AMT FÜR INFORMATIK
FÜRSTENTUM LIECHTENSTEIN

Vertraulichkeitserklärung, Non-Disclosure Agreement (NDA)

Name/ Vorname

Geboren am

Mitarbeitende/r der Organisation (Dienstleister)

verpflichtet sich als Dienstleister gegenüber der Liechtensteinischen Landesverwaltung bezüglich aller Wahrnehmungen aus dem Funktionsbereich des Auftraggebers absolutes Stillschweigen zu bewahren, insbesondere über:

a. den spezifischen Inhalt der Tätigkeiten für den Auftraggeber (Aufträge, Unterhalt, etc.);
b. dem Datenschutz unterliegende personenbezogene Daten;
c. den Verschwiegenheitspflichten des Auftraggebers unterliegende Informationen;
d. der amtlichen Tätigkeit des Auftraggebers entstammende Informationen;
e. Informationen betreffend ausgeführte Tätigkeiten in den Gebäuden des Auftraggebers;
f. Informationen im Zusammenhang mit Unterhalts-, Abklärungs-, Prüfungs- und anderen Arbeiten für den Auftraggeber.

Der Auftraggeber ist gesetzlich zur Verschwiegenheit verpflichtet über alle ihm aus der amtlichen Tätigkeit bekannt gewordenen Tatsachen. Er hat daher ein gesetzlich verankertes Interesse daran, dass vertrauliche Informationen über amtliche Tätigkeiten oder diesbezügliche Sicherheitsvorkehrungen unberechtigten Dritten nicht offengelegt werden und datenschutzrechtliche Bestimmungen eingehalten werden.

Der Dienstleister verpflichtet sich, über alle ihm offen gelegten Informationen, das fachliche Know-how sowie Amts-, Geschäfts-, Berufs- und Betriebsgeheimnisse, die er im Rahmen von Arbeiten beim oder für den Auftraggeber erfährt, Stillschweigen zu bewahren und Dritten weder ganz noch auszugsweise zugänglich zu machen. Die Vertraulichkeit ist schon vor Beginn des Vertragsabschlusses zu wahren und bleibt auch nach Beendigung des Vertragsverhältnisses bestehen. Vorbehalten bleiben gesetzliche Aufklärungspflichten.

Eine Verletzung der Verschwiegenheitspflicht kann strafrechtlich relevantes Verhalten darstellen und bestraft werden. Entsprechende, jedoch nicht abschliessend aufgeführte Gesetzesbestimmungen sind im Anhang dieser Erklärung aufgeführt. Ferner kann jede Verletzung der Verschwiegenheitspflicht, die beim Auftraggeber oder einem Dritten zu einem Schaden führt, zivilrechtliche Folgen haben. Der/Die Unterzeichnende bestätigt, von den im Anhang aufgeführten Gesetzesbestimmungen Kenntnis genommen zu haben, und erklärt, sich im vollen Umfang an diese Vertraulichkeitserklärung zu halten.

Ort, Datum ..... Unterschrift .....

Anhang – Auszug strafrechtlich relevanter Bestimmungen

§ 118a Strafgesetzbuch (Widerrechtlicher Zugriff auf ein Computersystem)

Abs. 1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,

1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder

2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,

3. ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Wer die Tat in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Ziff. 10) ist, begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Abs. 3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Abs. 4) Wer die Tat nach Abs. 1 im Rahmen einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu zwei Jahren, wer die Tat nach Abs. 2 im Rahmen einer kriminellen Vereinigung begeht, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

§ 119 Strafgesetzbuch (Verletzung des Kommunikationsgeheimnisses)

Abs. 1) Wer in der Absicht, sich oder einem anderen Unbefugten von einer im Wege eines elektronischen Kommunikationsnetzes übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung an einer Kommunikations- oder einer Datenverarbeitungsanlage anbringt oder sonst empfangsbereit macht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Ebenso ist zu bestrafen, wer eine Vorrichtung, die an einer Kommunikations- oder einer Datenverarbeitungsanlage angebracht oder sonst empfangsbereit gemacht worden ist, in der im Abs. 1 bezeichneten Absicht benützt.

