Creditreform Compliance

# Compliance & Risk Newsletter

## Ausgabe IV/2019
## Dezember 2019

**Inhaltsverzeichnis**

# Bessere Bekämpfung von Geldwäsche – Bundesrat gibt grünes Licht für neues Geldwäschegesetz

## Was ist ab 01.01.2020 zu beachten?

Der Bundesrat hat am 29. November 2019 dem Gesetzesentwurf zum neuen Geldwäschegesetz (GwG), den der Bundestag am 14. November 2019 beschlossen hat, zugestimmt.
Damit können die Neuregelungen zum 1. Januar 2020 in Kraft treten.

Aktuell steht noch die Unterschrift des Bundespräsidenten aus, was jedoch nur eine Formsache sein dürfte. Insofern ist davon auszugehen, dass das Gesetz noch zum Jahresende im Bundesgesetzblatt veröffentlicht wird.
Nachfolgend ein paar Hinweise auf wesentliche Änderungen:

### Inkassounternehmen

Bereits seit langem hat die Inkassobranche darum gekämpft, aus dem Kreis der Verpflichteten nach dem Geldwäschegesetz herausgenommen zu werden. In dem neuen GwG wurde dies vollzogen. In § 2 Abs. 1 Ziffer 11 wurde die Erbringung von Inkassodienstleistungen nach § 2 Abs. 2 Satz 1 des Rechtsdienstleistungsgesetzes aus dem Geltungsbereich des GwG entnommen.

### Holdinggesellschaften

Bei den Holdinggesellschaften gibt es eine Klarstellung dahingehend, dass Holdinggesellschaften, die ausschließlich Beteiligungen an Unternehmen außerhalb des Finanz- oder Versicherungssektors halten, nach dem neuen GwG nicht mehr unter den Begriff der Finanzunternehmen fallen und somit keine Verpflichtete mehr nach dem GwG (vgl. § 1 Abs. 24 GwG neu) sind. Voraussetzung ist hierbei jedoch, dass neben der Verwaltung des Beteiligungsbesitzes keine weiteren unternehmerischen Tätigkeiten verfolgt werden.

### Erweiterung des Kreises der Verpflichteten um Mietmakler

Nachdem bisher lediglich Immobilienmakler betroffen waren, die Immobilien- und Grundstückskäufe vermitteln, werden ab dem 01. Januar 2020 auch sogenannte Mietmakler von den Regelungen des GwG betroffen sein.

*© Adobe Stock / Sebastian Duda*

Was bedeutet das konkret?

Immobilienmakler müssen die Vertragsparteien geldwäscherechtlich legitimieren, wenn es sich um Mietimmobilien mit einem monatlichen Mietbetrag von 10.000 Euro und mehr oder um Kaufimmobilien handelt. Der Begriff „Miete“ ist aktuell nicht genauer definiert, es wird jedoch davon ausgegangen, dass es sich um Nettokaltmiete handelt.

Spätestens bei Übersenden des Entwurfs eines Kaufvertrages oder Mietvertrages müssen beide Parteien (Käufer und Verkäufer bzw. Mieter und Vermieter) geldwäscherechtlich legitimiert werden. Wird eine Partei dabei von einem Dritten vertreten (z.B. Geschäftsführer, Prokurist oder sonstiger Bevollmächtigter), so ist diese Person ebenfalls zu identifizieren.

Definition „legitimieren“

- Juristische Personen: Identifizierung anhand eines aktuellen Registerauszugs oder vergleichbaren Dokumenten, Ermittlung des wirtschaftlich Berechtigten (wB) und Dokumentation der Gesellschaftsstruktur
- Natürliche Personen: Identifizierung anhand eines gültigen Ausweisdokumentes (Personalausweis, Reisepass)

Weiterhin muss abgeklärt werden, ob die beteiligten Parteien eventuell als Treuhänder für einen Dritten handeln (für Rechnung eines Dritten).

Handelt es sich bei einer der beiden Parteien um eine juristische Person, so muss ebenfalls über das Transparenzregister (www.transparenzregister.de) abgeklärt werden, ob im Transparenzregister möglicherweise andere Informationen bezüglich des wB eingetragen sind, als über die Registerdaten ermittelt wurden. Bei Unstimmigkeiten ist das Transparenzregister zu informieren.

Hierzu ist eine Registrierung beim Transparenzregister notwendig. Die Abfrage kostet nach der aktuellen Gebührenordnung 4,50 EUR.

