CB-BEITRAG

Dr. Lukas Lezzi, RA, CIPP/E, Dr. Christian Kunz, RA, LL. M., und Jutta Sonja Oberlin, LL. M., CIPP/E, CIPM

Die datenschutzrechtliche Due Diligence: Ein praxisorientierter Leitfaden

Der vorliegende Beitrag ist an Personen gerichtet, die sich mit der Prüfung der datenschutzrechtlichen Compliance von Unternehmen, insbesondere im Zuge von M&A-Transaktionen, befassen. Dem Leser soll ein Leitfaden an die Hand gegeben werden, mit dem die aus Sicht der Autoren wichtigsten Punkte systematisch abgefragt und geprüft werden können. Die Prüfpunkte sind nach Themenkreisen gegliedert und mit Red Flags ergänzt, wie sie nach Erfahrung der Autoren bei datenschutzrechtlichen Due Diligence-Prüfungen häufig identifiziert werden. Grundsätzlich richtet sich dieser Leitfaden nach dem Standard der EU-Datenschutz-Grundverordnung (DSGVO). Wo sinnvoll wird auch auf das geltende und künftige Schweizer Recht (DSG und revDSG) Bezug genommen, insbesondere bei den Ausführungen zur grenzüberschreitenden Datenübermittlung. Zu beachten ist, dass das geltende DSG einen geringeren Datenschutzstandard als die DSGVO aufweist, aber im Gegensatz zur DSGVO auch die Personendaten von juristischen Personen schützt. Mit der Revision des DSG wird ein dem der DSGVO gleichwertiger Schutzstandard eingeführt, aber gleichzeitig auf den Schutz von Personendaten juristischer Personen verzichtet.

I. Einleitende Bemerkungen

Während die datenschutzrechtliche Compliance des Zielunternehmens vor einigen Jahren im Zuge der Due Diligence-Prüfung (DD) bei einer M&A-Transaktion kaum geprüft wurde und sich bestenfalls darauf beschränkte, die Verkäuferin gewährleisten zu lassen, dass das Zielunternehmen die anwendbaren Datenschutzgesetze einhält, hat der Datenschutz in jüngerer Zeit auch im Rahmen von M&A-Transaktionen an Bedeutung gewonnen. Es gehört heute zum Standard einer sorgfältigen DD, die datenschutzrechtliche Compliance des Zielunternehmens vertieft zu prüfen. Keinen nennenswerten Einfluss auf die datenschutzrechtliche DD hat die Strukturierung der Transaktion als Share Deal (Kauf der Aktien eines Unternehmens) oder Asset Deal (Kauf von Aktiven und ggf. Passiven eines Unternehmens), jedenfalls wenn bei einem Asset Deal ein Unternehmen oder ein Teil davon gekauft wird. Für die datenschutzrechtliche DD ist eine strukturierte Vorgehensweise, wie sie in vorliegendem Leitfaden erläutert wird, angezeigt.

II. Leitfaden

1. Grobanalyse der Datenverarbeitungen

Als Grundlage für die datenschutzrechtliche DD ist es unabdingbar, das Geschäft des zu prüfenden Zielunternehmens und, sofern auch dessen Tochtergesellschaften oder andere verbundene Gesellschaften gekauft werden, auch das Geschäft dieser Gruppengesellschaften und deren Funktion innerhalb der Gruppe zu verstehen. Zu ermitteln ist etwa, ob eine Gruppengesellschaft für die gesamte Gruppe Forschung und Entwicklung betreibt oder HR-, Marketing- oder ähnliche Dienstleistungen, die mit einer erhöhten datenschutzrechtlichen Risikoexposition verbunden sind, erbringt.

Hilfreich sind dafür Dokumente, deren Offenlegung für die DD regelmäßig ohnehin von der Verkäuferin verlangt wird, namentlich der Group Chart, der Jahresbericht und die Funktionsbeschreibungen der einzelnen Gruppengesellschaften.

Gestützt darauf kann grob beurteilt werden, welche Gruppengesellschaft welche Art von Personendaten verarbeitet, ob eine Gruppengesellschaft vermutlich besonders schützenswerte Personendaten verarbeitet und welche internen und externen Datenflüsse vorhanden sind (sog. Data Mapping). Dies wiederum erlaubt es, bei der folgenden datenschutzrechtlichen DD risikobasierte Schwerpunkte zu setzen.

Zudem lässt das Data Mapping erkennen, ob neben der DSGVO lokales Datenschutzrecht zur Anwendung kommt und dessen Einhaltung im Rahmen der DD daher ebenfalls zu prüfen ist. Zu denken ist beispielsweise an den Fall, in dem eine gruppeninterne Service-Gesellschaft mit Sitz in Deutschland HR-Dienstleistungen für eine Gruppengesellschaft mit Sitz in Singapur erbringt. In diesem Fall ist neben der DSGVO auch das singapurische Datenschutzrecht zu beachten.

Schließlich sollte auch ein Inventar über die eingesetzten IT-Applikationen eingefordert werden. Auf diese Weise können die einzelnen Applikationen bestimmt und zudem auch die Schnittstellen inner- und außerhalb der Applikationslandschaft des Zielunternehmens (Application Programming Interfaces, APIs) erkannt werden.

