Datenschutz-Grundverordnung (DSGVO):

Ein kurzer Leitfaden von Sage für Unternehmen

Inhalt

Einleitung

Die Datenschutz-Grundverordnung (DSGVO) ist ein neuer rechtlicher Rahmen, der am 25. Mai 2018 in der Europäischen Union (EU) in Kraft treten wird. Allen EU-Verordnungen kommt in den EU-Mitgliedstaaten unmittelbare Wirkung zu, das heißt, die DSGVO wird Vorrang vor dem jeweils nationalen Recht haben.

Ziel der DSGVO ist der Schutz personenbezogener Daten – also Daten zu natürlichen Personen (Betroffene). Die DSGVO ist eine der größten Umstrukturierungen bestehender Regelungen zum Umgang mit personenbezogenen Daten. Sie wird vermutlich nicht nur Auswirkungen auf Unternehmen, sondern auch auf natürliche Personen, Firmen, Behörden, Agenturen oder andere Einrichtungen haben, die personenbezogene Daten von natürlichen Personen verarbeiten, die in der EU ansässig sind. Das betrifft auch Zulieferer und andere Dritte, die von einem Unternehmen mit der Verarbeitung personenbezogener Daten beauftragt werden.

Der Anwendungsbereich ist überraschend groß. Er umfasst alle EU-Mitgliedstaaten sowie Großbritannien (UK) nach dem Brexit im Jahr 2019. Die Verordnung wird dann auch in britisches Recht umgesetzt. Im Gegensatz zur EU-Richtlinie 95/46 zum Schutz personenbezogener Daten betrifft die DSGVO auch alle Unternehmen außerhalb der EU, die natürlichen Personen in der EU Waren oder Dienstleistungen anbieten oder deren Verhalten innerhalb der EU überwachen. So sind zum Beispiel in den USA ansässige Web-Hosting-Unternehmen, die für natürliche Personen in der EU zugängliche Websites betreiben, direkt davon betroffen.

Die DSGVO hat weltweit massive Konsequenzen für alle Abteilungen eines jeden Unternehmens. Einige von ihnen müssen beispielsweise einen Datenschutzbeauftragten einstellen oder einsetzen. Fast alle Unternehmen werden zusätzliche Verfahren und Schutzmaßnahmen einführen müssen. Eine Prüfung durch einen entsprechend qualifizierten Prüfer wird dringend empfohlen. Insbesondere mit Blick auf die drohenden Geldbußen von bis zu 20 Mio. Euro oder sogar 4 % des weltweit erzielten Jahresumsatzes – je nachdem, welcher Betrag höher ist – sollte die Kenntnis der DSGVO obligatorisch sein.

Dieses Dokument soll eine knappe und vereinfachte Hilfestellung für Unternehmen darstellen. Weiterführende Informationen erhalten Sie bei den Aufsichtsbehörden, wie zum Beispiel der britischen Datenschutzbehörde ICO (Information Commissioner's Office) und deren „Überblick über die Datenschutz-Grundverordnung". Bitte lesen Sie den Sage Haftungsausschluss am Ende dieses Leitfadens.

Infografik:

Die DSGVO auf einen Blick

Einwilligung

Ist durch eine Erklärung oder eine andere eindeutige, bestätigende Handlung einzuholen. Einwilligung kann nicht vorausgesetzt oder durch vorausgewählte Kästchen eingeholt werden.

Betroffenenrechte

Betroffenenrechte werden gestärkt und Informationspflichten in Bezug auf Verarbeitungstätigkeiten erweitert.

Sanktionen

Mögliche Geldstrafen von bis zu 4 % des weltweiten Umsatzes oder 20 Mio. Euro – je nachdem, welcher Betrag höher ist. Die Gefahr von Geldstrafen besteht auch ohne Datenverlust.

Datenübertragbarkeit

Betroffene können ihre Daten jetzt auch verschieben, kopieren oder übertragen – selbst an einen Konkurrenten.