Verstöße gegen diese Vorgabe sind bußgeldbewehrt.

## Neuerung im Immobiliengeschäft für Notare

Notare sind verpflichtet, vor der Beurkundung des jeweiligen Vertragspartners die Identität des wB aufgrund der vorzulegenden Unterlagen auf Plausibilität zu prüfen!

Des Weiteren sind juristische Personen und Vereinigungen mit Sitz im Ausland verpflichtet, die Angaben zum wirtschaftlich Berechtigten aufzubewahren, aktuell zu halten und dem Transparenzregister zu melden (sofern sie dies nicht bereits an ein anderes Register in der EU übermittelt haben).

Dies ist jedoch keine Erleichterung für die Immobilienmakler, da bereits beim Vorliegen eines konkreten Kaufinteresses, also z.B. bei einer Reservierungsvereinbarung oder beim Versenden eines Vertragsentwurfes, eine Identifizierung weiterhin vorgeschrieben wird.

Somit muss die Identifizierung unabhängig von der des Notars erfolgen.

## Änderungen bei der Kundenidentifizierung durch Güterhändler

Bei Bartransaktionen ab 10.000 Euro müssen die Vertragspartner und, soweit vorhanden, die auftretende Person, identifiziert werden.

Für Edelmetallhändler (Gold, Silber oder Platin) sinkt der Betrag, ab dem eine Identifizierung durchgeführt werden muss, auf 2.000 Euro.

Das bedeutet grundsätzlich

- Juristische Personen: Identifizierung anhand eines aktuellen Registerauszugs oder vergleichbaren Dokumenten, Ermittlung des wirtschaftlich Berechtigten (wB) und Dokumentation der Gesellschaftsstruktur
- Natürliche Personen: Identifizierung anhand eines gültigen Ausweisdokumentes (Personalausweis, Reisepass)

Weiterhin muss abgeklärt werden, ob der Käufer eventuell für einen Dritten handelt.

Neben der Annahme von Bargeld (z.B. Verkauf eines PKW gegen Barzahlung, vorzeitige Ablöse) sind diese Vorgaben auch bei der Abgabe (Ankauf gegen Barzahlung) zu beachten. Auch sind eventuelle Anzahlungen in Bar mit der Restzahlung in Bar zusammenzurechnen.

## Neue Vorgabe ab 01.01.2020

Handelt es sich bei einer zu identifizierenden Person (z.B. Käufer eines PKWs) um eine juristische Person, so muss ebenfalls über das Transparenzregister (www.transparenzregister.de) abgeklärt werden, ob im Transparenzregister möglicherweise andere Informationen bezüglich des wB eingetragen sind, als über die Registerdaten ermittelt wurden. Bei Unstimmigkeiten ist das Transparenzregister zu informieren.

Hierzu ist eine Registrierung beim Transparenzregister notwendig.
Verstöße gegen diese Vorgabe sind bußgeldbewehrt.

## Erhöhtes Risiko bei Auslandsbezug (verstärkte Sorgfaltspflichten)

Ergeben sich bei der Prüfung der Vertragsparteien (nach aktuellem Stand nur bei Barzahlung, da ansonsten keine Identifizierungspflicht besteht) Hinweise darauf, dass ein Vertragspartner oder dessen wirtschaftlich Berechtigter seinen Sitz in einem Hoch-Risiko-Land (FATF-Länderliste oder Länderliste der EU) hat, so sind weitergehende Maßnahmen notwendig.
Nach dem aktuellen Gesetzestext sind in diesen Fällen folgende Punkte zu beachten:

- Einholen zusätzlicher Informationen über Vertragspartner und wB
- Information über Herkunft der Vermögenswerte und des Vermögens des Vertragspartners und des wB
- Zustimmung der Geschäftsleitung zu dem Geschäftsabschluss

## Fazit

Es ist deutlich zu erkennen, dass sich der Aufwand für die Verpflichteten auch bei dieser Gesetzesänderung wieder erhöht. Insbesondere der verpflichtende Abruf der im Transparenzregister gespeicherten Daten und die damit zusammenhängende Meldung bei eventuellen Unstimmigkeiten erhöht den Verwaltungsaufwand drastisch. Nach aktuellem Stand wird von Seiten des Transparenzregisters keine Schnittstelle angeboten, so dass ein derartiger Abgleich weitgehend manuell erfolgen muss.

