



## Consumer Law | Alert

[FORWARD](#)[CONTACT](#)[SUBSCRIBE](#)[DOWNLOAD](#)

### **New consumer information obligations as of February 1, 2017 Inadequate implementation may lead to injunctive proceedings**

On February 1, 2017, new information obligations pursuant to the [German Consumer Dispute Resolution Act \(Verbraucherstreitbeilegungsgesetz\)](#) will come into effect. Under the new law, consumers must be informed of the possibility of bringing an action to a consumer arbitration entity (Verbraucherschlichtungsstelle) in case of a dispute.

#### **General information and notification obligations**

Since the [European ODR Regulation](#) became applicable last year, online traders have already been obligated to provide a link to the European [online dispute resolution platform \(ODR platform\)](#) on their websites. As of February 1, 2017, **all companies which are using general terms and conditions (Allgemeine Geschäftsbedingungen) or maintaining a website** must inform consumers of whether they are willing or legally obligated to participate in dispute resolution proceedings before a consumer arbitration entity.

The information must be easily accessible to the consumer, as well as being clear and comprehensible and must appear on the company's website or be provided together with the general terms and conditions. If both a website and general terms and conditions are used, the information must be included in both.

The information obligation applies irrespective of whether the companies actually participate in the dispute resolution proceedings or are legally required to do so. Even if a company is neither willing nor obligated to participate, it must - due to a "negative information obligation" - inform the consumers accordingly.

However, companies which did not employ more than ten persons on December 31 of the previous year are excluded from the information obligation.

Should the company be willing or required to participate, it must also refer the consumer to the relevant consumer arbitration entity as well as provide information on the entity's address and website.

### **Additional notification obligations in case of a dispute**

If a dispute with a consumer concerning an agreement between the consumer and the company arises, the company must also inform the consumer in text form of the consumer arbitration entity that the consumer may contact, should the dispute not be resolved. This obligation applies to **all companies** including those which do not maintain a website or use general terms and conditions, as well as those which do not employ more than ten persons.

In addition, the company must, once again, provide information on whether it is willing or legally required to participate in the dispute resolution proceedings before this entity.

### **List of recognized consumer arbitration entities**

The consumer arbitration entities relating to the above-mentioned obligations are to be distinguished from the online dispute resolution platform which the EU Commission operates on the basis of the European ODR Regulation. The consumer arbitration entities which the above-mentioned obligations refer to are rather those which have been recognized or established either by the Federal Office of Justice (Bundesamt für Justiz, BfJ) or pursuant to statutory regulations on the implementation of consumer arbitration proceedings. The BfJ provides a list of recognized consumer arbitration entities on its [website](#).

### **Risk of injunctive proceedings**

Companies that have not duly implemented the new obligations by February 1 2017 may be at risk of becoming subject to injunctive proceedings initiated by consumer organizations or other third parties. Consequently, there is an **immediate need for action** for all companies which have not yet adjusted their general terms and conditions or websites to the new information requirements under the German Consumer Dispute Resolution Act.

## **Authors**



**Dr. Viola Bensinger**  
+ 49 30 700171-150  
[viola.bensinger@gtlaw.com](mailto:viola.bensinger@gtlaw.com)



**Carsten Kociok**  
+ 49 30 700171-119  
[carsten.kociok@gtlaw.com](mailto:carsten.kociok@gtlaw.com)

This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. —GreenbergTraurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. — Berlin - GT Restructuring is operated by Köhler-Ma GeiserPartnerschaft Rechtsanwälte, Insolvenzverwalter. \*Operates as Greenberg Traurig Maher LLP. \*\*Greenberg Traurig is not responsible for any legal or other services rendered by attorneys employed by the strategic alliance firms. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. \*Operates as GreenbergTraurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. xGreenberg Traurig Tokyo Law Offices are operated by GTTokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of GreenbergTraurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict GreenbergTraurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2017 Greenberg Traurig, LLP. All rights reserved.



