

**Угода
між Україною та Португальською Республікою
про взаємну охорону інформації з обмеженим доступом**

Україна та Португальська Республіка (далі – Сторони),

визнаючи потребу Сторін у забезпеченні охорони інформації з обмеженим доступом, обмін якою здійснюється між ними за контрактами про співробітництво у будь-якій формі, що укладено або мають укладатися, а також спільно створеної інформації з обмеженим доступом,

бажаючи створити правила щодо взаємної охорони інформації з обмеженим доступом, обмін якою здійснюється між Сторонами, або спільно створеної інформації з обмеженим доступом,

підтверджуючи, що ця Угода не впливатиме на зобов'язання обох Сторін, які випливають з інших міжнародних договорів, домовилися про таке:

**Стаття 1
Предмет**

1. Ця Угода встановлює правила безпеки, що застосовуються до усіх контрактів про співробітництво у будь-якій формі, що укладено або мають укладатися між уповноваженими особами обох Сторін, які передбачають обмін інформацією з обмеженим доступом, а також спільне створення такої інформації.

2. Жодна зі Сторін не може застосовувати цю Угоду для того, щоб отримати інформацію з обмеженим доступом, яку інша Сторона одержала від третьої сторони.

**Стаття 2
Визначення термінів**

Для цілей цієї Угоди терміни вживаються у такому значенні:

а) "інформація з обмеженим доступом" – інформація незалежно від її форми, природи та засобів передачі, визначена відповідно до національного законодавства як така, що потребує охорони від несанкціонованого розкриття, та доступ до якої обмежено згідно з відповідним ступенем обмеження доступу;

б) "порушення правил безпеки" – дія або бездіяльність, вчинена навмисно чи випадково, що суперечить національному законодавству Сторін, яка призводить до дійсної чи можливої компрометації інформації з обмеженим доступом;

с) "компрометація інформації з обмеженим доступом" – ситуація, коли за результатом порушення правил безпеки, інформація з обмеженим доступом втратила свою конфіденційність, цілісність чи доступність;

д) "національний орган безпеки" – державний орган, визначений Стороною для виконання та нагляду за застосуванням цієї Угоди;

е) "Сторона-джерело" – Сторона, яка передає інформацію з обмеженим доступом іншій Стороні;

ф) "Сторона-одержувач" – Сторона, яка одержує інформацію з обмеженим доступом від іншої Сторони;

г) "уповноважена особа" – державний орган або юридична особа, уповноважені відповідно до національного законодавства Сторін здійснювати діяльність, пов'язану з інформацією з обмеженим доступом;

h) "контракт з обмеженим доступом" – домовленість у будь-якій формі між уповноваженими особами Сторін, що стосується передачі інформації з обмеженим доступом або створення інформації з обмеженим доступом;

і) "допуск" – висновок Національного органу безпеки про те, що фізична особа згідно з відповідним національним законодавством має право мати доступ до інформації з обмеженим доступом;

j) "дозвіл на провадження діяльності, пов'язаної з інформацією з обмеженим доступом" – висновок Національного органу безпеки про те, що, з точки зору безпеки, згідно з національним законодавством установа має фізичну та організаційну здатність використовувати та зберігати інформацію з обмеженим доступом;

к) "необхідне знання" – принцип, згідно з яким доступ до інформації з обмеженим доступом може надаватися лише особі, яка має підтверджену потребу для знання інформації з обмеженим доступом або володіння нею для виконання своїх обов'язків.

Стаття 3

Національні органи безпеки

1. Національними органами безпеки, визначеними для виконання та нагляду за застосуванням цієї Угоди, є:

В Україні:

Служба безпеки України

В Португальській Республіці:

Національний орган безпеки

при Секретаріаті Ради Міністрів

2. Національні органи безпеки надають один одному свої офіційні контактні дані.

3. Національні органи безпеки інформують один одного про відповідне національне законодавство, що регламентує охорону інформації з обмеженим доступом, а також про зміни до нього.

4. З метою забезпечення тісного співробітництва з виконання цієї Угоди національні органи безпеки можуть проводити консультації за запитом одного з них.

Стаття 4

Правила безпеки

Охорона та використання інформації з обмеженим доступом, обмін якою здійснюється між Сторонами, регламентується такими правилами:

а) Сторона-одержувач забезпечує для одержаної інформації з обмеженим доступом рівень охорони, еквівалентний ступеню обмеження доступу, наданому інформації з обмеженим доступом Стороною-джерелом відповідно до статті 5 цієї Угоди;

б) Сторона-одержувач не повинна знижувати чи скасовувати ступінь обмеження доступу одержаної інформації з обмеженим доступом без попередньої письмової згоди Сторони-джерела;

в) доступ до інформації з обмеженим доступом обмежується особами, які для виконання своїх обов'язків мають доступ до інформації з обмеженим доступом на основі принципу "необхідного знання" та отримали допуск згідно з відповідним національним законодавством.