Zusätzlich ergibt sich für die Betroffenen auch noch ein Kostenfaktor durch den Abruf, der entweder an den Kunden weitergegeben werden muss, oder die eigene Ertragslage beeinflusst.

*(Ralf Inderwies, Senior Consultant Compliance & AML, Creditreform Compliance Services GmbH)*

## 14,5 Millionen Euro Strafe für nicht gelöschte Daten – wie kann man das verhindern? Ist ein Löschkonzept wirklich erforderlich?

Was macht man mit nicht mehr benötigten personenbezogenen Daten? Oftmals hält man diese nicht mehr weiterhin vor und macht sich in der Alltagshektik und der Akquise des nächsten Geschäftsabschlusses keine weiteren Gedanken. Oder die IT-Systeme sind über Jahre mit der Größe des Unternehmens chaotisch gewachsen und dabei wurde verpasst, ihnen eine beherrschbare Struktur zu geben. So erging es nun der Deutschen Wohnen AG, gegen die von der Berliner Landesdatenschutzbeauftragten ein Bußgeld von 14,5 Millionen Euro verhängt wurde. Dort wurden wohl bereits jahrelang veraltete Mieterdaten einschließlich deren Sozialversicherungsdaten gespeichert und waren in Archiven als nicht löschbar und weiterhin einsehbar abgelegt.

Generell ist die fehlende Löschpraxis ein Verstoß gegen geltendes Datenschutzrecht und kann auch beim bloßen Fehlen bereits mit einem Bußgeld geahndet werden. Die DS-GVO hat mit dem Recht auf Löschung („Recht auf Vergessenwerden“) gem. Art. 17 DS-GVO die Pflicht zum Löschen personenbezogener Daten ohne Anforderung des Betroffenen zur Pflicht erhoben. Das Löschen auf Anforderung des Betroffenen allein erfüllt also nicht die geltenden rechtlichen Anforderungen. Dafür müssen funktionierende systemische Prozesse entwickelt werden. Diese regeln, wann in jeder Abteilung des Unternehmens personenbezogene Daten zu löschen sind und folgen den Grundsätzen der Datenminimierung und Datensparsamkeit. Um behördlichen Prüfungen der Datenschutzorganisation standzuhalten, müssen diese Prozesse umfassend eingehalten, dokumentiert und die Einhaltung kontrolliert werden.

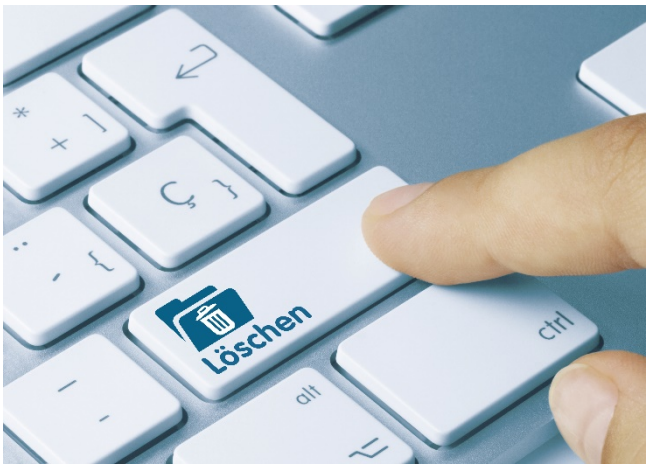
Dazu muss ein konzeptionelles Löschkonzept, das sämtliche Verarbeitungstätigkeiten beinhaltet und für die einzelnen Tätigkeiten die Speicherorte und –fristen definiert, entwickelt werden. Zwischen den einzelnen Abteilungen des Unternehmens ist ein intensiver Abstimmungsprozess erforderlich, weil oftmals keine ausreichend konkreten Informationen beim Datenschutzbeauftragten oder einem zentralen Datenschutzkoordinator zusammenlaufen. Dadurch wird die Entwicklung eines Löschkonzepts zeitaufwändiger, weil erst zahlreiche Gespräche mit den Fachabteilungen geführt werden müssen.