Meldepflicht von Datenschutzverstößen

Datencontroller müssen Verstöße innerhalb von 72 Stunden der Aufsichtsbehörde melden, etwa der ICO in UK. Bei schweren Verstößen sind Betroffene zu informieren.

Datenschutzbeauftragter

Könnte obligatorisch werden. Muss Fachwissen über Datenschutzgesetze besitzen. Kann ein Mitarbeiter oder ein Dienstleistungsauftrag sein.

Datenschutz von Anfang bis Ende

Datenschutzerwägungen sind in allen Stufen nötig und nur Daten, die für diesen Zweck zwingend erforderlich sind, können verarbeitet werden.

Erweiterter Anwendungsbereich

Gilt für Sie und auch für Dritte, die in Ihrem Auftrag Daten verarbeiten – auch außerhalb der EU.

Die Grundlagen

Die DSGVO legt Mindestanforderungen für die Behandlung sämtlicher personenbezogener Daten fest. Personenbezogen sind alle Daten, anhand derer eine natürliche Person identifiziert werden kann oder die ihr in verschiedener Hinsicht zugeordnet sind (einschließlich des Erscheinungsbildes oder sogar biometrischer Daten).

Die meisten Unternehmen erheben personenbezogene Daten von dem Moment an, in dem sie mit einer natürlichen Person in Kontakt treten. Oft tun sie dies noch nicht einmal bewusst. Zum Beispiel gehören zur Erhebung personenbezogener Daten so elementare Dinge wie Tracking-Cookies, die einen Nutzer auf Ihrer Website identifizieren. Weiter geht es mit detaillierten Einträgen zu einer Person in einer Customer-Relationship-Management-Datenbank (CRM) und weit darüber hinaus. Selbst wenn diese personenbezogenen Daten ausschließlich zum Vorteil und im Sinne der natürlichen Person erhoben oder verarbeitet werden, fallen sie dennoch in den Anwendungsbereich der DSGVO.

Wie bei der EU-Datenschutzrichtlinie 95/46 definiert die DSGVO drei grundlegende Regelwerke für den Umgang mit personenbezogenen Daten: die Datenschutzgrundsätze, die rechtmäßige Verarbeitung und die Einschränkungen des internationalen Datenverkehrs. Die meisten Unternehmen und viele betroffene Personen sollten diese bereits kennen. In diesem Leitfaden stellen wir Ihnen die drei grundlegenden Regelwerke vor. Auch wenn Sie bereits damit vertraut sind, lohnt sich das Lesen – nicht zuletzt, um Ihr Wissen aufzufrischen.

Schließlich bringt die DSGVO mehrere wichtige, neue Anforderungen mit sich.

Die DSGVO im Überblick

Im Folgenden sind alle wichtigen Bereiche der DSGVO mit Verweis auf die EU-Datenschutzrichtlinie 95/46 aufgeführt.

Betroffenenrechte und Informationspflicht

Die aktuellen EU-Datenschutzgesetze (Richtlinie 95/46) räumen natürlichen Personen (den Betroffenen) Rechte über ihre personenbezogenen Daten ein und legen fest, welche Informationen den Betroffenen von Unternehmen zur Verfügung gestellt werden müssen, einschließlich des Verwendungszwecks der personenbezogenen Daten. Dies erfolgte bislang meist in Form von Datenschutzerklärungen oder Benachrichtigungen auf einer Website.

Die DSGVO geht hier deutlich weiter und verleiht Betroffenen zusätzliche Rechte, über die sie wiederum aufgeklärt werden müssen. Betroffene sollten vor allem die folgenden Rechte kennen (Aufzählung unvollständig): Das Recht, …

1. sich bei Aufsichtsbehörden, wie etwa der Datenschutzbehörde ICO in UK, zu beschweren;
2. ihre Einwilligung zur Verarbeitung ihrer personenbezogener Daten zurückzuziehen (siehe unten);
3. ihre personenbezogenen Daten einzusehen und vom Unternehmen und allen Dritten, die Zugang dazu hatten, berichtigen oder löschen zu lassen (das „Recht auf Vergessenwerden“);
4. über alle angewendeten Verfahren zur automatisierten Verarbeitung personenbezogener Daten (auch der Profilerstellung) informiert zu werden;
5. bestimmten Formen der Verarbeitung zu widersprechen, z. B. Direktmarketing und Entscheidungen, die ausschließlich auf automatisierter Verarbeitung beruhen;
6. zu erfahren, wie lange ihre personenbezogenen Daten gespeichert werden;
7. Angaben zu allen eingesetzten Datenschutzbeauftragten zu erhalten (siehe unten).