Стаття 5

Порівняння національних грифів обмеження доступу

Сторони згідно зі своїм національним законодавством погоджуються з наступною еквівалентністю національних грифів обмеження доступу:

В Україні	В Португальській Республіці	Еквівалент англійською мовою
Особливої важливості	MUITO SECRETO	TOP SECRET
Цілковито таємно	SECRETO	SECRET
Таємно	CONFIDENCIAL	CONFIDENTIAL
Для службового користування	RESERVADO	RESTRICTED

Стаття 6

Процедура надання допуску та дозволу на провадження діяльності, пов'язаної з інформацією з обмеженим доступом

1. Сторони визнають допуски та дозволи на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, видані згідно з відповідним національним законодавством іншої Сторони.

2. Національні органи безпеки інформують один одного про будь-які зміни, що стосуються допусків та дозволів на провадження діяльності, пов'язаної з інформацією з обмеженим доступом.

3. Національні органи безпеки Сторін, беручи до уваги своє відповідне національне законодавство, за запитом сприяють один одному під час проведення процедури перевірки у зв'язку з оформленням допуску та дозволу на провадження діяльності, пов'язаної з інформацією з обмеженим доступом.

Стаття 7

Позначення грифами обмеження доступу

1. Сторони позначають всю інформацію з обмеженим доступом, одержану від іншої Сторони, національним грифом обмеження доступу того ж ступеня відповідно до статті 5 цієї Угоди.

2. Сторони інформують одна одну про усі подальші зміни грифів обмеження доступу переданої інформації.

Стаття 8

Переклад, відтворення та знищення

1. Переклади та відтворення інформації з обмеженим доступом здійснюється відповідно до наступних процедур:

- а) особи повинні мати відповідний допуск;
- б) на перекладах та відтвореннях повинні проставлятися такі ж грифи обмеження доступу, як і на оригіналі;
- с) кількість примірників перекладів та відтворень повинні обмежуватися обсягом, потрібним для службових цілей;
- д) переклади повинні мати позначку мовою перекладу, яка б вказувала, що вони містять інформацію з обмеженим доступом, одержану від Сторони-джерела.

2. Інформація з обмеженим доступом, позначена грифом "Цілком таємно"/SECRETO та вище, перекладається та відтворюється лише за письмовим дозволом національного органу безпеки Сторони-джерела згідно з відповідним національним законодавством.

3. Інформація з обмеженим доступом, позначена грифом "Цілком таємно"/SECRETO та вище, не знищується, а повертається до національного органу безпеки Сторони-джерела.

4. Інформація з обмеженим доступом, позначена грифами включно до "Таємно"/CONFIDENCIAL, знищується згідно з відповідним національним законодавством таким чином, щоб унеможливити її часткове чи повне відновлення.

5. У разі неможливості забезпечення охорони та повернення інформації з обмеженим доступом, переданої або створеної відповідно до цієї Угоди, інформація з обмеженим доступом негайно знищується. Сторона-одержувач повідомляє національний орган безпеки Сторони-джерела про знищення інформації з обмеженим доступом якнайшвидше.

Стаття 9

Передача інформації з обмеженим доступом

1. Перед передачею інформації з обмеженим доступом Сторона-джерело, через національний орган безпеки, отримує від національного органу безпеки Сторони-одержувача письмове підтвердження того, що уповноважена особа має відповідний дозвіл на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, наданий згідно з відповідним національним законодавством.

2. Інформація з обмеженим доступом, зазвичай, передається між Сторонами дипломатичними каналами.

3. Якщо використання дипломатичних каналів буде неможливим або призведе до надмірної затримки одержання інформації з обмеженим доступом, передача може здійснюватися відповідним персоналом, що має відповідний допуск, належним чином уповноваженим Стороною-джерелом.

4. Інформація з обмеженим доступом може передаватися через захищені електронні засоби, погоджені Сторонами згідно з національним законодавством.

5. Передача великогабаритних виробів або значної кількості інформації з обмеженим доступом погоджується обома національними органами безпеки для кожного випадку окремо.

6. Сторона-одержувача письмово підтверджує одержання інформації з обмеженим доступом.

Стаття 10

Використання інформації з обмеженим доступом

1. Передана інформація з обмеженим доступом використовується лише у цілях, для яких була передана.

2. Кожна Сторона забезпечує належне виконання усіма фізичними та юридичними особами, які одержують інформацію з обмеженим доступом, зобов'язань, встановлених цією Угодою.

