

DATENSCHUTZERKLÄRUNG BEZÜGLICH DER VERARBEITUNG PERSONENBEZOGENER DATEN IM RAHMEN DER PRÄVENTIONSPFLICHTEN ZUR BEKÄMPFUNG VON GELDWÄSCHE UND TERRORISMUSFINANZIERUNG SOWIE DES UBO-REGISTERS

A. EINLEITUNG - GESETZLICHE VERPFLICHTUNGEN

Im Rahmen der Präventionspflichten zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung sieht das novellierte Gesetz vom 10. Juni 1999 über die Organisation des Berufs der Buchhalter, insbesondere im Sinne des novellierten Gesetzes vom 12. November 2004 (im Folgenden "AML/CFT-Gesetz"), zur Umsetzung der Richtlinie 2015/849, das Gesetz vom 27. Oktober 2010, das Gesetz vom 13. Februar 2018 sowie der großherzogliche Erlass vom 29. Oktober 2010 zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung folgende berufliche Verpflichtungen vor:

- Die Verpflichtung, *die Kunden zu kennen*, gemäß Artikel 3 des Gesetzes vom 12. November 2004;
- Die Verpflichtung zur *Zusammenarbeit mit den Behörden* gemäß Artikel 5 des Gesetzes vom 12. November 2004.

In diesem Zusammenhang sind wir als Buchhalter dazu verpflichtet, Geldwäsche- und Terrorismusfinanzierungsrisiken zu identifizieren und zu bewerten. Wir sind dazu verpflichtet, die durchgeführten Risikobewertungen zu dokumentieren, zu aktualisieren und den Aufsichts- und Selbstregulierungsbehörden gegebenenfalls zur Verfügung zu stellen.

Die Sorgfaltspflicht, die uns auferlegt ist und die wir vor Beginn einer Geschäftsbeziehung, zum Zeitpunkt des Eingehens einer Geschäftsbeziehung und während der gesamten Geschäftsbeziehung, insbesondere wenn sich die Situation des Kunden ändert, ausüben müssen, umfasst:

- Die Identifikation des Kunden und die Überprüfung seiner Identität;
- Die Identifizierung des wirtschaftlich Berechtigten sowie die Identifizierung von Eigentums- und Kontrollstrukturen in Bezug auf juristische Personen;
- Die Identifizierung und Bewertung des Zwecks und der beabsichtigten Art der Geschäftsbeziehung;
- Eine ständige Wachsamkeit im Rahmen der Geschäftsbeziehung, insbesondere durch Prüfung der abgeschlossenen Geschäfte und gegebenenfalls der Herkunft der finanziellen Mittel.

Das "AML/CFT-Gesetz" verpflichtet uns in unserer Eigenschaft als Buchhalter und Steuerberater, auf jede rechtliche Anfrage der Strafverfolgungsbehörden in Ausübung ihrer Befugnisse so umfassend wie möglich zu reagieren und mitzuwirken.

Als Buchhalter und Steuerberater sind wir auch dazu verpflichtet, uneingeschränkt mit den für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung zuständigen luxemburgischen Behörden zusammenzuarbeiten, indem wir diesen Behörden auf deren Verlangen alle erforderlichen Informationen nach den in den geltenden Rechtsvorschriften vorgesehenen Verfahren zur Verfügung stellen und aus eigener Initiative die Financial Intelligence Unit der Staatsanwaltschaft beim Bezirksgericht Luxemburg über jeden Sachverhalt informieren, der auf eine Terrorismusfinanzierung hindeuten könnte.

Als Buchhalter und Steuerberater in Luxemburg unterliegen wir auch den Verpflichtungen aus dem AML/CFT-Gesetz.

B. VERARBEITUNG PERSONENBEZOGENER DATEN

1. Der Zweck der Verarbeitung und die Rechtsgrundlage der Verarbeitung:

1.1. Der Zweck:

Die beruflichen Verpflichtungen aus dem "AML/CFT-Gesetz" beinhalten, dass NEOVIAQ (im Folgenden auch "wir" genannt) in unserer Eigenschaft als Buchhalter und Steuerberater bestimmte Sie betreffende personenbezogene Daten im Sinne der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden auch "DGMP" genannt) verarbeiten muss.