2. Prüfung der Datenverarbeitungsvorgänge

Ausgangspunkt der Prüfung der einzelnen Datenverarbeitungsvorgänge ist das bereits durchgeführte Data Mapping.

Die Prüfung stützt sich insbesondere, soweit vorhanden, auf Verzeichnisse der Verarbeitungsvorgänge gemäß Art. 30 DSGVO, durchgeführte Datenschutz-Assessments gemäß Art. 25 und 35 DSGVO inklusive Templates/Datenschutz-Management-Tools, Projektpläne zum Stand der Umsetzung der rechtlichen Anforderungen des Datenschutzes (insb. die Roadmap, um den weiteren Implementationsverlauf zu beurteilen) und Policies/Prozessbeschriebe aller Art (z.B. Vorgehen bei Anfragen von betroffenen Personen, Löschkonzepte, Data Breach-Prozesse). Auch wird geprüft, wie und wo die Ergebnisse der Prozesse dokumentiert werden. Auf diese Weise kann verifiziert werden, ob das Zielunternehmen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nachkommen kann.

- Sind die zwingenden Informationen in den Verzeichnissen der Verarbeitungsvorgänge und den Templates/Datenschutz-Management-Tools der Datenschutz-Assessments in der nötigen Granularität enthalten? Sind die jeweiligen Informationen korrekt (z.B. die Rechtsgrundlagen der jeweiligen Datenverarbeitung)?
- Sind die Risikoabschätzungen in den durchgeführten Datenschutz-Assessments verhältnismäßig und nachvollziehbar und in den getroffenen Maßnahmen zu erkennen?
- Welche Arten von Personendaten werden verarbeitet? Wenn Persönlichkeitsprofile erstellt oder besonders schützenswerte Personendaten verarbeitet werden, sind die damit verbundenen weitergehenden Pflichten (z.B. Informationspflicht bei Beschaffung der Daten; Einholung einer ausdrücklichen Einwilligung für die Bekanntgabe an Dritte oder die Übermittlung an Drittländer, falls beruhend auf einer Einwilligung), erfüllt?
- Gibt es Datenverarbeitungsvorgänge, die über die erklärten Zwecke hinausgehen (Bsp.: Ein Zielunternehmen, das Kreditkartenabrechnungen ausfertigt, setzt die gesammelten Daten auch zu Marktforschungs- oder Marketingzwecken ein)? Falls ja, handelt es sich hierbei um einen Einzelfall oder um ein systematisches Vorgehen? Falls systematisch, war dies der Geschäftsleitung, der Compliance-Abteilung oder dem Datenschutzbeauftragten bewusst? Falls ja, ist zu erwägen, aus datenschutzrechtlicher Sicht davon abzuraten, die Transaktion weiterzuverfolgen, insbesondere wenn das Geschäftsmodell des Zielunternehmens im Wesentlichen auf Datenverarbeitung basiert (wie dies z.B. bei Technologieunternehmen häufig der Fall ist).
- Sind Rechtsgrundlagen für die jeweilige Datenverarbeitung vorhanden, korrekt (Vorsicht: das „berechtigte Interesse“[1] wird z.B. oft falsch oder zu weit ausgelegt) und dokumentiert?
- Benötigen die Datenverarbeitungsprozesse eine Einwilligung der Betroffenen? Werden diese rechtsgültig eingeholt und dokumentiert? Wird der Widerruf der Einwilligung dokumentiert und, falls ja, wie? Bestehen Prozesse, um einen Widerruf an Auftragsverarbeiter weiterzuleiten?
- Für die Schweiz: Werden Datensammlungen an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet, wenn regelmäßig besonders schützenswerte Personendaten oder Persönlichkeitsprofile verarbeitet oder Personendaten an Dritte bekannt gegeben werden[2]? Wenn nicht, hat das Zielunternehmen z.B. einen internen Datenschutzbeauftragten oder besteht eine gesetzliche Verpflichtung zur Verarbeitung[3]?

Red Flags:

- Grundsätzlich ist eine lückenhafte bzw. nicht vorhandene Dokumentation eine Red Flag. Können wichtige Grundlagendokumente bzw. Anforderungen der DSGVO, wie z.B. das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO nicht geliefert werden, ist die ganze Datenschutzorganisation in Frage zu stellen. Diese Grundlagendokumente sind regelmäßig auch jene, welche der Verantwortliche einer Aufsichtsbehörde im Falle einer Untersuchung bereitstellen[4] müsste und die auch ohne lange Vorbereitungszeit von dieser eingefordert werden könnten. Zudem ist zu beachten, dass der Aufbau eines bisher fehlenden Datenschutz-Frameworks des Zielunternehmens nach dem Vollzug der Transaktion mit hohen Kosten verbunden sein kann.
- Das Zielunternehmen verarbeitet Daten in systematischer Weise über die erklärten Zwecke hinaus.
- Es fehlen Rechtsgrundlagen für die vom Zielunternehmen durchgeführten Datenverarbeitungen, z.B. wenn das Zielunternehmen Datenverarbeitungen auf ein „berechtigtes Interesse“ abstützt, ein solches bei näherer Betrachtungsweise aber nicht besteht und auch keine sonstige Rechtsgrundlage für die Datenverarbeitung vorhanden ist.
- Für die Schweiz: Das Zielunternehmen meldet Datensammlungen trotz Pflicht dazu nicht an den EDÖB.