Abs. 3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

§ 119a Strafgesetzbuch (Missbräuchliches Abfangen von Daten)

Abs. 1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

§ 122 Strafgesetzbuch (Verletzung eines Geschäfts- oder Betriebsgeheimnisses)

Abs. 1) Wer ein Geschäfts- oder Betriebsgeheimnis (Abs. 3) offenbart oder verwertet, das ihm bei seiner Tätigkeit in Durchführung einer durch Gesetz oder behördlichen Auftrag vorgeschriebenen Aufsicht, Überprüfung oder Erhebung anvertraut oder zugänglich geworden ist, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

Abs. 2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Abs. 3) Unter Abs. 1 fällt nur ein Geschäfts- oder Betriebsgeheimnis, das der Täter kraft Gesetzes zu wahren verpflichtet ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des von der Aufsicht, Überprüfung oder Erhebung Betroffenen zu verletzen.

Abs. 4) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.

Abs. 5) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 3) zu verfolgen.

§ 123 Strafgesetzbuch (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses)

Abs. 1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Abs. 2) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen.

§ 124 Strafgesetzbuch (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands)

Abs. 1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, dass es im Ausland verwertet, verwendet oder sonst ausgewertet werde, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen

Abs. 2) Ebenso ist zu bestrafen, wer ein Geschäfts- oder Betriebsgeheimnis, zu dessen Wahrung er verpflichtet ist, der Verwertung, Verwendung oder sonstigen Auswertung im Ausland preisgibt.

§ 126a Strafgesetzbuch (Datenbeschädigung)

Abs. 1) Wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht, oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Wer durch die Tat an den Daten einen 7'500 Franken übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Abs. 3) Wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, beeinträchtigt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Abs. 4) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer

1. durch die Tat einen 300 000 Franken übersteigenden Schaden herbeiführt,

2. durch die Tat wesentliche Bestandteile der kritischen Infrastruktur (§ 74 Abs. 1 Ziff. 10) beeinträchtigt oder

3. die Tat als Mitglied einer kriminellen Vereinigung begeht.

4.

§ 126b Strafgesetzbuch (Störung der Funktionsfähigkeit eines Computersystems)

Abs. 1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

Abs. 3) Wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, eines Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, schwer stört, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Abs. 4) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer

1. durch die Tat einen 300 000 Franken übersteigenden Schaden herbeiführt,

2. die Tat gegen ein Computersystem verübt, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Ziff. 10) ist, oder

3. die Tat als Mitglied einer kriminellen Vereinigung begeht.

§ 126c Strafgesetzbuch (Missbrauch von Computerprogrammen oder Zugangsdaten)

Abs. 1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Kommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder

2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräussert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Ziff. 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

§ 148a Strafgesetzbuch (Betrügerischer Datenverarbeitungsmissbrauch)

Abs. 1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmässig zu bereichern, einen anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Wer die Tat gewerbsmässig begeht oder durch die Tat einen 7 500 Franken übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen 300 000 Franken übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

§ 225a Strafgesetzbuch (Datenfälschung)

Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

Art. 41 Datenschutzgesetz (Unbefugtes Beschaffen von personenbezogenen Daten)

Wer unbefugt personenbezogene Daten, die nicht frei zugänglich sich, aus einer Datenverarbeitung beschafft, ist auf Verlangen des Verletzten vom Landgericht wegen Vergehens mit Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Art. 42 Datenschutzgesetz (Verletzung des Datengeheimnisses)

Abs. 1) Wer vorsätzlich geheime, personenbezogene Daten unbefugt einem anderen zugänglich macht, veröffentlicht oder verwertet, von denen er bei der Ausübung seines Berufes, der die Kenntnis solcher Daten erfordert, erfahren hat, ist auf Verlangen des Verletzten vom Landgericht wegen Vergehens mit Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist auf Verlangen des Verletzten mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Abs. 3) Ebenso ist zu bestrafen, wer vorsätzlich geheime, personenbezogene Daten unbefugt einem anderen zugänglich macht, veröffentlicht oder verwertet, von denen er bei seiner Tätigkeit für den Geheimhaltungspflichtigen oder während der Ausbildung bei diesem erfahren hat.

Abs. 4) Das unbefugte einem anderen zugänglich machen oder veröffentlichen geheimer, personenbezogener Daten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.