Personenbezogene Daten, die auf der Grundlage des "AML/CFT-Gesetzes" erhoben werden, dürfen nur zum Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Die Verarbeitung dieser personenbezogenen Daten für andere Zwecke ist untersagt.

Schließlich können personenbezogene Daten, die auf der Grundlage des in Punkt 1.1 beschriebenen Zwecks erhoben und verarbeitet werden, in Ihrem Namen für die Erstellung Ihres UBO-Registers verwendet werden.

1.2. Die Rechtsgrundlage:

Die Rechtsgrundlage für die Verarbeitung ist eine rechtliche Verpflichtung im Sinne von Artikel 6 Absatz 1 Buchstabe c) der DSGVO. Ohne die Verarbeitung einiger Ihrer personenbezogenen Daten auf der Grundlage des "AML/CFT-Gesetzes" können wir keine Geschäftsbeziehung mit Ihnen abschließen oder gegebenenfalls fortsetzen. In solchen Fällen verpflichtet uns die Gesetzgebung, entweder keine Geschäftsbeziehung einzugehen, keine Transaktion durchzuführen oder die Geschäftsbeziehung zu beenden und gegebenenfalls einen verdächtigen Transaktionsbericht an die Financial Intelligence Unit zu übermitteln.

Der Hauptzweck dieses Dokuments ist es, Sie darüber zu informieren, wie wir Ihre personenbezogenen Daten im Rahmen unserer gesetzlichen Verpflichtungen zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung verarbeiten, und Sie über Ihre Rechte im Zusammenhang mit dem Schutz Ihrer Privatsphäre zu informieren.

2. Die Kategorien der verarbeiteten Daten:

Im Rahmen der Erfüllung unserer gesetzlichen Verpflichtungen zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung sind wir verpflichtet, vor allem die folgenden Datenkategorien zu verarbeiten:

- **Grundlegende Identifikationsdaten:** Nachname; Vorname; Geburtsdatum; Geburtsort; Adresse; Nationalität; Wohnsitz oder Sitz; offizielle nationale Identifikationsnummer; Kopie eines gültigen Ausweises; familiäre Bindungen; besondere Informationen über Eltern, Verwandte, etc.

- **Daten zur beruflichen Tätigkeit:** z. B. Beruf, Handelsermächtigungen, die Tatsache, dass ein Mandat in einer Gesellschaft oder Vereinigung ausgeübt wird oder dass man Aktionär ist; etc.
- **Einkommensquellen/finanzielle Mittel (Beruf/Tätigkeit):** Einkommensquelle; Vermögensbestand; etc.
- Gegebenenfalls **Adressnachweis und Geburtsdatum:** aktuelle Kontoauszüge; aktuelle Rechnung (Gas, Wasser, Strom); etc.
- **Einige spezifische Daten:** die Tatsache, ein politisches Mandat oder eine politische Funktion auszuüben; die Tatsache, eine politisch exponierte Person zu sein (PEP); einige Daten über strafrechtliche Verurteilungen und andere Straftaten (z.B. Steuerbetrug); usw.

3. Filtern von Namen mit PSA-Listen und / oder schwarzen Listen (Profiling und potenziell sensible Daten):

In Übereinstimmung mit dem "AML/CFT-Gesetz" können wir, wenn wir es für notwendig halten, prüfen, ob unsere Kunden politisch exponierte Personen (nachfolgend "PEPs" genannt) sind oder deren Namen auf schwarzen Listen geführt werden. Dazu nutzen wir einen externen Lieferanten: "Dow Jones Riskcenter".

3

Zu den Quellen, die das Dow Jones Riskcenter für diese Berichte verwendet, gehören Regierungs- und andere offizielle Websites, Regierungsverzeichnisse, Riskcenter (das Informationsarchiv von Dow Jones mit fast 33.000 Quellen, einschließlich Nachrichtenagenturen, Zeitungen, Zeitschriften, Pressemitteilungen und anderen, die die letzten 30 Jahre abdecken), andere Online-Zeitungen und -Magazine, die nicht im Dow Jones Riskcenter verfügbar sind, Print- oder Online-Verzeichnisse und Websites für Geschäftsdaten.