An diesem Punkt erschöpfen sich unserer Erfahrung nach die Inhouse-Ressourcen vieler Unternehmen. Hinzugezogene Berater können ein individuell abgestimmtes Löschkonzept entwickeln und vor Ort implementieren. Hilfreich ist dafür eine umfassende Erfahrung im Finanz-, Handels- und Industriesektor, um den unterschiedlichen Unternehmenskulturen gerecht zu werden. Neben der Koordination von verschiedenen Vorstellungen der Fachbereiche sind dabei die fachlichen Voraussetzungen eines umfassenden juristischen und IT-bezogenen Verständnisses der Berater für den Projekterfolg entscheidend.

Die personenbezogenen Daten müssen unter Beachtung etwaiger vorhandener Rechtsansprüche oder nach den gesetzlichen Aufbewahrungspflichten, wenn diese nicht vorhanden sind, nach der Erforderlichkeit zur Zweckerreichung kategorisiert werden. Die Annahme korrekter

Aufbewahrungsfristen ist sehr wichtig, weil ein Verstoß, also eine verfrühte, verspätete oder gar keine Vernichtung, Sanktionen wie Geldbußen oder eine Strafe nach sich ziehen kann.

Beispielsweise sind Handelsrechtliche Aufbewahrungsfristen i.S.d. §§ 257 HGB, 147 AO regelmäßig bei buchungs- und besteuerungsrelevanten Unterlagen zu beachten. Der Fristbeginn muss zur Fristberechnung richtig festgelegt werden, um zu wissen, wann die Frist zu laufen beginnt. Fristbeginn ist in diesen Fällen entsprechend der Rechtslage im Bürgerlichen Gesetzbuch regelmäßig der Schluss des jeweiligen Kalenderjahres.




*© Adobe Stock / momius*

Die Entwicklung und Implementierung eines Löschkonzepts sollte also mit einem konkreten Fahrplan angegangen und in allen Bereichen des Unternehmens umgesetzt werden. Das Schreiben und Ablegen bloßer Arbeitsanweisungen für Mitarbeiter genügt den Anforderungen des geltenden Datenschutzrechts nicht, auch wenn hohe Bußgelder wie gegen die Deutsche Wohnen AG bisher noch selten sind. Die Aufmerksamkeit der Datenschutzbehörden zur korrekten Entfernung nicht mehr benötigter personenbezogener Daten ist aber stark gewachsen, wie die Verhängung des Bußgeldes belegt. Riskieren Sie also nicht mit Ihrer Untätigkeit ein Tätigwerden der Behörden. Mit der Entwicklung und Implementierung eines auf Ihr Unternehmen individuell abgestimmten Löschkonzeptes stellen Sie datenschutzrechtliche Compliance her und treten Bußgeldrisiken effektiv entgegen. Die Consultants der Creditreform Compliance Services GmbH beraten Sie effektiv.

*(Alexander Schmidt, Senior Consultant Data Protection Services, Creditreform Compliance Services GmbH)*

## Auswirkungen der DSGVO auf Suchmaschinenwerbung - ist SEA datenschutzkonform?

Nach dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) sind viele Unternehmen verunsichert, ob Leadgenerierung mittels Search Engine Advertising (SEA) datenschutzkonform ist.
In diesem Beitrag erläutern wir was SEA genau ist, weshalb SEA datenschutzkonform ist und durch welche Maßnahmen auch die unterstützenden Tools von Google datenschutzkonform verwendet werden können.

### SEA was ist das?

SEA zu Deutsch Suchmaschinenwerbung, bezeichnet die bezahlte Platzierung von Werbeanzeigen auf Suchmaschinenseiten. Da Google in Deutschland einen Marktanteil von über 90% hat, wird oft auch lediglich von Google Ad Anzeigen (früher Google AdWords) gesprochen. Bei den Google Ad Anzeigen gibt es neben Textanzeigen auch Display- und Shoppinganzeigen. Für die reine Einblendung der Werbeanzeige fallen für den Werbetreibenden noch keine Kosten an, erst wenn ein Interessent auf eine der Anzeigen klickt und somit auf die hinterlegte Zielseite gelangt, fallen sogenannte Kosten pro Klick (CPC) an.

