Digital Due Diligence zum Datenschutz

Ulrich Herfurth, Rechtsanwalt in Hannover und Brüssel

Juli 2025

Einordnung und Bedeutung des Datenschutzes im M&A-Kontext

Der Datenschutz hat sich in den vergangenen Jahren grundlegend gewandelt. Während er lange Zeit als rein regulatorisches Nebenfeld wahrgenommen wurde, ist er heute ein zentraler wirtschaftlicher und haftungsrelevanter Faktor unternehmerischer Tätigkeit. Diese Entwicklung wirkt sich besonders deutlich im Kontext von Unternehmenskäufen und Beteiligungstransaktionen aus. Nahezu jedes moderne Geschäftsmodell beruht auf der Verarbeitung personenbezogener Daten – sei es im Kundenkontakt, im Personalbereich, im Marketing, in digitalen Plattformen oder in datengetriebenen Geschäftsmodellen.

Personenbezogene Daten sind damit zugleich Produktionsfaktor, Wettbewerbsressource und Haftungsrisiko. Ihre rechtmäßige Nutzung kann erheblichen wirtschaftlichen Wert generieren, während datenschutzrechtliche Defizite diesen Wert innerhalb kürzester Zeit zunichtemachen können. Für den Erwerber eines Unternehmens bedeutet dies, dass Datenschutz nicht nur als Compliance-Thema, sondern als eigenständiger Transaktions- und Integrationsfaktor zu betrachten ist.
Die datenschutzrechtliche Due Diligence ist daher integraler Bestandteil der Digital Due Diligence. Sie dient nicht allein der Feststellung formaler Rechtskonformität, sondern vor allem der Identifikation von Risiken, die sich nach dem Closing in Form von Bußgeldern, Schadensersatzansprüchen, Reputationsverlusten oder operativen Einschränkungen realisieren können. Gleichzeitig beeinflussen diese Risiken unmittelbar die Bewertung des Zielunternehmens, die Strukturierung des Kaufvertrags sowie die Planung der Post-Merger-Integration.

Datenschutz als wirtschaftlicher Risikofaktor

Datenschutzrechtliche Risiken wirken sich im Transaktionskontext auf mehreren Ebenen aus. Zunächst drohen behördliche Sanktionen. Die Datenschutzaufsichtsbehörden verfügen über weitreichende Befugnisse zur Anordnung von Maßnahmen, zur Untersagung bestimmter Datenverarbeitungen und zur Verhängung empfindlicher Bußgelder. Diese können – abhängig von Art, Dauer und Schwere des Verstoßes – ein erhebliches finanzielles Volumen erreichen.
Daneben gewinnen zivilrechtliche Schadensersatzansprüche zunehmend an Bedeutung. Betroffene Personen können immaterielle und materielle Schäden geltend machen, etwa bei Datenschutzverletzungen, unzulässigem Tracking oder Datenpannen. Diese Ansprüche richten sich regelmäßig gegen den Verantwortlichen der Datenverarbeitung und treffen damit nach dem Unternehmenskauf den Erwerber, sofern dieser die Verarbeitung fortführt.

Hinzu kommen mittelbare wirtschaftliche Folgen. Datenschutzverstöße können das Vertrauen von Kunden, Geschäftspartnern und Mitarbeitenden nachhaltig beeinträchtigen. In datenbasierten Geschäftsmodellen kann dies unmittelbar zu Umsatzverlusten führen. Auch behördliche Auflagen oder Nutzungsbeschränkungen für bestimmte Datenbestände können die wirtschaftliche Tragfähigkeit des Geschäftsmodells infrage stellen.

Datenschutzrechtliche Due Diligence als Teil der Digital Due Diligence

Die datenschutzrechtliche Due Diligence ist Teil einer umfassenden Digital Due Diligence, die sämtliche digitalen Vermögenswerte, Prozesse und Risiken des Zielunternehmens erfasst. Ihr Ziel ist es, Transparenz über die datenschutzrechtliche Ausgangslage zu schaffen und potenzielle Risiken für den Erwerber zu identifizieren.

Dabei geht es nicht nur um die Frage, ob Datenschutzverstöße in der Vergangenheit vorliegen, sondern auch um die Beurteilung der zukünftigen Compliance-Fähigkeit. Ein Unternehmen kann aktuell noch unauffällig sein, aber strukturelle Defizite aufweisen, die mit zunehmender Datenmenge oder veränderten Geschäftsmodellen zu erheblichen Risiken führen.