3. Сторона-одержувач не передає інформацію з обмеженим доступом третій стороні без попереднього письмового дозволу Сторони-джерела.

Стаття 11

Контракти з обмеженим доступом

1. Національний орган безпеки одної Сторони, перед укладенням контракту з обмеженим доступом або його виконанням на території іншої Сторони, письмово підтверджує, що уповноважена особа Сторони-одержувача, запропонована для участі в контракті, має відповідний дозвіл на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, наданий згідно з відповідним національним законодавством.

2. Будь-яка юридична особа, що укладає контракт з уповноваженою особою Сторони-одержувача, який стосується або включає доступ до інформації з обмеженим доступом, пов'язаної з контрактом з обмеженим доступом, що має виконуватися уповноваженою особою, повинна виконувати такі ж саме зобов'язання з питань безпеки, як і уповноважена особа.

3. Національний орган безпеки здійснює нагляд за дотриманням уповноваженою особою Сторони-одержувача правил безпеки, що застосовуються до контракту з обмеженим доступом.

4. Кожен контракт з обмеженим доступом, укладений між уповноваженими особами Сторін згідно з положеннями цієї Угоди, повинен містити правила безпеки, що визначають наступні аспекти:

а) зобов'язання уповноваженої особи Сторони-одержувача забезпечувати надання відповідного допуску фізичним особам, які для виконання своїх обов'язків потребують доступу до інформації з обмеженим доступом;

б) зобов'язання уповноваженої особи Сторони-одержувача забезпечувати, щоб усі особи, які мають доступ до інформації з обмеженим доступом, інформувались про відповідальність, пов'язану з охороною інформації з обмеженим доступом, згідно з відповідним національним законодавством;

в) зобов'язання уповноваженої особи Сторони-одержувача дозволяти проведення у своїх приміщеннях інспектувань з питань безпеки;

г) перелік інформації з обмеженим доступом та відповідних грифів обмеження доступу;

е) процедура повідомлення про зміни грифів обмеження доступу;

ф) комунікаційні канали та засоби електронної передачі;

г) процедура передачі інформації з обмеженим доступом;

д) зобов'язання уповноваженої особи Сторони-одержувача повідомляти Сторону-джерело та національний орган безпеки Сторони-одержувача про будь-яку дійсну або підозрювану компрометацію інформації з обмеженим доступом.

5. Правила безпеки будь-якого контракту з обмеженим доступом надсилаються національному органу безпеки Сторони-одержувача для забезпечення належного нагляду з питань безпеки.

6. Представники національних органів безпеки можуть відвідувати один одного з метою здійснення контролю ефективності заходів, що вживаються уповноваженою особою Сторони-одержувача для охорони інформації з обмеженим доступом, пов'язаної з контрактом з обмеженим доступом.

Стаття 12

Візити

1. Візити громадян Сторони-джерела до Сторони-одержувача, що передбачають доступ до інформації з обмеженим доступом, повинні здійснюватися за попереднім письмовим дозволом національних органів безпеки згідно з відповідним національним законодавством.

2. Запит на візит подається до національного органу безпеки Сторони-одержувача та повинен бути отриманим принаймні за тридцять днів до здійснення візиту чи візитів.

3. В термінових випадках запит на візит подається принаймні за сім днів заздалегідь.

4. Візити, що передбачають доступ до інформації з обмеженим доступом, дозволяються Стороною-одержувачем відвідувачам Сторони-джерела тільки якщо вони:

а) перевірені відповідним чином національним органом безпеки Сторони-джерела, що надсилає запит, та отримали допуск;

б) уповноважені отримувати інформацію з обмеженим доступом або мати доступ до неї на основі принципу "необхідного знання" згідно з відповідним національним законодавством.

5. Національний орган безпеки Сторони, що одержує запит на візит, якнайшвидше інформує про рішення національний орган безпеки Сторони, що робить запит.

6. У разі погодження візиту національний орган безпеки Сторони-одержувача надає копію запиту на візит уповноваженій особі, яку планується відвідати.

7. Термін дії дозволу на візит не може перевищувати дванадцяти місяців.

8. Сторони можуть погодити питання щодо встановлення списку осіб, яким дозволяється здійснювати періодичні візити. Такі списки діють протягом дванадцяти місяців.

9. Після погодження списків національними органами безпеки умови проведення окремих візитів визначаються безпосередньо уповноваженими особами, яких планується відвідати.