Außerdem sind Betroffene berechtigt, gemeinnützige Organisationen mit der Ausübung ihrer Rechte und der Geltendmachung von Forderungen in ihrem Namen zu beauftragen, ähnlich wie bei amerikanischen Sammelklagen.

Einwilligung

Wenn Sie Daten auf Grundlage der Einwilligung von Betroffenen erheben, sollten Sie beachten, dass diese Einwilligung im Rahmen der DSGVO nicht wie nach bisherigen EU-Datenschutzgesetzen ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt, sondern durch eine Erklärung oder eine andere eindeutige, bestätigende Handlung einzuholen ist. Anders gesagt stellen vorausgewählte Kästchen für die Einwilligung auf Websites oder das Schweigen/die Untätigkeit eines Betroffenen nach dem Lesen einer Datenschutzerklärung keine Einwilligung mehr dar.

Außerdem ist eine Einwilligung nicht universell gültig. Ein Unternehmen darf also eine Einwilligung, die ein Betroffener in einem bestimmten Schritt der Geschäftsabwicklung erteilt hat, nicht automatisch als Einwilligung für andere Arten der Verarbeitung personenbezogener Daten betrachten. Für alle Schritte der Verarbeitung personenbezogener Daten sind separate Einwilligungen einzuholen.

Betroffene müssen außerdem darüber informiert werden, dass sie ihre Einwilligung jederzeit widerrufen können, und der Widerruf der Einwilligung muss genauso einfach erfolgen können, wie die Einwilligung selbst.

Deshalb müssen bereits erteilte Einwilligungen von Betroffenen daraufhin überprüft werden, ob sie den Anforderungen der DSGVO genügen. Bei Widersprüchen oder Unklarheiten müssen Unternehmen für eine neue Rechtsgrundlage für die Datenverarbeitung sorgen (z. B. ist dies für die Vertragserfüllung erforderlich), eine neue Einwilligung einholen oder die Verarbeitung personenbezogener Daten einstellen.

Recht der Verschiebung und Übertragung personenbezogener Daten (Datenübertragbarkeit)

Betroffene sind jetzt berechtigt, ihre personenbezogenen Daten von einem Ort an einen anderen – sogar zu einem Konkurrenten – zu verschieben, zu kopieren oder zu übertragen. So kann zum Beispiel ein Nutzer eine Wiedergabeliste, die ein Musikanbieter für ihn erstellt hat, beim Wechsel zu einem anderen Anbieter mitnehmen. Die personenbezogenen Daten müssen demzufolge in einem strukturierten, gängigen und maschinenlesbaren Format vorliegen, sodass sie problemlos verwendet und geteilt werden können.

Die Notwendigkeit, Daten in einem portablen Format zu speichern, das man leicht verarbeiten kann, wird in der Zukunft erhebliche IT-Anpassungen und damit Kosten nach sich ziehen.

Deutlich erweiterter Anwendungsbereich

Einfach gesagt macht die DSGVO nicht nur das datenerhebende Unternehmen, sondern auch alle Dritten für Verstöße verantwortlich, die im Auftrag dieses Unternehmens Daten verarbeiten – egal, ob es sich um ein anderes Unternehmen, eine Organisation oder eine natürliche Person handelt. Das heißt aber nicht, dass ein Unternehmen an einen Dritten einfach die personenbezogenen Daten und damit die Verantwortung abgeben kann. Das Unternehmen muss dafür sorgen, dass der Drittanbieter die DSGVO ebenfalls einhält.