Identifikation datenschutzrelevanter Verarbeitungen

Ausgangspunkt jeder datenschutzrechtlichen Prüfung ist die systematische Erfassung sämtlicher Verarbeitungen personenbezogener Daten. Dazu gehören insbesondere:

- Mitarbeiterdaten (HR-Systeme, Bewerbermanagement, Leistungsbewertungen)
- Kundendaten (CRM, Support-Systeme, Marketing)
- Nutzerdaten digitaler Produkte oder Plattformen
- Lieferanten- und Partnerdaten
- Tracking-, Analyse- und Profiling-Daten

In der Praxis zeigt sich häufig, dass personenbezogene Daten in einer Vielzahl von Systemen verarbeitet werden, ohne dass eine vollständige Übersicht über Zweck, Rechtsgrundlage, Speicherorte und Zugriffsrechte besteht. Für den Erwerber besteht hier das Risiko, unbewusst rechtswidrige Verarbeitungen zu übernehmen und fortzuführen.

Rechtsgrundlagen und Zweckbindung

Ein zentraler Prüfpunkt ist die Frage, auf welcher Rechtsgrundlage die jeweilige Datenverarbeitung erfolgt. Fehlende oder unzureichende Rechtsgrundlagen gehören zu den häufigsten Datenschutzverstößen. Besonders risikobehaftet sind dabei Verarbeitungen, die auf Einwilligungen gestützt werden, da diese strengen formalen und materiellen Anforderungen unterliegen. Auch die Zweckbindung ist kritisch zu prüfen. Es ist zu analysieren, ob die tatsächlich gelebte Nutzung der Daten noch vom ursprünglichen Zweck gedeckt ist oder ob Zweckänderungen ohne ausreichende rechtliche Grundlage erfolgt sind. Gerade im M&A-Kontext ist dies relevant, da der Erwerber häufig plant, Daten in neue Konzernstrukturen oder für neue Zwecke zu integrieren.

Datenschutzkonzept und organisatorische Reife

Ein tragfähiges Datenschutzkonzept ist ein wesentlicher Indikator für die organisatorische Reife eines Unternehmens. Zu prüfen ist, ob Datenschutz systematisch verankert ist oder lediglich reaktiv behandelt wird. Ein rein formales Datenschutzhandbuch ohne tatsächliche Umsetzung deutet regelmäßig auf erhebliche Defizite hin.

Von besonderer Bedeutung ist die Frage, ob Datenschutz in Entscheidungsprozesse integriert ist, etwa bei der Einführung neuer IT-Systeme, Produkte oder Geschäftsmodelle. Fehlt diese Integration, besteht die Gefahr, dass datenschutzrechtliche Risiken erst spät erkannt werden – häufig zu spät, um sie ohne erhebliche Kosten zu beheben.

Technische und organisatorische Maßnahmen (TOMs)

Die technischen und organisatorischen Maßnahmen bilden das Rückgrat des praktischen Datenschutzes. Sie dienen dem Schutz personenbezogener Daten vor unbefugtem Zugriff, Verlust oder Manipulation. Im Rahmen der Due Diligence ist zu prüfen, ob die implementierten Maßnahmen dem Stand der Technik entsprechen und angemessen dokumentiert sind.
Unzureichende TOMs erhöhen nicht nur die Wahrscheinlichkeit von Datenschutzverletzungen, sondern wirken sich auch haftungsverschärfend aus. Bei Datenpannen prüfen Aufsichtsbehörden regelmäßig, ob angemessene Schutzmaßnahmen getroffen wurden. Defizite können hier zu deutlich höheren Bußgeldern führen.

Datenschutz-Governance und Verantwortlichkeiten

Datenschutz erfordert klare Verantwortlichkeiten. Zu prüfen ist, ob ein Datenschutzbeauftragter wirksam bestellt ist, ob seine Rolle klar definiert ist und ob er organisatorisch unabhängig agieren kann. Ebenso relevant ist, ob Datenschutzaufgaben auf weitere Funktionen verteilt sind und ob es funktionierende Kontroll- und Eskalationsmechanismen gibt.