3. Prüfung der Datenschutzorganisation

a) Verschaffen eines Überblicks über die vorhandene Dokumentation

Es ist notwendig, von der Verkäuferin die Offenlegung aller internen Weisungen und weiterer Dokumente betreffend Datenschutz zu verlangen. Erfahrungsgemäß gibt schon die vorhandene Dokumentation eine erste Indikation über die Qualität der Datenschutzorganisation eines Unternehmens. Bei der Prüfung der Dokumente sind immer die konkreten Umstände des Unternehmens zu beachten, wie etwa dessen Größe und Komplexität sowie die Art und der Zweck der Datenverarbeitungsaktivitäten. Dies ist jeweils ein Zusammenspiel aller Umstände unter Berücksichtigung der datenschutzrechtlichen Risikoexposition des Zielunternehmens. Hilfreich und, sofern vorhanden, zu konsultieren sind auch die Berichte der internen und externen Revisionsstelle.

- Einverlangen aller Weisungen betreffend Datenschutz-/Risk-Management, IT/Cybersecurity, Change-Management, Organisationsreglement, Organigramme, Codes of Conduct, Schulungsunterlagen, HR-Weisungen, Auftragsverarbeitungsverträge, Revisionsberichte (der internen und externen Revisionsstelle).

Red Flags:

- Die internen Weisungen sind lückenhaft oder gar nicht vorhanden.
- Die Dokumentation ist undurchsichtig, geschönt oder widerspricht den eigenen Findings. Die weitere Prüfung sollte mit diesem Wissen kritischer fortgeführt werden. In der Praxis stellen wir immer wieder fest, dass insbesondere interne Revisionsberichte von der Realität abweichen, da Aussagen aus unternehmensinternen Interviews teils ohne weitere kritische Prüfung übernommen werden.

---

1 Vgl. Art. 6 Abs. 1 lit. f DSGVO.
2 Vgl. Art. 11a Abs. 3 DSG.
3 Vgl. Art. 11a Abs. 5 lit. a und e DSG.
4 Gemäß Art. 58 Abs. 1 lit. a DSGVO hat die Aufsichtsbehörde die Befugnis, den Verantwortlichen […] anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind.

b) Datenschutz-Governance

Die folgenden Fragen zielen darauf ab, das Datenschutzniveau bzgl. der Organisation des Zielunternehmens feststellen zu können. Zu prüfen ist, ob das Zielunternehmen den Datenschutz systematisch in seine Prozesse integriert hat und klar geregelt ist, wer für die Einhaltung der datenschutzrechtlichen Vorgaben im Unternehmen auf allen Ebenen verantwortlich ist. Sofern vorhanden sind auch die Berichte der internen und externen Revisionsstelle zu konsultieren.

Die Einsetzung eines Datenschutzbeauftragten ist gemäß Art. 37 DSGVO nicht in jedem Fall gesetzlich vorgeschrieben, zeugt aber von einem hohen Datenschutzstandard im Unternehmen.

- Sind Verantwortlichkeiten und Zuständigkeiten klar geregelt? Sind die Verantwortlichen frei von Interessenkonflikten[5]?
- Ist das Verantwortlichkeitsmodell in verschiedene Stufen eingeteilt? Ist der First Point of Contact, z. B. das Call Center bzw. der Kundenberater, in das Verantwortlichkeitsmodell eingebunden? In der Praxis stellen wir immer wieder fest, dass betroffene Personen ihre Anfragen an das Call Center bzw. ihren Kundenberater richten.
- Gibt es einen Datenschutzbeauftragten mit entsprechendem Pflichtenheft[6], einer angemessenen Ausbildung/Erfahrung[7] und ist dieser bei der zuständigen Aufsichtsbehörde gemeldet?
- Sind Prozesse zur Berücksichtigung des Datenschutzes bei neuen bzw. veränderten Datenverarbeitungsaktivitäten vorhanden (Einbindung Datenschutz in „New Business"-Projekte, Einhaltung von Privacy-by-Design und Privacy-by-Default gemäß Art. 25 DSGVO)? Ist sichergestellt, dass die interne Datenschutzstelle dabei frühzeitig involviert wird?
- Gibt es eine klare Weisung für den Umgang und die Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO? Falls Datenschutz-Folgenabschätzungen bereits durchgeführt wurden, sollten diese eingesehen und insbesondere die Risikoabschätzung kritisch begutachtet werden.
- Gibt es eine Liste mit den implementierten technischen und organisatorischen Maßnahmen (TOM)? Falls ja, sind die TOM gemäß Art. 32 DSGVO angemessen umgesetzt? Für diese Prüfung müssen in aller Regel IT- und IT Security-Experten beigezogen werden.
- Besteht ein Prozess, der sicherstellt, dass alle TOM periodisch überprüft und ggf. angepasst werden?
- Ist ein Datensicherheitskonzept vorhanden (inkl. allfälliger anerkannter Zertifizierungen wie z. B. ISO 27001)?
- Sind Prozesse zur Einhaltung des Datenschutzes bei Outsourcing-Projekten vorhanden (z. B. Auswahlkriterien für Dienstleister, Audits der definierten Datensicherheitsstandards bei der Drittpartei, vorhandene und ausreichende vertragliche Grundlage wie z. B. Auftragsverarbeitungsverträge)?