Der potentielle räumliche Geltungsbereich wird zudem über die EU hinaus auf alle Unternehmen – oder wie bereits erwähnt auf alle Dritte, die personenbezogene Daten in deren Auftrag verarbeiten – erweitert, die natürlichen Personen in der EU Waren oder Dienstleistungen anbieten oder deren Verhalten innerhalb der EU überwachen. Es ist vor allem irrelevant, ob für diese Waren und Dienstleistungen eine Zahlung gefordert wird oder nicht. Daher gilt die DSGVO auch für gemeinnützige und nichtstaatliche Organisationen.

Da die EU ein Handelspartner der meisten Länder ist, geht der erweiterte Anwendungsbereich der DSGVO mit Konsequenzen für viele weltweit agierende Unternehmen einher. Diese Länder müssen die DSGVO-Bestimmungen einhalten, wenn sie in EU-Mitgliedstaaten entweder direkt oder als Dritter für andere tätig sein wollen.

Nachweis der Einhaltung

Mit der Einhaltung der DSGVO ist es noch nicht getan. Gemäß der in der DSGVO vorgesehenen „Rechenschaftspflicht" muss ein Unternehmen die Einhaltung auch nachweisen können, was wiederum umfassende Aufzeichnungspflichten mit sich bringt. Insbesondere sind Einzelheiten zu Datenverarbeitungstätigkeiten*, Bitten um die Offenlegung der gespeicherten Daten, Verstößen, zur Einholung von Einwilligungen sowie Datenschutz-Folgenabschätzungen (siehe unten) zu dokumentieren.

Diese Verpflichtung betrifft auch wieder diejenigen Dritten, die im Auftrag eines Unternehmens personenbezogene Daten verarbeiten, wobei die Pflichten für diese Dritten nicht ganz so weit gehen.

** Dies betrifft Unternehmen mit mehr als 250 Mitarbeitern oder Unternehmen mit weniger Mitarbeitern, deren Datenverarbeitungsaktivitäten allerdings ein Risiko für die Rechte und Freiheiten natürlicher Personen bergen, nicht nur vereinzelt durchgeführt werden oder besondere Datenkategorien beinhalten, wie Informationen zu Gesundheit, Religion oder sexueller Orientierung.*

Datenschutz von Anfang bis Ende

Um die Datenschutzerwartungen eines Betroffenen während der gesamten Lebensdauer der personenbezogenen Daten zu erfüllen, sind technische und organisatorische Maßnahmen umzusetzen – vom Beginn über die Ausführung bis hin zur Beendigung der Tätigkeit. Dieser sog. „eingebaute Datenschutz" (Privacy by Design) bedeutet, dass Datenschutzerwägungen von Anfang an in jede Stufe dieser Verarbeitungsaktivität integriert werden müssen.

Zudem dürfen nur die personenbezogenen Daten verarbeitet werden, die für diesen Zweck zwingend erforderlich sind. Dies wird auch als Datenminimierung oder „datenschutzfreundliche Voreinstellungen" (Privacy by Default) bezeichnet.

In der Praxis wird die Umsetzung des eingebauten Datenschutzes und datenschutzfreundlicher Voreinstellungen etliche Maßnahmen erfordern: fortlaufende Schulungen, regelmäßige Prüfungen, die Datenminimierung, die Zugangsbeschränkung zu personenbezogenen Daten auf den jeweils nötigen Umfang und die Umsetzung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, wie Pseudonymisierung oder Verschlüsselung, erfordern.

Meldepflicht von Datenschutzverstößen

Sollte es zu einem Verstoß gegen die DSGVO kommen, müssen Unternehmen, die personenbezogene Daten erheben, innerhalb von 72 Stunden die Aufsichtsbehörden informieren, wie etwa die ICO in UK. Dritte, die im Auftrag dieser Unternehmen personenbezogene Daten verarbeiten, müssen dem entsprechenden Unternehmen den Verstoß unverzüglich melden.

Sollte der Verstoß ein hohes Risiko für die Betroffenen darstellen, müssen die Unternehmen auch die Betroffenen unverzüglich darüber informieren.