Wir weisen Sie daher darauf hin, dass die Berichte des Dow Jones Risk Centers besondere Kategorien von personenbezogenen Daten im Sinne der Artikel 9 und 10 der DSGVO enthalten können, insbesondere: politische Meinungen, Daten über strafrechtliche Verurteilungen und andere Straftaten (z. B. Steuerbetrug), Familienbeziehungen, die wir im Rahmen unserer gesetzlichen Verpflichtungen zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung verarbeiten müssen.

Darüber hinaus möchten wir darauf hinweisen, dass Sie zwar das Recht haben, nicht Gegenstand einer automatisierten Einzelentscheidung, einschließlich der Erstellung von Profilen, zu sein, dies aber eine für den Abschluss eines Vertrages erforderliche Praxis ist (Artikel 22, §2, a), der DSGVO), die durch das Recht der Europäischen Union (Artikel 22, §2, b), der DSGVO) auferlegt und genehmigt wurde. Darüber hinaus heißt es in Erwägungsgrund 71 der DSGVO eindeutig, dass: "(...) die Entscheidungsfindung auf der Grundlage einer solchen Verarbeitung, einschließlich der Erstellung von Profilen, zulässig sein sollte, wenn sie nach dem Unionsrecht ausdrücklich genehmigt ist (...), auch zum Zwecke der Kontrolle und Verhütung von Betrug und Steuerhinterziehung (...)".

In Anbetracht all dieser Punkte haben wir angemessene Sicherheitsvorkehrungen getroffen, um Ihre Privatsphäre bestmöglich zu schützen.

4. Die betroffenen Personen:

Im Rahmen der Erfüllung unserer gesetzlichen Verpflichtungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung sind wir dazu verpflichtet, hauptsächlich Daten der folgenden Kategorien von betroffenen Personen zu verarbeiten:

- Unsere Kunden, ihre Mitarbeiter, Vertreter und deren Angehörige (Familienbeziehungen);
- Potentielle Kunden, ihre Mitarbeiter, ihre Vertreter und deren Angehörige (Familienbeziehungen);
- Die wirtschaftlichen Eigentümer bzw. Endberechtigten, Gesellschafter und Geschäftsführer unserer Kunden / potentiellen Kunden.

5. Die Empfänger:

Insofern es nicht notwendig ist, personenbezogene Daten an Organisationen oder Einrichtungen weiterzugeben, deren Intervention als Drittspielstelle für die oben genannten Zwecke erforderlich ist (z.B. ein Notar im Rahmen einer Unternehmensgründung), geben wir die gesammelten personenbezogenen Daten nicht an externe Organisation oder Einrichtung weiter.

4

Wir müssen personenbezogene Daten auf Anfrage einer rechtlich zuständigen Behörde oder aus eigener Initiative übermitteln, wenn wir in gutem Glauben der Ansicht sind, dass die Übermittlung dieser Informationen notwendig ist, um die Gesetze oder Vorschriften einzuhalten oder unsere Rechte oder unser Eigentum zu schützen.

In diesem Zusammenhang erinnern wir Sie daran, dass wir gesetzlich verpflichtet sind, der Financial Intelligence Unit der Staatsanwaltschaft beim Bezirksgericht Luxemburg jeden Sachverhalt mitzuteilen, der auf Geldwäsche oder Terrorismusfinanzierung hinweisen könnte. Ebenso sind wir gesetzlich verpflichtet, auf jede rechtliche Anfrage, die die für die Umsetzung des "AML/CFT-Gesetzes" zuständigen Behörden in Ausübung ihrer Befugnisse an uns richten, so umfangreich wie möglich zu reagieren und mitzuwirken.

Wir weisen darauf hin, dass gemäß Artikel 5 Absatz (4) und (5) des "AML/CFT-Gesetzes":

- Das Berufsgeheimnis nicht für die Financial Intelligence Unit gilt;
- Wir und unsere Führungskräfte und Mitarbeiter Kunden oder Dritten gegenüber nicht offenlegen dürfen, dass Informationen gemäß dem "AML/CFT-Gesetz" an Behörden weitergegeben oder zur Verfügung gestellt werden oder dass eine Untersuchung der Financial Intelligence Unit bezüglich Geldwäsche oder Terrorismusfinanzierung läuft oder eingeleitet werden kann.