Red Flags:

- Keine Regelung der Verantwortlichkeit für den Datenschutz.
- Fehlen eines Datenschutzbeauftragten trotz Pflicht dazu, keine ausreichenden Qualifikationen, fehlende Unabhängigkeit/Interessenkonflikte des Datenschutzbeauftragten aufgrund weiterer Funktionen im Unternehmen.
- Keine systematische Einbindung des Datenschutzes in Prozesse bei großen Unternehmen oder bei solchen, die Personendaten besonderer Kategorien im Sinne von Art. 9 DSGVO verarbeiten.
- TOM sind nicht vorhanden bzw. nicht der Verarbeitungsaktivität angemessen implementiert (z. B. sind die Anforderungen an die TOM höher, wenn gemäß Art. 9 DSGVO besondere Kategorien von Personendaten verarbeitet werden).
- Fehlen notwendiger Auftragsverarbeitungsverträge.

c) Umgang mit verarbeiteten Personendaten

Die nachfolgenden Fragen dienen dazu, den Umgang des Zielunternehmens mit den von ihm verarbeiteten Personendaten zu analysieren. Wichtig ist hierbei, dass die internen Weisungen Vorgaben zur Klassifizierung und für den Umgang mit Personendaten enthalten. Für jede dieser Kategorien müssen die Weisungen klare Handlungsanweisungen geben und Sicherheitsanforderungen definieren.

Häufig verarbeitet das Zielunternehmen Personendaten seiner eigenen Arbeitnehmer/innen oder von Arbeitnehmern/innen einer Gruppengesellschaft. Weil die Verarbeitung von Daten von Arbeitnehmern/innen in der Regel strengen Anforderungen unterliegt, ist zu prüfen, ob das Unternehmen für die Verarbeitung von Daten von Arbeitnehmern/innen spezielle Regelungen getroffen hat. Zu denken ist insbesondere an spezielle Datenschutzerklärungen für Arbeitnehmer/innen und spezielle interne Weisungen für den Umgang mit und die Archivierung von Daten von Arbeitnehmern/innen.

- Sind klare Regeln für die Klassifizierung und den Umgang mit Personendaten (insb. Personendaten besonderer Kategorien im Sinne von Art. 9 DSGVO) vorhanden (z. B. Einhaltung strengerer Anforderungen an die Einwilligung, höherer Sicherheitsstandard)?
- Falls das Zielunternehmen durch andere Gesetze als Datenschutzgesetze geschützte Daten verarbeitet (z. B. Daten, die durch Berufsgeheimnisse wie das Arzt-, Bank- oder – in der Schweiz – das Finanzmarktinfrastrukturgeheimnis[8], geschützt sind): Gibt es für diese Daten ein spezielles Schutzkonzept?
- Gibt es eine interne, externe und eine Datenschutzrichtlinie für Arbeitnehmer/innen?

Red Flags:

- Keine interne, externe und Arbeitnehmer-Datenschutzrichtlinie.
- Keine speziellen internen Regeln für den Umgang mit Personendaten besonderer Kategorien im Sinne von Art. 9 DSGVO.
- Keine speziellen internen Regeln für die Verarbeitung von Personendaten, die einem Berufsgeheimnis unterstehen.

d) Datenverlust

Es ist wichtig, dass das Zielunternehmen TOM und Prozesse implementiert hat, damit Datenverluste festgestellt werden können, das Unternehmen entsprechend auf solche Vorkommnisse reagieren und vor allem auch die Daten unter Umständen wiederherstellen kann (Incident Recovery Plan). Datenlecks (sog. Data Breaches) können auch bei guten Vorkehrungen und belastbaren Sicherheitsmaßnahmen vorkommen. Allerdings ist es wichtig zu wissen, aus welchem Grund es zu Datenverlusten gekommen ist und welche Maßnahmen zu treffen sind. Deshalb sind auch immer die Berichte zu Data Breaches zu konsultieren. Es ist ratsam, IT-Experten für diese Prüfung beizuziehen.

- Sind interne Prozesse zur Entdeckung von Data Breaches und zum weiteren Vorgehen im Falle eines Data Breach vorhanden, z. B. um

5 Art. 38 Ziff. 6 DSGVO.
6 Art. 39 DSGVO.
7 Art. 37 Ziff. 5 DSGVO.
8 Vgl. Art. 147 des Finanzmarktinfrastrukturgesetzes (SR 958.1).

sicherzustellen, dass der zuständigen Aufsichtsbehörde innerhalb der gesetzlichen Frist Meldung erstattet wird[9]?
- Gab es bereits Data Breaches? Wenn ja, welche und wie viele? Sind Maßnahmen getroffen, umgesetzt und dokumentiert worden?