Cyber Security, Datenschutz und Krisenmanagement

Alert

[FORWARD](#)[CONTACT](#)[SUBSCRIBE](#)[DOWNLOAD](#)

Mai 2016

## Die EU-Datenschutz-Grundverordnung: Was Unternehmen beachten müssen

Nach jahrelangen Verhandlungen wurde am 4. Mai 2016 die EU-Datenschutz-Grundverordnung („DGVO“) im Amtsblatt der Europäischen Union veröffentlicht. **Die DGVO tritt am 25. Mai 2016 in Kraft und erlangt nach einer zweijährigen Übergangsphase am 25. Mai 2018 Gültigkeit.** Zugleich hebt sie mit Wirkung zum 25. Mai 2018 die bisherige Datenschutzrichtlinie 95/46/EG („Datenschutzrichtlinie“) auf.

Aufgrund der oftmals komplexen Anpassungsprozesse sollten Unternehmen, die dem Anwendungsbereich der neuen DGVO unterliegen, auf keinen Fall die zweijährige Übergangsphase abwarten, bevor sie sich mit der DGVO befassen. Vielmehr sollten sie sich bereits jetzt mit den neuen Anforderungen vertraut machen und die Umsetzung vorbereiten.

### Weltweite Geltung für Unternehmen innerhalb und außerhalb der EU

Die DGVO gilt weltweit: Betroffen sind zum einen **alle in der EU niedergelassenen Unternehmen**, die im Rahmen ihrer Tätigkeiten personenbezogene Daten verarbeiten, und zwar unabhängig davon, ob die Verarbeitung selbst in der EU erfolgt.

Daneben müssen aber auch **Unternehmen, die außerhalb der EU niedergelassen sind**, die neuen Vorgaben beachten. Dies ist dann der Fall, wenn die außereuropäischen

Unternehmen personenbezogene Daten von Personen verarbeiten, die sich in der EU befinden und die Verarbeitung im Zusammenhang damit steht:

- diesen Personen in der EU entgeltlich oder unentgeltlich Waren oder Dienstleistungen anzubieten, oder
- das Verhalten dieser Personen innerhalb der EU zu beobachten.

Letzteres umfasst insbesondere sogenannte Profiling-Maßnahmen.

Somit fällt jede **Webseite oder App**, die Waren oder Dienstleistungen gegenüber Kunden in der EU bewirbt und über die Personendaten verarbeitet werden, in den Anwendungsbereich der DSGVO. Das kann schon dann vorliegen, wenn Preise in Euro angegeben werden. Auch die **Verwendung von Cookies** oder anderen technischen Mitteln auf der Website oder App eines Anbieters, die die Erhebung von Daten über das Verhalten von in der EU ansässigen Nutzern ermöglicht, kann – wie auch bisher – eine Datenverarbeitung innerhalb der EU darstellen, auf die die DSGVO Anwendung findet.

## Die wichtigsten inhaltlichen Änderungen im Überblick

Primäres Ziel der DSGVO ist es, eine über die Datenschutzrichtlinie hinausgehende Harmonisierung der unterschiedlichen mitgliedstaatlichen Regelungen zum Datenschutz zu erreichen. Zugleich sollen die Rechte der Betroffenen gestärkt und Erleichterungen für Unternehmen eingeführt werden, die grenzüberschreitend tätig sind und somit unterschiedliche Datenschutzvorgaben verschiedener Mitgliedstaaten beachten müssen. Nachfolgend stellen wir die für Unternehmen wichtigsten Änderungen vor:

### > Einheitliche Regelungen... weitgehend

Anders als die Datenschutzrichtlinie ist die Datenschutz-Grundverordnung in allen EU-Mitgliedstaaten **direkt anwendbar**. Einer separaten Umsetzung in nationales Recht durch die einzelnen Mitgliedstaaten bedarf es nicht. Hierdurch sollen unterschiedliche nationale Regelungen vermieden werden, die auf divergierenden nationalen Umsetzungsrechtsakten beruhen.