Fehlende oder unklare Governance-Strukturen erhöhen das Risiko systematischer Verstöße und erschweren eine schnelle Reaktion im Schadensfall. Für den Erwerber sind sie zudem ein Hinweis auf erhöhten Integrations- und Nachbesserungsaufwand.

Dokumentation und Verzeichnis von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten ist ein zentrales Dokument der datenschutzrechtlichen Compliance. Es dient nicht nur der formalen Erfüllung gesetzlicher Pflichten, sondern auch als Grundlage für Risikoanalysen und Audits.
Im Rahmen der Due Diligence ist zu prüfen, ob das Verzeichnis vollständig, aktuell und realitätsnah ist. Abweichungen zwischen dokumentierten und tatsächlichen Prozessen sind häufig und stellen ein erhebliches Risiko dar, insbesondere im Falle behördlicher Prüfungen.

Datenschutzvorfälle und Incident-Response

Ein weiterer Schwerpunkt der datenschutzrechtlichen Due Diligence ist der Umgang mit Datenschutzvorfällen. Zu prüfen ist, ob es in der Vergangenheit meldepflichtige Vorfälle gab, wie diese behandelt wurden und ob daraus organisatorische Lehren gezogen wurden.
Darüber hinaus ist zu analysieren, ob klare Incident-Response-Prozesse existieren. Verspätete oder unterlassene Meldungen stellen eigenständige Verstöße dar und können zusätzliche Bußgelder auslösen.

Schulungen und Unternehmenskultur

Der Faktor Mensch spielt im Datenschutz eine zentrale Rolle. Fehlende oder unzureichende Schulungen sind eine der häufigsten Ursachen für Datenschutzverstöße. Im Rahmen der Due Diligence ist zu prüfen, ob Schulungen regelmäßig stattfinden, dokumentiert sind und zielgruppenspezifisch ausgestaltet werden.
Darüber hinaus ist die datenschutzbezogene Unternehmenskultur zu bewerten. Wird Datenschutz als lästige Pflicht oder als integraler Bestandteil verantwortungsvoller Unternehmensführung verstanden? Diese Frage ist insbesondere für die Post-Merger-Integration von Bedeutung.

Vertragliche Datenverarbeitungen und Drittparteien

Ein erheblicher Teil datenschutzrechtlicher Risiken entsteht in der Zusammenarbeit mit Dienstleistern und Partnern. Zu prüfen ist, ob

Auftragsverarbeitungsverträge bestehen, ob sie aktuell sind und ob die tatsächliche Zusammenarbeit den vertraglichen Regelungen entspricht.

Unklare oder fehlende Verträge können zu erheblichen Haftungsrisiken führen, da der Verantwortliche für die Auswahl und Kontrolle von Dienstleistern haftet.

Schadensersatzrisiken bei Datenschutzverstößen als eigenständiger Transaktionsfaktor

Neben behördlichen Bußgeldern stellen zivilrechtliche Schadensersatzansprüche eines der am häufigsten unterschätzten Risiken im Zusammenhang mit Datenschutzverstößen dar. Während Bußgelder typischerweise einmalige, wenn auch teils erhebliche Belastungen darstellen, können Schadensersatzansprüche eine dauerhafte, schwer kalkulierbare und sich dynamisch entwickelnde Haftung begründen. Im Kontext von Unternehmenskäufen sind sie daher von besonderer Relevanz, da sie regelmäßig erst nach dem Closing entstehen oder geltend gemacht werden und wirtschaftlich vollständig auf den Erwerber durchschlagen.

Rechtsgrundlagen und Anspruchsstruktur

Datenschutzrechtliche Schadensersatzansprüche knüpfen unmittelbar an Datenschutzverstöße an. Anspruchsberechtigt sind betroffene Personen, deren personenbezogene Daten rechtswidrig verarbeitet wurden oder die von einer Datenschutzverletzung betroffen sind. Dabei ist nicht erforderlich, dass ein klassischer Vermögensschaden vorliegt. Vielmehr genügt bereits ein immaterieller Schaden, etwa in Form von Kontrollverlust, Bloßstellung, Vertrauensverlust oder psychischer Belastung.