Red Flags:
- Wiederholte Data Breaches in den letzten zwei Jahren vor der Prüfung.
- Keine Analyse der Ursachen von Data Breaches und keine Einleitung von Maßnahmen.
- Nicht rechtskonforme Abwicklung eines Data Breach, z. B. keine Meldung an die zuständige Aufsichtsbehörde gemäß Art. 33 DSGVO oder, obwohl eine Pflicht dazu besteht, keine Benachrichtigung der betroffenen Person gemäß Art. 34 DSGVO.
- Falsche Evaluierung des Risikens für die betroffenen Personen.

4. Verhalten gegenüber betroffenen Personen

Die folgenden Fragen dienen zur Beurteilung, ob die Datenverarbeitungen, die das Zielunternehmen durchführt, gegenüber den betroffenen Personen transparent und klar kommuniziert wurden, und das Zielunternehmen die betroffenen Personen hinreichend über ihre Rechte aufgeklärt hat, insbesondere wenn das Zielunternehmen die Datenverarbeitung mit einer Einwilligung der betroffenen Personen rechtfertigt.

Zudem muss das Zielunternehmen Prozesse implementiert haben, die sicherstellen, dass betroffene Personen ihre Rechte auf Information[10], Widerspruch[11], Auskunft[12], Berichtigung[13], Löschung[14], Datenportabilität[15] und Einschränkung der Verarbeitung[16] ausüben können.

Je nach Geschäftsmodell ist auch an Spezialfälle wie etwa die Rechte der betroffenen Personen im Zusammenhang mit automatisierten Entscheidungen[17] zu denken.

Für die Schweiz ist zu beachten, dass das revDSG für ein sog. Hochrisiko-Profiling (d. h. ein Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt), eine ausdrückliche Einwilligung der betroffenen Person voraussetzt.[18]

Zudem ist zu raten, eigene Testanfragen auszulösen. Eine solche Anfrage kann z. B. den Ablauf bei einer Anfrage auf Löschung aufzeigen und auf effiziente Weise allfällige Probleme aufdecken.
- Bestehen die notwendigen transparenten Informationsgrundlagen gegenüber den betroffenen Personen (z. B. Datenschutzerklärungen)?
- Sind für Datenverarbeitungen, die eine Zustimmung voraussetzen, die entsprechenden Einwilligungen vorhanden, rechtsgültig und dokumentiert? Wird der Widerruf der Einwilligung dokumentiert und, falls ja, wie? Bestehen Prozesse, um einen Widerruf an Auftragsverarbeiter weiterzuleiten?
- Sind die Rechte der betroffenen Personen in den Dokumenten betreffend die Informationspflichten aufgelistet?
- Falls Datenverarbeitungen im Rahmen von automatisierten Entscheidungen oder Profiling stattfinden: Ist die zugrundeliegende Logik klar und verständlich dokumentiert?
- Gibt es Prozesse oder Weisungen, die sicherstellen, dass die Rechte der betroffenen Personen auch tatsächlich durchgesetzt werden können?

Red Flags:
- Ungenügende Datenschutzerklärungen (Verletzung der Transparenzpflicht).
- Keine Prozesse zur Abwicklung von Anfragen von betroffenen Personen.
- Prozesse zur Abwicklung von Anfragen sind zwar vorhanden, werden jedoch nicht gelebt.
- Automatisierte Entscheidung ohne Überprüfung, sofern unter Art. 22 DSGVO notwendig.

5. Umgang mit Behörden

Je nach internationaler Ausrichtung und Komplexität der Konzernstruktur des Zielunternehmens sind verschiedene Aufsichtsbehörden im Bereich des Datenschutzes zu berücksichtigen.[19] Hierbei hilft ein Konzept, das die Verantwortlichkeiten, Zuständigkeiten und Herangehensweise im Umgang mit solchen Behörden klar festlegt. Ein solches Konzept ist nicht zwingend erforderlich, zeugt aber von einem hohen Datenschutzstandard im Unternehmen.
- Ist die federführende Aufsichtsbehörde bekannt?
- Gibt es ein Konzept für den Umgang mit den Aufsichtsbehörden?
- Falls ja, regelt das Konzept die Verantwortlichkeiten und Zuständigkeiten im Umgang mit solchen Behörden?
- Besteht nachweislich eine gute Beziehung zur den Aufsichtsbehörden?

6. Interne Mitarbeiterschulungen

Weder die DSGVO noch das DSG bzw. revDSG sehen eine ausdrückliche Pflicht vor, Mitarbeiter zu schulen. Jedoch kann wirkungsvoller Datenschutz unternehmensweit nur umgesetzt werden, wenn alle Mitarbeiter gut geschult und auf Datenschutz sensibilisiert sind. Schulungen reduzieren zudem das Risiko von Datenschutzverletzungen, was im Eigeninteresse eines Unternehmens liegt. Und letztlich zeugen Mitarbeiterschulungen auch von einer im Unternehmen tatsächlich gelebten Datenschutzkultur.
- Gibt es ein Schulungskonzept? Falls ja:
  - Wird dieses eingehalten und gibt es dafür Nachweise?
  - Sieht es ein Ersttraining mit regelmäßigen Wiederholungskursen vor?