### Auswirkungen der DSGVO auf Werbung mittels SEA

In der DSGVO wird der Umgang mit personenbezogenen Daten geregelt. Sobald ein Unternehmen auf irgendeine Art und Weise personenbezogene Daten, die den Nutzern direkt oder indirekt zugeordnet werden können, wie z.B. Name, Anschrift, E-Mail-Adresse, Kontodaten oder Geburtstag sammelt und verarbeitet, findet die DSGVO Anwendung.
Beim Google-Dienst „Google Ads“ verwaltet Google als Verantwortlicher eigene Nutzerdaten, d.h. die datenschutzrechtliche Beziehung besteht lediglich zwischen der betroffenen Person und Google. Als Werbetreibender, welcher Google Ads nutzt, profitiert man somit von der großen Datenmenge, die Google bereitstellt, ohne selbst personenbezogene Daten zu sammeln oder zu verarbeiten. Da Google die Daten nicht mit den Nutzern von Google Ads teilt, hat die DSGVO keine Auswirkung auf die Suchmaschinenwerbung.

### Unterstützende Google Produkte datenschutzkonform verwenden

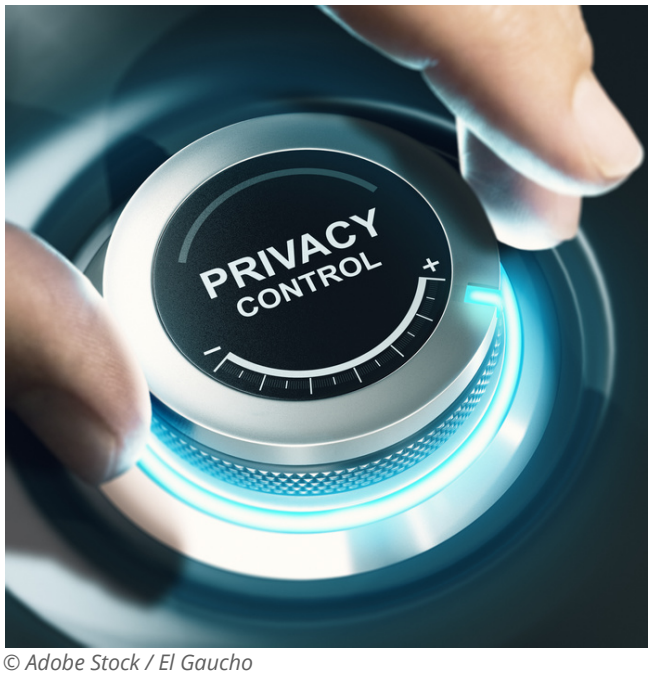
Oft wird **Google Analytics** als ergänzendes Analysetool auf der Website eines Werbetreibenden implementiert, um tiefergehende Informationen, z.B. über die Besucher, die durch Google Ads auf die Website gelangt sind, zu erhalten. Es ist von Google prinzipiell untersagt personenbezogene Daten in Analytics zu speichern, allerdings wertet Google hierbei die IP-Adresse nicht als personenbezogene Daten. Um Google Analytics datenschutzkonform zu verwenden, muss daher die IP-Adresse anonymisiert werden. Die IP-Anonymisierung kann hierbei im Google Tag Manager, im Google Analytics Universal Code, Google Analytics Classic Code sowie im gTag aktiviert werden.
Obwohl nach vorherrschender Rechtsmeinung bei der Verwendung von Google Analytics keine vorherige Zustimmung des Nutzers notwendig ist, da das Tracking der Website-Nutzung als „berechtigtes Interesse“ im Sinne der DSGVO gilt, sollten folgende Maßnahmen ergriffen werden, damit der Einsatz von Google Analytics rechtskonform ist:

- Vertrag mit Google zur Auftragsverarbeitung abschließen
- Qualifizierte Datenschutzerklärung bereitstellen
- Speicherdauer von nutzerbezogenen Daten befristen
- Individuelle Löschung von erhobenen Daten ermöglichen
- Effektive Opt-out-Möglichkeit anbieten
- Keine persönlichen Identifikationsmerkmale erfassen
- Löschung von unrechtmäßig erhobenen vergangenen Daten

In Google Analytics gibt es die Möglichkeit, erweiterte „Datenerfassung für Werbefunktionen" zu aktivieren. In den Standardeinstellungen werden Google Analytics Daten nicht mit personenbezogenen Daten aus anderen Quellen zusammengeführt, was bedeutet, dass Google kein Google-Profil den getrackten Websitebesuchern zuordnen kann. Werden die Zusatzfunktionen „Remarketing" oder „Funktionen für Werbeberichte" jedoch aktiviert, so werden die Nutzerprofile zusammengeführt. Daher sind diese Funktionen aus Datenschutzsicht kritischer zu betrachten. Da es hierzu aber noch keine konkrete Rechtsprechung gibt, setzen viele Unternehmen weiterhin, ohne vorherige Zustimmung der Nutzer, Remarketing ein, um Wettbewerbsnachteile zu vermeiden. Um auch hier gänzlich rechtskonform zu handeln, sollte man vorab die Zustimmung der Nutzer einholen und die sich daraus ergebende Einschränkungen für die Suchmaschinenwerbung in Kauf nehmen.