Trotzdem finden sich in der DSGVO zahlreiche Vorschriften, die den einzelnen Mitgliedstaaten **Handlungsspielraum in Bezug auf die gesetzliche Ausgestaltung** einzelner Regelungen einräumen: Beispielsweise geht die DSGVO davon aus, dass Minderjährige erst ab 16 Jahren in die Verarbeitung ihrer personenbezogenen Daten rechtswirksam einwilligen können. Mitgliedstaaten können jedoch die Altersgrenze auf 13 Jahre herabsetzen. Daneben können die Mitgliedstaaten beispielsweise für zahlreiche Verstöße gegen die DSGVO weitere Geldbußen selbst festlegen.

### > Abschaffung der Registrierungspflicht

Die in manchen EU-Mitgliedstaaten gegenwärtig bestehende Pflicht zur Registrierung der eigenen Datenverarbeitungstätigkeit bei den nationalen Datenschutzbehörden wird unter der DSGVO abgeschafft. Die Registrierungspflicht sorgte für erheblichen Verwaltungsaufwand und Kosten, insbesondere weil sich die Anforderungen und der Ablauf der Registrierung von Land zu Land unterschieden. Ihre Abschaffung könnte daher für viele Unternehmen erhebliche Einsparungen bedeuten, insbesondere für solche Unternehmen, die in mehreren Mitgliedstaaten tätig sind.

Anstelle der Registrierungspflicht unterliegen Unternehmen zukünftig allerdings einer **Pflicht zur vorherigen Konsultation** mit der zuständigen Aufsichtsbehörde, wenn eine selbst vorzunehmende „Datenschutz-Folgenabschätzung“ zu dem Ergebnis kommt, dass die eigene Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat und das Unternehmen keine Maßnahmen zur Eindämmung dieses Risikos trifft. Die

Datenschutzbehörde wird sodann die Verarbeitung prüfen, Empfehlungen aussprechen oder, sofern nötig, andere Maßnahmen ergreifen (beispielsweise Anordnung zur Beschränkung des Verarbeitungsvorgangs, Bußgeld etc.). Soweit die Datenverarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe dient, können die Mitgliedstaaten darüber hinaus vorsehen, dass die Aufsichtsbehörde in jedem Fall zu konsultieren und eine vorherige Genehmigung einzuholen ist.

Daneben müssen sowohl verantwortliche Stellen als auch Auftragsdatenverarbeiter schriftliche oder elektronische **Verzeichnisse aller ihrer Verarbeitungstätigkeiten** führen und diese der Datenschutzbehörde auf Verlangen vorlegen. Die Aufzeichnungen müssen bestimmte Mindestinformationen wie Zweck der Verarbeitung, Kategorien von Daten und Betroffenen, Kategorien von Empfängern, denen die Daten offengelegt werden, eine allgemeine Beschreibung der vorgehaltenen technischen und organisatorischen Sicherungsmaßnahmen sowie die voraussichtliche Frist für die Löschung der Daten beinhalten. Unternehmen mit weniger als 250 Mitarbeitern trifft diese Pflicht jedoch nicht, sofern die durch sie vorgenommene Datenverarbeitung kein Risiko für die Rechte und Freiheiten der Betroffenen birgt, oder die Verarbeitung nur gelegentlich erfolgt oder nicht besonders sensible Daten betrifft.

### > **One-Stop-Shop**

Das One-Stop-Shop-Konzept soll Unternehmen, die in mehreren Mitgliedstaaten Daten verarbeiten, die Möglichkeit bieten sich nur noch an eine einzige, sogenannte **federführende Aufsichtsbehörde** zu wenden. Bisher musste sich ein Unternehmen mit allen nationalen Aufsichtsbehörden derjenigen Mitgliedstaaten auseinandersetzen, in denen es tätig ist. Nunmehr wird als federführende Aufsichtsbehörde diejenige nationale Aufsichtsbehörde zuständig sein, die für die Hauptniederlassung des Unternehmens zuständig ist.