---

9 Vgl. Art. 33 DSGVO.
10 Art. 13 und 14 DSGVO.
11 Art. 21 DSGVO.
12 Art. 15 DSGVO.
13 Art. 16 DSGVO.
14 Art. 17 DSGVO.
15 Art. 20 DSGVO.
16 Art. 19 DSGVO.
17 Art. 22 DSGVO.
18 Vgl. Art. 6 Abs. 7 lit. b revDSG. Die DSGVO kennt die Unterscheidung zwischen „normalem" und Hochrisiko-Profiling nicht. Somit ist unter der DSGVO Hochrisiko-Profiling unter den gleichen Voraussetzungen wie „normales" Profiling erlaubt, d. h. gemäß Art. 22 Abs. 2 DSGVO nicht nur, wenn die betroffene Person ausdrücklich eingewilligt hat (lit. c), sondern auch, wenn die Entscheidung (i) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist (lit. a) oder (ii) aufgrund von Rechtsvorschriften, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten (lit. b).
19 Achtung: Bei grenzüberschreitenden Datenverarbeitungen bestimmt sich die federführende Aufsichtsbehörde gemäß Art. 56 Abs. 1 DSGVO nach der Hauptniederlassung bzw. der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters. Das Verfahren hierzu bestimmt sich nach Art. 60 DSGVO.

- Werden Mitarbeiter in Unternehmensbereichen mit erhöhter datenschutzrechtlicher Risikoexposition, wie z. B. HR, gesondert und häufiger geschult?
- Wird geprüft und dokumentiert, ob die Mitarbeiter die Schulungen auch tatsächlich absolviert haben?
- Stehen den Mitarbeitern FAQs zur Verfügung?

7. Vertreter in der EU

Es ist weiter zu prüfen, ob das Zielunternehmen mit Sitz außerhalb der EU verpflichtet ist, einen EU-Vertreter zu ernennen und, falls ja, ob es dies ordnungsgemäß getan hat.

- Ist das Zielunternehmen verpflichtet, einen Vertreter in der EU zu ernennen?
- Falls eine solche Verpflichtung besteht:
  - Gibt es einen schriftlichen Vertrag zwischen dem Zielunternehmen und dem EU-Vertreter (z. B. EU Data Representative Appointment Letter)?
  - Enthält der Vertrag Bestimmungen zum Schutz des Zielunternehmens (z. B. Haftungsbeschränkung des Zielunternehmens, Schadloshaltungs- und Geheimhaltungspflicht des EU-Vertreters)?

8. Zusammenarbeit mit Auftragsverarbeitern (Data Processors)

Es ist sodann zu prüfen, ob das Zielunternehmen Dritte mit einer Datenverarbeitung (sog. Auftragsverarbeiter gemäß Art. 28 DSGVO) beauftragt und, falls ja, die damit einhergehenden Pflichten, die sich je nach anwendbarem Datenschutzrecht unterscheiden, einhält.

Die nachfolgenden Fragen decken die Themenbereiche ab, die regelmäßig in einem Auftragsverarbeitungsvertrag geregelt werden sollten bzw. müssen. Ein solcher Auftragsverarbeitungsvertrag soll gemäß Art. 28 DSGVO eine hinreichende Garantie dafür bieten, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen garantiert.

In diesem Zusammenhang ist auch immer zu prüfen, ob anstelle eines Auftragsverarbeitungsverhältnisses nicht vielmehr eine gemeinsame Verantwortlichkeit (Joint Controllership) vorliegt. Eine solche liegt regelmäßig dann vor, wenn zwei Parteien gemeinsam den Zweck und die Mittel der Datenverarbeitung festlegen.

- Besteht ein Muster-Auftragsverarbeitungsvertrag, der bei der Beauftragung Dritter standardmäßig eingesetzt wird?
- Falls ja, enthält dieses Muster den gesetzlich notwendigen Inhalt? Dieser unterscheidet sich je nach anwendbarem Datenschutzrecht in den Details, umfasst aber typischerweise insbesondere Folgendes:
  - Weisungsrecht des Zielunternehmens als für die Datenverarbeitung Verantwortlicher;
  - Unterstützungspflicht des Auftragsverarbeiters bei Anfragen von betroffenen Personen;
  - Löschungspflicht des Auftragsverarbeiters nach Beendigung des Auftragsverarbeitungsvertrags;
  - Auditrechte des Zielunternehmens; und
  - Verpflichtung des Auftragsverarbeiters zur Einhaltung von TOM zur Datensicherheit.
- Sind mit allen Auftragsverarbeitern Auftragsverarbeitungsverträge abgeschlossen worden? Falls ja, verstoßen die Auftragsverarbeitungsverträge gegen vertragliche oder gesetzliche Geheimhaltungspflichten (z. B. Bank-, Arzt- oder – in der Schweiz – Finanzmarktinfrastrukturgeheimnis[20])?
- Sind die Verhältnisse mit Dritten rechtlich korrekt analysiert worden bzgl. gemeinsamer Verantwortlichkeit gemäß Art. 26 DSGVO bzw. Auftragsverarbeitung gemäß Art. 28 DSGVO?