Schließlich müssen wir bei Transaktionen oder Geschäftsbeziehungen mit politisch exponierten oder neu exponierten Personen die Genehmigung der höheren Hierarchie einholen, bevor wir in einem solchen Fall mit dem Kunden eine Geschäftsbeziehung eingehen oder unterhalten können. In diesem Zusammenhang sind wir verpflichtet, dieser Kategorie von Empfängern gewisse personenbezogene Daten mitzuteilen.

6. Aufbewahrungsfristen:

Gemäß Artikel 3 Absatz (6) des "AML/CFT-Gesetzes" sind wir verpflichtet, Dokumente, Daten und Informationen bezüglich der Verhinderung und Aufdeckung möglicher Geldwäsche oder Terrorismusfinanzierung sowie die damit zusammenhängenden Untersuchungen der für die Bekämpfung der Geldwäsche und der Terrorismusfinanzierung zuständigen luxemburgischen Behörden aufzubewahren:

- Im Hinblick auf Kunden-Due-Diligence-Maßnahmen eine Kopie oder Verweise auf die Dokumente, Daten und Informationen, die zur Erfüllung der Kunden-Due-Diligence-Verpflichtungen erforderlich sind, für eine Dauer von fünf Jahren nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Datum der gelegentlich abgeschlossenen Transaktion;
- Belege und Transaktionsaufzeichnungen, die zur Identifizierung oder Rekonstruktion von Transaktionen erforderlich sind, für eine Dauer von fünf Jahren nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Datum des gelegentlich abgeschlossenen Geschäfts.

Wir sind ebenfalls verpflichtet, Informationen über die Maßnahmen zur Identifizierung von wirtschaftlich Berechtigten aufzubewahren.

5

Die Aufsichtsbehörden können im Einzelfall verlangen, dass wir die Daten für einen zusätzlichen Zeitraum, der fünf Jahre nicht überschreiten darf, aufzubewahren, wenn dies für die Erfüllung ihrer Aufgaben gemäß des "AML/CFT-Gesetzes" erforderlich ist.

Schließlich können wir personenbezogene Daten für einen weiteren Zeitraum von fünf Jahren speichern, wenn dies für die wirksame Umsetzung interner Maßnahmen zur Verhinderung oder Aufdeckung von Geldwäsche oder Terrorismusfinanzierung erforderlich ist.

Unbeschadet längerer Aufbewahrungsfristen, die durch andere Gesetze vorgeschrieben sind, sind wir verpflichtet, personenbezogene Daten nach Ablauf der oben genannten Aufbewahrungsfristen zu löschen.

7. Sicherheitsmaßnahmen

Wir setzen eine Reihe von technischen und organisatorischen Maßnahmen ein, um Ihre personenbezogenen Daten zu schützen und um das Risiko der Zerstörung, des Verlusts, der Veränderung, der Offenlegung, des Zugriffs oder der unbefugten Verarbeitung dieser Daten, sei es versehentlich oder unrechtmäßig, zu begrenzen.

Diese Maßnahmen, die darauf abzielen, ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, und die physischen, elektronischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit, Genauigkeit und Aktualisierung Ihrer personenbezogenen Daten umfassen, können konkret Folgendes beinhalten:

- Aus- und Weiterbildung des zuständigen Personals, damit es über unsere Verpflichtung zum Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten informiert ist;
- Technologische Sicherheitsmaßnahmen wie Firewalls, Verschlüsselung und Antivirenssoftware;
- Mittel zur Gewährleistung der ständigen Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von Datenverarbeitungssystemen und -diensten (wie Zugangskontrollen zu Einrichtungen, Medien, Speichermedien, organisatorische Maßnahmen bzgl. Zugang, Übertragung, Einführung, Transport, usw. von Daten);
- Backup Dienste, um die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Vorfalls innerhalb angemessener Fristen wiederherzustellen.