Datenschutzbeauftragter (Data Protection Officer, DPO)

Die DSGVO verlangt, dass Unternehmen und Dritte, die personenbezogene Daten im Auftrag dieser Unternehmen verarbeiten, einen Datenschutzbeauftragten (Data Protection Officer, DPO) ernennen, wenn: (i) sie eine öffentliche Einrichtung sind; (ii) die Haupttätigkeit des Unternehmens oder des Dritten die groß angelegte Überwachung natürlicher Personen beinhaltet; oder wenn die Hauptaktivität in der groß angelegten Verarbeitung besonderer Kategorien personenbezogener Daten besteht, einschließlich der Daten, die strafrechtliche Verurteilungen und Straftaten betreffen. Der DPO muss Fachwissen über Datenschutzgesetze besitzen und nicht zwingend ein Mitarbeiter sein. Er oder sie kann diese Aufgabe zum Beispiel auch im Rahmen von Dienstleistungsaufträgen ausführen. Die Angaben des DPO müssen der Aufsichtsbehörde mitgeteilt werden, in UK etwa der Datenschutzbehörde ICO.

Sanktionen

Die Nichteinhaltung der DSGVO wird mit scharfen Sanktionen belegt, die Geldstrafen von bis zu 4 % des weltweiten Jahresumsatzes des Unternehmens oder 20 Mio. Euro betragen können – je nachdem, welcher Betrag der höhere ist. Ihnen kann sogar dann eine Geldstrafe drohen, wenn es zu keinem Datenverlust gekommen ist. Hier ist anzumerken, dass die DSGVO dabei keine Ausnahmen für Kleinunternehmen vorsieht. Außerdem haben natürliche Personen die Möglichkeit, mittels einer Sammelklage eine förmliche behördliche Untersuchung zu verlangen, wenn ein Unternehmen die DSGVO nicht einhält.

Brexit

Nach den britischen Parlamentswahlen 2017 wurde die konservative Regierung für fünf weitere Jahre wiedergewählt. In dieser Zeit, genauer im Jahr 2019, wird UK die EU verlassen. Wie für alle EU-Mitgliedstaaten gilt die DSGVO bis zu diesem Zeitpunkt auch für Großbritannien. In der Ankündigung der neuen Gesetzgebung nach der Wahl hieß es in Bezug auf die neuen Datenschutzgesetze:

> *„... die Datenschutz-Grundverordnung und die neue Richtlinie umsetzen, welche die Datenverarbeitung durch Strafverfolgungsbehörden betrifft, unsere Verpflichtungen als EU-Mitgliedstaat erfüllen, und dafür sorgen, dass Großbritannien auch nach dem EU-Austritt in der Lage ist, Daten mit anderen EU-Mitgliedstaaten und auch international auszutauschen."*
>
> *Quelle: Queen's Speech, Juni 2017*

Es kann zwar nicht davon ausgegangen werden, ist jedoch möglich, dass die Europäische Kommission Großbritannien in die Liste der Länder aufnimmt, die „angemessenen" Schutz bieten, und Großbritannien dadurch nicht von möglichen Datenschutzrestriktionen, wie Verboten der Datenübertragung, betroffen ist. Auf dieser Seite finden Sie alle zukünftigen Entscheidungen.

Die neuen britischen Rechtsvorschriften ersetzen das Datenschutzgesetz von 1998, das auf der EU-Richtlinie 95/46 beruhte.

Grundsätze der DSGVO

Zusätzlich zu den oben genannten Anforderungen und wie bei der EU-Datenschutzrichtlinie 95/46 definiert die DSGVO drei grundlegende Regelwerke für den Umgang mit personenbezogenen Daten. Diese können vereinfacht wie folgt beschrieben werden:

- ***Datenschutzgrundsätze:*** Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Sie müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Sie müssen sachlich richtig und auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden. Sie müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es erforderlich ist; sie müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor Verlust, Zerstörung, Schädigung oder unrechtmäßigem Zugang.
- ***Rechtmäßige Verarbeitung*** Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: Die betroffene Person hat ihre Einwilligung für einen oder mehrere bestimmte Zwecke gegeben; die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich, dessen Vertragspartei die betroffene Person ist oder in Kürze sein wird; die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich (z. B. Einreichung von Steuerunterlagen durch ein Unternehmen); die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt; die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen (oder eines Dritten) erforderlich, sofern nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.
- ***Internationaler Datenverkehr:*** Auch bei der DSGVO besteht das generelle Verbot, personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums an ein Land zu versenden, das keinen angemessenen Schutz bietet. Zum Zeitpunkt der Textabfassung hat die Europäische Komission folgende Länder in die Liste der Länder aufgenommen, die „angemessenen" Schutz bieten: US-Unternehmen, die ihren Beitritt zum EU-US-Datenschutzschild selbst zertifizieren (Hinweis: das bedeutet jedoch nicht, dass die USA als ein Land angesehen werden, das angemessenen Schutz bietet), Andorra, Argentinien, Kanada (beschränkt auf das Datenschutzgesetz PIPEDA), Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz und Uruguay. Wurde kein Beschluss über die Angemessenheit getroffen, kann die Datenübertragung nur unter bestimmten Umständen erfolgen, einschließlich auf Grundlage der Einwilligung, der Anwendung von Standardvertragsklauseln, die von der Europäischen Kommission veröffentlicht wurden, oder – im Fall von unternehmensinternen Übertragungen – der Anwendung verbindlicher unternehmensinterner Vorschriften.

Was Sie jetzt schon tun können

- Weitere Informationen erhalten Sie auf der ICO Website unter dem Bereich Datenschutzreform. Dort finden Sie auch verschiedene Leitfäden und allgemeine Hinweise. Wir empfehlen vor allem die englischsprachige Veröffentlichung der ICO „Preparing for the General Data Protection Regulation (GDPR) – 12 steps to take now".
- Überprüfen Sie, ob Ihre bestehenden Systeme für die Erhebung und Verarbeitung von personenbezogenen Daten in Einklang mit der DSGVO stehen. Vielleicht ist eine DSGVO-Prüfung aus rechtlicher, aber auch aus technologischer Perspektive angebracht?
- Sorgen Sie dafür, dass Ihre Mitarbeiter und Partner mit der DSGVO vertraut und als Vorbereitung darauf entsprechend geschult sind. Denken Sie daran, dass Sie im Rahmen der DSGVO auch für Dritte verantwortlich sind, die in Ihrem Auftrag personenbezogene Daten verarbeiten.
- Holen Sie rechtlichen Rat ein, um die Folgen der DSGVO für Ihr Unternehmen richtig einzuschätzen.

Weitere Informationen erhalten Sie unter: Sage.com/DSGVO

Sage Haftungsausschluss

Die hier enthaltenen Informationen dienen lediglich als allgemeine Anleitung. Sie sind weder geeignet noch dazu bestimmt, als rechtliche Auskunft herangezogen zu werden. Wir weisen besonders darauf hin, dass Kunden trotz dieser Informationen eigene eingehende Untersuchungen anstellen oder professionellen Rat einholen sollten, wenn sie Zweifel bezüglich der Folgen der DSGVO für ihr Unternehmen haben.

Obwohl wir alle Anstrengungen unternommen haben, um die Richtigkeit und Aktualität der Informationen auf dieser Website zu gewährleisten, übernimmt Sage keine Garantie für deren Vollständigkeit oder Richtigkeit. Die Informationen werden ohne Gewähr, das heißt ohne ausdrückliche oder stillschweigende Garantien, zur Verfügung gestellt. Sage übernimmt keine Haftung für Fehler oder Auslassungen und ist darüber hinaus nicht für Schäden jedweder Art haftbar zu machen (insbesondere Schäden aufgrund von Geschäftsausfällen bzw. entgangenen Gewinnen), die sich aus dem Vertrag, einer unerlaubten Handlung oder anderweitig aus der Nutzung oder dem Vertrauen auf diese Informationen oder aus Maßnahmen und Entscheidungen, die infolge einer Nutzung dieser Informationen ergriffen wurden, ergeben.