Red Flags:

- Kein Auftragsverarbeitungsvertrag vorhanden.
- Auftragsverarbeitungsvertrag vorhanden, aber das Zielunternehmen und der „Auftragsverarbeiter" sind eigentlich gemeinsam Verantwortliche (Joint Controllers).
- Auftragsverarbeitungsvertrag vorhanden, er weist aber den gesetzlich notwendigen Inhalt nicht auf.

9. Datenübermittlung ins Ausland (DSG) bzw. Drittländer (DSGVO)

Weiter ist zu prüfen, ob das Zielunternehmen Personendaten ins Ausland (DSG) bzw. Drittländer (DSGVO)[21] übermittelt (cross-border data transfer) und, falls ja, das Drittland ein angemessenes Datenschutzniveau aufweist, das Zielunternehmen für den Schutz der Personendaten geeignete Garantien vorgesehen hat oder ein Ausnahmetatbestand, der die Datenübermittlung rechtfertigt, vorliegt.

- Übermittelt das Zielunternehmen Personendaten in Drittländer?
- Falls ja:
  - Weist das Drittland ein angemessenes Datenschutzniveau aus Sicht der EU bzw. Schweiz auf? Vgl. hierzu die von der Europäischen Kommission[22] bzw. vom EDÖB[23] veröffentlichte Liste der Staaten, die ein angemessenes Datenschutzniveau gewährleisten.
  - Falls nein, verwendet das Zielunternehmen die EU-Standardvertragsklauseln (Standard Contractual Clauses), andere vom EDÖB erstellte oder anerkannte Musterverträge, eigene Vertragsklauseln (in der EU von der zuständigen Aufsichtsbehörde zu genehmigen), verbindliche interne Datenschutzvorschriften (Binding Corporate Rules), einen Code of Conduct,

---

20 Siehe oben Ziffer 3 c), Fn. 8.

21 Im Folgenden wird einheitlich der Begriff „Drittland" verwendet.

22 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents, zuletzt besucht am 26.10.2020. Im Schrems II-Urteil erklärte der EuGH den EU-US-Privacy Shield für ungültig und die EU-Standardvertragsklauseln (SCC) im konkreten Fall als ungenügend, um Personendaten in die USA zu übermitteln (siehe hierzu auch *Dörrwächter/Brinkkötter*, CB 2020, 429). Der Datenexporteur kann die SCC künftig nicht mehr unbesehen verwenden, sondern muss im Einzelfall prüfen, ob die Einhaltung der SCC im Drittland gewährleistet ist und, falls nicht, die SCC ergänzen oder eine andere geeignete Garantie vorsehen. Welche Ergänzungen allerdings notwendig sind, damit die SCC wieder hinreichenden Schutz bieten, ist zurzeit unklar. Dies schafft erhebliche Unsicherheit für Datenübermittlungen in Drittländer ohne angemessenes Datenschutzniveau wie z. B. die USA, China und Russland. Die Europäische Kommission ist derzeit dabei, die SCC zu überarbeiten. Zudem prüfen das U. S. Department of Commerce und die Europäische Kommission zurzeit eine Anpassung des EU-US-Privacy Shield (vgl. die gemeinsame Medienmitteilung, https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836, zuletzt besucht am 26.10.2020).

23 https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/staatenliste.pdf.download.pdf/20181213_Staatenliste_d.pdf, zuletzt besucht am 26.10.2020. Die USA wurde von der Liste dieser Drittländer per 8.9.2020 gestrichen, nachdem der EDÖB zu dem Schluss kam, dass das Privacy Shield-Regime kein adäquates Schutzniveau für Datenbekanntgaben von der Schweiz an die USA bietet (vgl. die Medienmittteilung des EDÖB, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80318.html, zuletzt besucht am 26.10.2020). Im Rahmen der DD ist folglich zu prüfen, ob andere für den Schutz der Personendaten geeignete Garantien bestehen.

einen Zertifizierungsmechanismus oder hat das Zielunternehmen andere geeignete Garantien vorgesehen?
  - Falls nein, liegt ein Ausnahmetatbestand vor, der eine Datenübermittlung ins Drittland rechtfertigt? Bsp.: Ausdrückliche Einwilligungen der betroffenen Personen; Verträge, für deren Abschluss oder Erfüllung die Datenübermittlung erforderlich ist; Rechtsansprüche, zu deren Feststellung, Ausübung oder Durchsetzung vor einem ausländischen Gericht bzw. (nur nach der DSGVO und dem revDSG) einer ausländischen Behörde die Datenübermittlung notwendig ist; Übermittlung nur von Personendaten, welche die betroffene Person selber zugänglich gemacht oder die aus einem öffentlich zugänglichen Register (wie z. B. dem Handelsregister) stammen.
- Falls notwendig, wurde der EDÖB über die Datenübermittlung informiert bzw. wurde sie von der zuständigen EU-Aufsichtsbehörde genehmigt?