Die federführende Behörde kann bindende Entscheidungen treffen, muss ihre Arbeit jedoch unter Einhaltung eines komplexen Koordinierungssystems mit den anderen nationalen Aufsichtsbehörden abstimmen und den Vorschlägen der anderen Aufsichtsbehörden „weitestgehend Rechnung tragen“.

Die nationalen Datenschutzbehörden werden weiterhin für Angelegenheiten zuständig sein, die sich auf ihren Mitgliedstaat beschränken. Die neue One-Stop-Shop-Struktur hat daher in erster Linie Auswirkungen auf multinational tätige Unternehmen mit Niederlassungen in mehreren EU-Ländern.

### > **Übermittlung von Daten außerhalb der EU**

Wie bisher erfordert die DSGVO das Vorliegen bestimmter Voraussetzungen, wenn personenbezogene Daten aus der EU hinaus in ein Drittland übermittelt werden sollen. Diese Voraussetzungen sind denjenigen unter der Datenschutzrichtlinie sehr ähnlich:

- Ein **Angemessenheitsbeschluss der Europäischen Kommission** stellt die Existenz eines angemessenen Datenschutzniveaus in dem Drittland fest. In diesem Zusammenhang hält die DSGVO fest, dass unter der Datenschutzrichtlinie ergangene Angemessenheitsentscheidungen unter der DSGVO weiterhin Bestand haben.

ODER

- Vorliegen einer geeigneten Datenschutzgarantie wie beispielsweise:
  - **Verbindliche interne Datenschutzvorschriften** (sogenannte **Binding Corporate Rules**, „BCR“): Soweit diese von der zuständigen Datenschutzbehörde genehmigt wurden, können die BCR die Übermittlung von Personendaten zwischen Konzernunternehmen rechtfertigen. Um die Genehmigung zu erhalten, ist allerdings ein aufwendiges Verfahren erforderlich, das bis zu zwei Jahre in Anspruch nehmen kann;

- Abschluss von **Standarddatenschutzklauseln**, die von der EU-Kommission erlassen oder genehmigt wurden;
- **Genehmigte Verhaltensregeln** gemeinsam mit verbindlichen und durchsetzbaren Verpflichtungen der verantwortlichen Stelle oder des Auftragsverarbeiters, angemessene Schutzvorkehrungen im Hinblick auf die Rechte der Betroffenen im Drittland anzuwenden; oder
- **Genehmigte Zertifizierungsmechanismen** gemeinsam mit verbindlichen und durchsetzbaren Verpflichtungen der verantwortlichen Stelle oder des Auftragsverarbeiters, angemessene Schutzvorkehrungen im Hinblick auf die Rechte des Betroffenen im Drittland anzuwenden.

ODER

- Vorliegen einer „**Ausnahme für bestimmte Fälle**“ wie beispielsweise:
  - ausdrückliche **Einwilligung** des Betroffenen in die Datenübermittlung, nachdem er über die möglichen Risiken unterrichtet wurde;
  - die Übermittlung ist **zur Erfüllung eines mit dem Betroffenen geschlossenen Vertrags** erforderlich;
  - die Übermittlung ist für den Abschluss oder zur Erfüllung eines mit einem Dritten **im Interesse des Betroffenen geschlossenen Vertrags** erforderlich.

### > **Rechtmäßigkeit der Datenverarbeitung**

Wie bisher bedarf die Verarbeitung personenbezogener Daten einer Rechtfertigungsgrundlage, die sich entweder aus Gesetz oder aus der Einwilligung des Betroffenen ergeben kann. Die jeweiligen Voraussetzungen entsprechen weitgehend denjenigen unter der Datenschutzrichtlinie. Allerdings gibt es auch verschiedene Neuerungen. Die wichtigsten gesetzlichen Fallgruppen, die eine Datenverarbeitung rechtfertigen, sind:

- Die Verarbeitung ist **für die Erfüllung eines Vertrags** mit dem Betroffenen oder zur Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen **erforderlich**. (Diese Regelung entspricht den bisherigen Vorgaben.)
- Die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung erforderlich**, welcher der Verantwortliche unterliegt. (Diese Regelung entspricht ebenfalls den bisherigen Vorgaben. Die Mitgliedstaaten haben hier aber die Möglichkeit, die einzelnen Anforderungen präziser zu bestimmen.)
- Die Verarbeitung ist **zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten** erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen.