Diese weite Auslegung führt dazu, dass Schadensersatzansprüche nicht auf Einzelfälle beschränkt bleiben, sondern sich schnell zu Massenansprüchen entwickeln können, etwa bei Datenpannen, unzulässigem Tracking oder systematischen Verstößen gegen Transparenz- und Informationspflichten. Für den Erwerber eines Unternehmens bedeutet dies, dass ein zunächst überschaubar erscheinender Datenschutzverstoß erhebliche finanzielle Langzeitfolgen nach sich ziehen kann.

Typische Schadensszenarien in der Praxis

In der Transaktionspraxis lassen sich mehrere typische Konstellationen identifizieren, in denen Schadensersatzrisiken eine besondere Rolle spielen:

- Datenpannen (z. B. Hackerangriffe, Fehlkonfigurationen, Verlust von Datenträgern), bei denen eine große Anzahl betroffener Personen gleichzeitig Ansprüche geltend macht.
- Unzulässiges Tracking oder Profiling, etwa im Online-Marketing, bei dem über längere Zeiträume personenbezogene Daten ohne wirksame Einwilligung verarbeitet wurden.
- Fehlerhafte oder fehlende Informationspflichten, die zu systematischen Rechtsverstößen führen, ohne dass dies im operativen Alltag unmittelbar auffällt.
- Unzureichende Zugriffsbeschränkungen, insbesondere im Mitarbeiterbereich, die zu internen Datenschutzverletzungen führen.

In all diesen Fällen besteht das Risiko, dass sich Schadensersatzansprüche zeitlich verzögert, gebündelt oder koordiniert realisieren, etwa durch spezialisierte Kanzleien oder Verbände.

Kumulatives Haftungsrisiko und wirtschaftliche Dimension

Ein wesentliches Merkmal datenschutzrechtlicher Schadensersatzansprüche ist ihre Kumulativität. Während Bußgelder regelmäßig einmalig verhängt werden, können Schadensersatzansprüche von einer

Vielzahl betroffener Personen parallel geltend gemacht werden. Bereits moderate Einzelbeträge können sich bei einer großen Zahl von Betroffenen zu erheblichen Gesamtrisiken summieren.

Für den Erwerber ist dieses Risiko besonders kritisch, da es häufig nicht bilanziert, nicht versichert oder nicht vollständig dokumentiert ist. Im Rahmen der Due Diligence lassen sich potenzielle Anspruchsgrundlagen zwar identifizieren, die tatsächliche Inanspruchnahme hängt jedoch von externen Faktoren ab, etwa öffentlicher Wahrnehmung, Medienberichterstattung oder behördlichen Untersuchungen.

Zurechnung und Fortwirkung nach dem Unternehmenskauf

Ein zentrales Problem im M&A-Kontext ist die Frage der Haftungszurechnung. Schadensersatzansprüche richten sich regelmäßig gegen den aktuellen Verantwortlichen der Datenverarbeitung. Setzt der Erwerber die Datenverarbeitung nach dem Closing fort, kann er auch für Verstöße haftbar gemacht werden, deren Ursachen in der Zeit vor dem Unternehmenskauf liegen. Dies gilt insbesondere dann, wenn der datenschutzwidrige Zustand fortbesteht oder nicht unverzüglich beendet wird. Für den Erwerber besteht daher die Gefahr, durch bloße Fortführung bestehender Prozesse in eine eigene Haftung einzutreten. Datenschutzrechtliche Altlasten können sich so in eine dauerhafte Haftungskette verwandeln.

Bedeutung für Due Diligence und Vertragsgestaltung

Die Analyse von Schadensersatzrisiken muss daher integraler Bestandteil der datenschutzrechtlichen Due Diligence sein. Zu prüfen ist insbesondere:

- ob es bereits bekannte oder angedrohte Ansprüche gibt,
- ob frühere Datenschutzverstöße dokumentiert und aufgearbeitet wurden,
- ob betroffene Personen informiert wurden,
- ob Rückstellungen gebildet wurden oder hätten gebildet werden müssen.

Die identifizierten Risiken wirken sich unmittelbar auf die Gestaltung des Unternehmenskaufvertrags aus. Typische Instrumente sind spezifische Garantien, Freistellungen, Haftungshöchstbeträge oder Kaufpreisanpassungen. In besonders risikobehafteten Konstellationen können auch Escrow-Modelle oder aufschiebende Bedingungen sinnvoll sein.

