu ernennen? Falls ja, gibt es einen schriftlichen Vertrag zwischen dem Zielunternehmen und dem EU-Vertreter?
- Werden Mitarbeiter des Zielunternehmens, insbesondere jene in Funktionen mit erhöhter datenschutzrechtlicher Risikoexposition (wie z.B. HR), geschult? Falls ja, werden diese Schulungen dokumentiert?

Red Flags:

- Keine Regelung der Verantwortlichkeit für Datenschutz.
- Fehlen eines Datenschutzbeauftragten trotz Pflicht dazu.
- Keine systematische Einbindung des Datenschutzes in Prozesse.
- TOMs sind nicht vorhanden bzw. nicht angemessen.

Umgang mit Personendaten

Die relevanten Fragen lauten:

- Sind klare Regeln für die Klassifizierung und den Umgang mit Personendaten vorhanden?
- Falls das Zielunternehmen Daten bearbeitet, die durch andere Gesetze als Datenschutzgesetze geschützt sind (z.B. Bankkundendaten), gibt es für diese Daten ein spezielles Schutzkonzept?

Red Flags:

- Keine spezifischen internen Regeln für die Bearbeitung von Personendaten, die einem Berufsgeheimnis unterstehen.
- Keine spezifischen Regelungen für speziell zu schützende Personendaten.

Datenverlust

Das Zielunternehmen sollte technische und organisatorische Massnahmen implementiert haben, damit Datenverluste festgestellt werden können und es entsprechend auf solche Vorkommnisse reagieren und vor allem die Daten unter Umständen wiederherstellen kann.

Die relevanten Fragen lauten:

- Sind interne Prozesse zur Entdeckung von Datenlecks und Vorgehensweisen bei Datenverlusten vorhanden, insbesondere in Bezug auf die Meldung innert der gesetzlichen Frist an die Aufsichtsbehörde?
- Gab es bereits Datenverluste? Wenn ja, welche und wie viele?

Red Flags:

- Wiederholte Datenverluste oder unberechtigte Zugriffe in den letzten zwei Jahren vor der Prüfung, insb. wenn die Ursachen nicht aufgearbeitet worden sind.
- Nicht datenschutzkonforme Abwicklung eines eingetretenen Datenverlusts (z.B. keine Meldung an die zuständige Aufsichtsbehörde oder gar, trotz Pflicht, keine Benachrichtigung der betroffenen Personen).

Teil II folgt in RR-COMP 2020 Nr. 6.