Hier gibt es eine **wesentliche Neuerung**: Das berechtigte Interesse kann auch darin liegen, personenbezogene Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke (z.B. zur Verarbeitung von Kunden- oder Beschäftigendaten) zu übermitteln. Die DSGVO führt hiermit ein **allgemeines Konzernprivileg** ein, das zumindest in Deutschland so bisher nicht bestand. Zugleich grenzt sie das Konzernprivileg aber auch wieder ein, indem sie bestimmt, dass die Datenübertragung zu einem verbundenen Unternehmen nur dann zulässig ist, wenn die Interessen oder Grundrechte und Grundfreiheiten der jeweils Betroffenen nicht überwiegen. Letzteres könnte etwa der Fall sein, wenn die übermittelten Daten beim Datenempfänger nicht ausreichend gegen Missbrauch geschützt werden.

Wird die Verarbeitung auf eine **Einwilligung des Betroffenen** gestützt, so muss die Einwilligung von dem Betroffenen wie bisher auch **freiwillig** für den konkreten Fall, **in informierter Weise** und **unmissverständlich** ausdrücklich oder konkludent abgegeben werden. Bei einer schriftlichen Erklärung, die auch andere Angelegenheiten betrifft, muss die Einwilligung nun zudem in einer **verständlichen und leicht zugänglichen Form** sowie in einer **klaren und einfachen Sprache** formuliert sein. Außerdem ist die Einwilligung so

darzustellen, dass sie sich **deutlich von den anderen Angelegenheiten unterscheidet**.

Die DSGVO schreibt ferner vor, dass die im Rahmen von E-Commerce-, Social-Media-, Content- oder Informationsdiensten abgegebene **Einwilligung von Minderjährigen** in die Verarbeitung ihrer personenbezogenen Daten nur wirksam ist, wenn diese das 16. Lebensjahr (oder ggf. das 13. Lebensjahr) vollendet haben. Anderenfalls ist die Einwilligung oder Zustimmung des Erziehungsberechtigten erforderlich.

Seine Einwilligung kann der Betroffene jederzeit mit Wirkung für die Zukunft **widerrufen**. Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein.

### > **Meldepflichten bei Verstößen**

Bei einer „Verletzung des Schutzes personenbezogener Daten“ sieht die DSGVO **zwei verschiedene Meldepflichten** des Verantwortlichen vor: einmal gegenüber der Datenschutzbehörde und einmal gegenüber den Betroffenen.

Die **Datenschutzbehörde** muss „unverzüglich“ und „möglichst binnen 72 Stunden“ informiert werden, nachdem die Verletzung bekannt wurde, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Hat die Verletzung voraussichtlich ein „hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen“ zur Folge und greift keine der in der DSGVO geregelten Ausnahmen, so muss der Verantwortliche auch den **Betroffenen** unverzüglich von der Verletzung benachrichtigen.

### > **Datenschutzbeauftragter**

Die DSGVO verpflichtet Unternehmen, deren Kerntätigkeit eine der folgenden Aktivitäten umfasst, einen Datenschutzbeauftragten zu bestellen:

- die umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen;
- die umfangreiche Verarbeitung sensibler Daten; oder
- die umfangreiche Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten.

Die Verpflichtung zur Bestellung des Datenschutzbeauftragten gilt unabhängig von der Anzahl der Mitarbeiter, die innerhalb des Unternehmens mit der Verarbeitung von Daten beschäftigt sind. Die in Deutschland gegenwärtig geltende 9-Personen-Grenze wurde nicht in die DSGVO übernommen. Allerdings können die Mitgliedstaaten weitere Umstände festlegen, unter denen Unternehmen, die nicht in eine der vorgenannten Kategorien fallen, ebenfalls einen Datenschutzbeauftragten bestellen müssen.