Versicherbarkeit und Grenzen des Versicherungsschutzes

Häufig wird versucht, Schadensersatzrisiken über Cyber- oder Haftpflichtversicherungen abzusichern. In der Praxis ist jedoch zu beachten, dass der Versicherungsschutz regelmäßig begrenzt, ausschlussbehaftet oder an enge Voraussetzungen geknüpft ist. Insbesondere systematische Datenschutzverstöße oder vorsätzliche Pflichtverletzungen sind häufig vom Versicherungsschutz ausgeschlossen.
Für den Erwerber ist daher entscheidend, nicht allein auf bestehende Versicherungen zu vertrauen, sondern die zugrunde liegenden Risiken strukturell zu analysieren und – soweit möglich – vor dem Closing zu adressieren.

Schadensersatz als langfristiges M&A-Risiko

Schadensersatzansprüche bei Datenschutzverstößen stellen ein eigenständiges, langfristiges und schwer kalkulierbares Risiko beim Unternehmenskauf dar. Sie können den wirtschaftlichen Erfolg einer Transaktion auch dann erheblich beeinträchtigen, wenn behördliche Bußgelder bereits abgegolten oder vermieden wurden. Eine fundierte datenschutzrechtliche Due Diligence muss diese Risiken daher ausdrücklich berücksichtigen und in die wirtschaftliche und vertragliche Strukturierung der Transaktion einbeziehen.

Auswirkungen auf Kaufvertrag und Bewertung

Die Ergebnisse der datenschutzrechtlichen Due Diligence haben unmittelbare Auswirkungen auf die Strukturierung des Unternehmenskaufvertrags. Datenschutzrisiken schlagen sich regelmäßig in Garantien, Freistellungen, Kaufpreisanpassungen oder spezifischen Closing-Conditions nieder.

Je nach Schwere der identifizierten Risiken kann auch ein Earn-out-Modell oder ein Kaufpreisabschlag sinnvoll sein. In gravierenden Fällen kann Datenschutz sogar zum Deal-Breaker werden.

Datenschutz und Post-Merger-Integration

Nach dem Closing stellt die Integration der Datenschutzstrukturen eine erhebliche Herausforderung dar. Unterschiedliche Datenschutzniveaus, Prozesse und Kulturen müssen harmonisiert werden. Fehlende Planung kann hier zu neuen Risiken führen, insbesondere wenn Datenbestände zusammengeführt oder neu genutzt werden.

Fazit

Datenschutz ist im Rahmen der Digital Due Diligence ein zentraler Wert- und Risikofaktor beim Unternehmenskauf. Eine sorgfältige und tiefgehende Prüfung ermöglicht es, Haftungs- und Bußgeldrisiken frühzeitig zu erkennen, den Unternehmenswert realistisch zu bewerten und die Grundlage für eine erfolgreiche Integration zu schaffen. Datenschutz ist damit nicht nur eine rechtliche Pflicht, sondern ein strategischer Faktor moderner M&A-Transaktionen.

+ + +

Aus der Compact Reihe zur Digital Due Diligence:

- Digital Due Diligence beim Unternehmenskauf
- Digital Due Diligence zu Datensicherheit
- Digital Due Diligence zu Datenrechten und IP
- Digital Due Diligence zum Datenschutz
- Digital Due Diligence zur Datensouveränität

+ + +

IMPRESSUM

HERAUSGEBER

herfurth.partner

Herfurth & Partner Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-307 56-0 Fax 0511-307 56-10
Mail info@herfurth.de, Web www.herfurth.de

Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.), Antonia Herfurth, Rechtsanwältin, LL.M. (Göttingen)
Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Dipl.-Kfm. Günter Stuff; Xiaomei Zhang, Juristin (China), Mag. iur. (D); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Konstantin Kuhle, Rechtsanwalt; Sara Nesler, Mag. iur. (Torino), LL.M. (Münster), Dr. jur Amelia Kuschel, LL.M. (Pittsburgh); Dr. jur. Dr. rer. pol. Karoline H. Köhler, Rechtsanwältin

KORRESPONDENTEN

alliuris

u.a. Amsterdam, Athen, Brüssel, Budapest, Helsinki, Istanbul, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Paris, Stockholm, Warschau, Wien, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Peking, Tokio.

VERLAG

CASTON

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511-307 56-50 Fax 0511-307 56-60
Mail info@caston.info; Web www.caston.info