Zu beachten ist, dass das Zielunternehmen für eine datenschutzrechtlich zulässige Datenübermittlung in Drittländer nicht nur die speziellen Sorgfaltspflichten von Art. 44 ff. DSGVO bzw. Art. 6 DSG beachten, sondern auch die allgemeinen Datenverarbeitungsgrundsätze[21] einhalten und (nur unter der DSGVO) die Datenverarbeitung rechtfertigen können muss.

Red Flags:
- Das Drittland weist kein angemessenes Datenschutzniveau auf, und es bestehen weder für den Schutz der Personendaten geeignete (insbesondere nach dem Schrems II-Urteil unzureichende) Garantien noch liegt ein Ausnahmetatbestand vor.
- Verletzung der allgemeinen Datenverarbeitungsgrundsätze, fehlender Rechtfertigungsgrund.
- Trotz Pflicht dazu keine Information des EDÖB über die Datenübermittlung bzw. keine Genehmigung der Datenübermittlung durch die zuständige EU-Aufsichtsbehörde.

10. Prüfung allfälliger Datenschutzbegehren, Klagen und Sanktionen

Schließlich ist zu prüfen, welche Art und Anzahl von Datenschutzbegehren das Zielunternehmen in der Vergangenheit erhalten hat und ob gegen das Zielunternehmen wegen (möglicher) Datenschutzverletzungen zivil- oder strafrechtliche Verfahren laufen oder in der Vergangenheit geführt wurden und wie diese ausgegangen sind.
- Einverlangen einer Übersicht über eingegangene Datenschutzbegehren (z. B. Auskunft, Berichtigung, Löschung).
- Gibt es abgeschlossene oder laufende Straf- oder Zivilverfahren aufgrund von Datenschutzverletzungen?
- Gibt es abgeschlossene oder laufende aufsichtsrechtliche Verfahren oder Anfragen von Aufsichtsbehörden?
- Wurden in der Vergangenheit Sanktionen ausgesprochen? Falls ja, wie hoch waren die Bußen? Was waren die Gründe für die Bußen?
- Gab es schon ein behördliches Audit?
- Gibt es Informationen dazu, wie allfällige Data Breaches gelöst wurden und ob und an wen sie gemeldet wurden? Stehen die Meldungen der Data Breaches im Datenraum zur Verfügung?

Red Flags:
- Abgeschlossene Verfahren mit Sanktionen.
- Laufende Verfahren.
- Hohe Anzahl von Datenschutzbegehren bei geringer allgemeiner datenschutzrechtlicher Risikoexposition des Zielunternehmens.

III. Abschließende Bemerkungen

Der aufgezeigte Fragenkatalog ist umfassend und erlaubt eine eingehende Analyse der datenschutzrechtlichen Compliance des Zielunternehmens im Rahmen einer DD. Nicht in jedem Fall ist es in der Praxis angezeigt, sämtliche Fragen abzuarbeiten. Es empfiehlt sich, abhängig von der allgemeinen datenschutzrechtlichen Risikoexposition des Zielunternehmens, der Bedeutung der datenschutzrechtlichen Compliance für das Geschäftsmodell des Zielunternehmens, den Erwartungen der Klienten und nicht zuletzt dem für die DD vorhandenen Budget, eine im Einzelfall sinnvolle und risikobasierte Auswahl an Fragen zu treffen und den Umfang der datenschutzrechtlichen DD den Klienten gegenüber im DD-Bericht darzulegen.

Als DD-Bericht erwarten die Klienten heute in aller Regel keinen detaillierten, beschreibenden Bericht aller Erkenntnisse, sondern eine konzise Darstellung der identifizierten Red Flags einschließlich Priorisierung und möglicher Lösungsansätze. Identifizierte datenschutzrechtliche Red Flags sind bei den Kaufvertragsverhandlungen zu berücksichtigen (Gewährleistungen, Schadloshaltungen), können sich allenfalls kaufpreismindernd auswirken und sind, sofern möglich, nach dem Vollzug der Transaktion zu beheben.

AUTOREN

Dr. Lukas Lezzi, *Rechtsanwalt, CIPP/E, hat in Zürich Rechtswissenschaften studiert und im Finanzmarktrecht promoviert. Er war als betrieblicher Datenschutzbeauftragter einer großen schweizerischen Finanzmarktinfrastruktur tätig. Zurzeit arbeitet er als Associate bei Meyerlustenberger Lachenal AG in Zürich, hauptsächlich im Bereich des Finanzmarkt- und Datenschutzrechts.*

Dr. Christian Kunz, *Rechtsanwalt, LL. M., hat in Zürich Rechtswissenschaften studiert und promoviert. Er 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, *LL. M., CIPP/E, CIPM, arbeitet als Managerin im Bereich Regulatory Compliance bei PricewaterhouseCoopers in Zürich. Zudem ist sie Mitglied der IAPP Leadership Community und engagiert sich in der Schweiz als Young Privacy Professional Lead. Ihre Expertise umfasst die Beratung von datenschutzrechtlichen Sachverhalten und Problemstellungen unter diversen Regulationen wie der DSGVO, CH-DSG und weiteren internationalen Bestimmungen.*

21 Vgl. Art. 4, 5 und 7 DSG bzw. Art. 5 ff. DSGVO.