Um den Erfolg der Suchmaschinenwerbung zu messen, wird oftmals das **Google Ads Conversion Tracking** verwendet. Hierbei wir ein Conversion-Tracking-Tag oder ein Code-Snippet auf der Website eingebunden, welches ausgelöst wird, wenn das Ziel der Suchmaschinenwerbung, z.B. der Kauf eines Produktes, die Anmeldung zum Newsletter oder das Absenden eines Kontaktformulars, erfolgt ist. Die Verwendung des Conversion-Trackings ist datenschutzkonform, da hierbei keine personenbezogenen Daten erhoben werden. Es muss jedoch auf die Verwendung in der Datenschutzerklärung hingewiesen werden.

Der **Google Tag Manager**, welcher zur Einbindung von Tracking- und Remarketing-Codes verwendet wird, speichert selbst keine Daten. Daher müssen bei dessen Verwendung weder Maßnahmen ergriffen werden, um die Verwendung datenschutzkonform zu machen, noch muss in der Datenschutzerklärung auf die Verwendung des Tools hingewiesen werden.




*© Adobe Stock / El Gaucho*

### Weitere Punkte, die im Zusammenhang mit der DSGVO beachtet werden müssen

- SSL-Verschlüsselung der Website ist seit der DSGVO Pflicht, ebenso müssen Kontaktformulare SSL-verschlüsselt werden.
- Die Datenschutzerklärung muss explizit auf die Erhebung personenbezogener Daten, z.B. bei Erstellung von Kundenkonten und bei Bestellungen (Onlineshops) aber auch bei Versand von Werbemails und Newslettern, eingehen. Hierbei muss dargelegt werden, welche personenbezogenen Daten, für welchen Zweck, wie lange gespeichert werden.
- Bei der Verwendung von Cookies muss dies durch den Einsatz eines Cookie-Banners auf der Website erkennbar sein sowie hierzu ein Hinweis in der Datenschutzerklärung hinterlegt werden. Dabei ist inzwischen explizit ein Opt-In des Nutzers notwendig. Das heißt, dass die unterschiedlichen Cookies, durch z.B. das Setzen eines Häkchens, in einer Box vom Nutzer wissentlich erlaubt sein müssen.

### Fazit

Suchmaschinenwerbung mit Google Ads kann datenschutzkonform eingesetzt werden, wenn keine personenbezogenen Daten erfasst und verarbeitet werden. Wird in Betracht gezogen erweiterte Funktionen wie Remarketing zu verwenden, sollte im Vorfeld eine Einwilligung er Nutzer eingeholt werden.

Dieser Artikel soll einen Einblick in die datenschutzkonforme Anwendung von Suchmaschinenwerbung geben und erhebt keinen Anspruch auf Vollständigkeit und Aktualität, da sich hier täglich Neuerungen ergeben. Die im Artikel enthaltenen Empfehlungen ersetzen keine Rechtsberatung. Bei Fragen zum Datenschutz stehen Ihnen unsere Kollegen, die Experten der Creditreform Compliance Services GmbH, sehr gerne mit Rat und Tat zur Seite.
Bei der technischen Umsetzung der DSGVO auf Ihrer Website oder der datenschutzkonformen Erstellung von Suchmaschinenwerbung, ist Digitalraum Ihr richtiger Ansprechpartner.

*(Anja Brinner, Consultant, Digitalraum GmbH)*

## Impressum

**Herausgeber**

Creditreform Compliance Services GmbH

Hellersbergstraße 11

41460 Neuss

Tel: +49 2131 109-1089

Fax: +49 2131 109-81089

www.creditreform-compliance.de

info@creditreform-compliance.de

Amtsgericht Neuss HRB 4213

USt-IdNr.: DE120690803

**Geschäftsführung**

Silvia Rohe

**Redaktion, Layout und Satz**

Jasmin Falk

**Autoren dieser Ausgabe**

Ralf Inderwies, Alexander Schmidt, Anja Brinner

**Bildnachweis**

Adobe Stock

**Redaktioneller Hinweis**