Anders als bisher sind die Kontaktdaten des Datenschutzbeauftragten **der Aufsichtsbehörde mitzuteilen**. Ein weiterer Unterschied besteht darin, dass Unternehmensgruppen zukünftig einen **gemeinsamen Konzern-Datenschutzbeauftragten** bestellen können.

### > **Geldbußen**

Bei Verstößen kann die zuständige Aufsichtsbehörde Geldbußen von **bis zu 20 Millionen Euro** oder im Fall eines Unternehmens von bis zu **4% seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängen.

Daneben eröffnet die DSGVO den Mitgliedstaaten die Möglichkeit, Verstöße gegen die DSGVO zusätzlich zu sanktionieren.

## Die nächsten Schritte

Unternehmen sollten die zweijährige Übergangsfrist nutzen, um sich auf die veränderten Anforderungen einzustellen. Der Anpassungsaufwand an die Vorgaben der DSGVO sollte dabei nicht unterschätzt werden. Zugleich bleibt abzuwarten, ob und wie die Mitgliedstaaten ihre Befugnisse zur ergänzenden Gesetzgebung ausgestalten und ob die Datenaufsichtsbehörden die Übergangsfrist nutzen, um bisher noch unbestimmte Rechtsbegriffe (wie beispielsweise das „hohe Risiko“ bei Verletzungen der Datensicherheit) näher zu definieren.

Insgesamt dürfte die Umsetzung der DSGVO eine beachtliche Aufgabe darstellen und eine koordinierte Zusammenarbeit und Abstimmung zwischen der Wirtschaft und den Regierungen auf der einen und den Datenaufsichtsbehörden auf der anderen Seite erfordern.

Dieser GT Alert wurde erstellt von:



**Dr. Viola Bensinger**  
Partnerin  
+49 (0) 30 700 171 150

EMAIL



**Carsten Kociok**  
Senior Associate  
+49 (0) 30 700 171 119

EMAIL

Fragen hierzu können Sie an die Verfasser oder gerne auch an folgende Praxisgruppenmitglieder aus unseren internationalen Büros richten:

- [Françoise Gilbert](#) | Silicon Valley | +1 650.804.1235 | [gilbertf@gtlaw.com](mailto:gilbertf@gtlaw.com)
- [Ian C. Ballon](#) | Silicon Valley/Los Angeles | +1 650.289.7881 | [ballon@gtlaw.com](mailto:ballon@gtlaw.com)
- [Luke Dixon](#) | London | +44 (0) 203 349 8756 | [dixonl@gtmlaw.com](mailto:dixonl@gtmlaw.com)
- [Lori S. Nugent](#) | Dallas | +1 214.665.3630 | [nugentl@gtlaw.com](mailto:nugentl@gtlaw.com)
- [Radboud Ribbert](#) | Amsterdam | +31 (0) 20 301 7333 | [ribbertr@eu.gtlaw.com](mailto:ribbertr@eu.gtlaw.com)
- [Elizabeth C. Rogers](#) | Austin | +1 512.320.7256 | [rogersel@gtlaw.com](mailto:rogersel@gtlaw.com)
- [Alan N. Sutin](#) | New York | +1 212.801.9286 | [sutina@gtlaw.com](mailto:sutina@gtlaw.com)

This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. -GreenbergTraurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. - Berlin - GT Restructuring is operated by Köhler-Ma GeiserPartnerschaft Rechtsanwälte, Insolvenzverwalter. \*Operates as Greenberg Traurig Maher LLP. \*\*Greenberg Traurig is not responsible for any legal or other services rendered by attorneys employed by the strategic alliance firms. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. \*Operates as GreenbergTraurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. xGreenberg Traurig Tokyo Law Offices are operated by GTTokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of GreenbergTraurig, P.A. and Greenberg Traurig, LLP.

Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict GreenbergTraurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2017 Greenberg Traurig, LLP. All rights reserved.

To manage your interest area subscriptions, please click [here](#).