8. Ihre Rechte:

8.1. Auflistung der Rechte :

Vorbehaltlich des Umfangs der durch die "DSGVO" vorgesehenen Rechte und der diesbezüglichen gesetzlichen Ausnahmen hat die betroffene Person folgende Rechte:

6

- eine Liste der personenbezogenen Daten zu erhalten, die wir über Sie gespeichert haben (**Zugangsrecht**).
- zu beantragen, dass die von uns über Sie gespeicherten personenbezogenen Daten aktualisiert, korrigiert oder vervollständigt werden (**Recht auf Berichtigung**).
- vorbehaltlich der in Artikel 17 der DSGVO enthaltenen Bedingungen, die Löschung der Sie betreffenden personenbezogenen Daten zu beantragen (**Recht auf Vergessen**).
- unter Beachtung der gesetzlichen Bestimmungen, denen wir unterliegen, zu verlangen, dass wir die von uns über Sie gespeicherten personenbezogenen Daten löschen oder die Art und Weise, wie wir diese personenbezogenen Daten verwenden, einschränken (**Recht auf Einschränkung**).
- Ihre Einwilligung in die Verarbeitung Ihrer personenbezogenen Daten zu widerrufen, soweit diese auf einer Einwilligung beruht (**Recht auf Widerruf der Einwilligung**).
- eine Kopie der Sie betreffenden personenbezogenen Daten, die Sie uns zur Verfügung gestellt haben, in strukturierter, allgemein gebräuchlicher und maschinenlesbarer Form zu erhalten und an Dritte weiterzugeben, soweit die Verarbeitung auf Ihrer Zustimmung oder einem Vertrag beruht (**Recht auf Datenübertragbarkeit**).
- der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen (**Widerspruchsrecht**).
- Wenn Sie mit der Art und Weise, wie wir mit Ihren personenbezogenen Daten umgehen, nicht zufrieden sind, haben Sie das Recht, eine Beschwerde bei der zuständigen Aufsichtsbehörde einzureichen. Wenn Sie an die zuständige Aufsichtsbehörde verwiesen werden möchten, kontaktieren Sie uns bitte wie unten angegeben (**Recht zur Einreichung einer Beschwerde bei der zuständigen Aufsichtsbehörde**):

In Luxemburg ist die zuständige Aufsichtsbehörde die „Commission nationale pour la protection des données“ ([CNPD](#)):

Wenn Sie eine Beschwerde einreichen möchten, wird dringend empfohlen, [das Online-Formular zu verwenden](#), das unter <https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html> verfügbar ist.

Die Verwendung dieses Formulars wird es uns ermöglichen, Ihre Anfrage schneller zu bearbeiten.

Sie können sich auch entscheiden, das Formular auszudrucken und von Hand auszufüllen.

In diesem Fall senden Sie es bitte an die folgende Adresse:

Nationale Datenschutzkommission CNPD - Beschwerdeservice

1, Avenue du Rock'n'Roll, Avenue du Rock'n'Roll.

L-4361 Esch-sur-Alzette

Tel: (+352) 26 10 60 1

Fax. : (+352) 26 10 60 29

8.2. Einschränkung Ihres Zugangsrechts:

7

Gemäß Artikel 14 des Gesetzes vom 1. August 2018 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in Strafsachen sowie in Fragen der nationalen Sicherheit kann Ihr Recht auf Zugang eingeschränkt und/oder verweigert werden:

a) um die Beeinträchtigung von Untersuchungen, Nachforschungen, behördlichen oder gerichtlichen Verfahren zu vermeiden;

b) zur Vermeidung von Eingriffen in die Verhütung, Ermittlung, Aufdeckung, Verfolgung von Straftaten.

In diesem Fall werden wir Sie so schnell wie möglich schriftlich über eine Verweigerung oder Einschränkung des Zugangs sowie über die Gründe für die Verweigerung oder Einschränkung informieren.

Diese Informationen dürfen jedoch nicht weitergegeben werden, wenn ihre Offenlegung eines der in den Buchstaben a) und b) genannten Ziele gefährden könnte.

Wir werden Sie auch über die Möglichkeiten informieren, bei der zuständigen Aufsichtsbehörde eine Beschwerde einzureichen oder eine gerichtliche Beschwerde einzulegen.