10. Запит на візит повинен містити наступну інформацію:

- а) ім'я та прізвище відвідувача, місце та дата народження, громадянство, номер паспорту чи посвідчення;
- б) найменування уповноваженої особи, яку представляє або до якої належить відвідувач;
- с) назва та адреса уповноваженої особи, яку планується відвідати;
- д) підтвердження щодо наявності у відвідувача допуску та його термін дії;
- е) ціль та мета візиту чи візитів;
- ф) очікувана дата та тривалість візиту чи візитів та, у разі періодичних візитів, загальний період їх здійснення;
- г) контактні дані установи, яку планується відвідати, попередні контакти та будь-яка інша інформація, корисна для визначення обґрунтування візиту чи візитів;
- h) дата, підпис та відбиток офіційної печатки національного органу безпеки.

Стаття 13

Порушення правил безпеки

1. У разі порушення правил безпеки, пов'язаних з отриманою або спільно створеною інформацією з обмеженим доступом, національний орган безпеки Сторони-одержувача якнайшвидше інформує національний орган безпеки Сторони-джерела та забезпечує проведення належного розслідування згідно з відповідним національним законодавством.

2. Якщо порушення правил безпеки відбувається під час передачі інформації з обмеженим доступом на території, що не підпадає під юрисдикцію однієї із Сторін, національний орган безпеки Сторони-джерела здійснює заходи, передбачені пунктом 1 цієї статті.

3. Національний орган безпеки Сторони-джерела, у разі потреби, сприяє у розслідуванні.

4. У будь-якому разі національний орган безпеки Сторони-джерела повинен письмово інформуватися про результати розслідування, а також про причини порушення правил безпеки, розмір шкоди та висновки розслідування.

Стаття 14

Витрати

Кожна Сторона самостійно несе свої витрати, які виникають у зв'язку із застосуванням та наглядом за усіма аспектами цієї Угоди.

Стаття 15

Вирішення спорів

Будь-який спір щодо тлумачення чи застосування цієї Угоди вирішується шляхом переговорів.

Стаття 16

Набрання чинності

Ця Угода набирає чинності на 30 (тридцятий) день після отримання дипломатичними каналами останнього письмового повідомлення, яке стверджує, що усі необхідні внутрішньодержавні вимоги обох Сторін для набрання чинності виконано.

Стаття 17

Зміни та доповнення

1. До цієї Угоди може бути внесено зміни та доповнення на основі взаємної письмової згоди Сторін.

2. Зміни та доповнення набирають чинності відповідно до статті 16 цієї Угоди.

Стаття 18

Термін та припинення дії

1. Ця Угода укладається на невизначений період.

2. Кожна Сторона може у будь-який час припинити дію цієї Угоди шляхом надсилання через дипломатичні канали письмового повідомлення. У такому випадку припинення вступає в силу через шість місяців після дати одержання повідомлення іншою Стороною.

3. Незважаючи на припинення дії, уся інформація з обмеженим доступом, передана згідно з цією Угодою, продовжує охоронятися відповідно до встановлених положень, доки Сторона-джерело не звільнить Сторону-одержувача від цього зобов'язання.

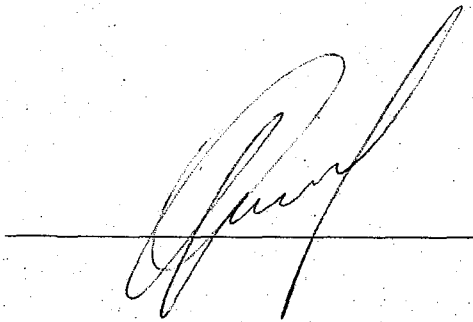
Стаття 19 Реєстрація

Сторона, на території якої підписується ця Угода, передає її для реєстрації до Секретаріату Організації Об'єднаних Націй відповідно до статті 102 Статуту Організації Об'єднаних Націй та повідомляє іншій Стороні про завершення процедури із зазначенням відповідного реєстраційного номеру.

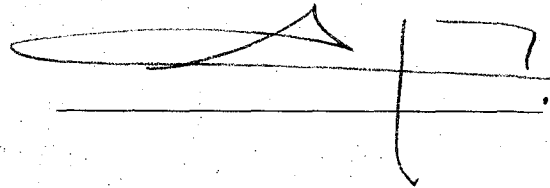
На посвідчення чого, належним чином уповноважені представники Сторін підписали цю Угоду.

Вчинено у м. Київ "22" травня 2017 року, у двох примірниках, кожен українською, португальською та англійською мовами, при цьому усі тексти є автентичними. У випадку виникнення розбіжностей стосовно тлумачення текст, викладений англійською мовою, має переважну силу.

За Україну



За Португальську Республіку



ACORDO
ENTRE A UCRÂNIA E A REPÚBLICA PORTUGUESA
SOBRE PROTEÇÃO MÚTUADA DE INFORMAÇÃO CLASSIFICADA

A Ucrânia e a República Portuguesa,

Doravante designadas por Partes:

Reconhecendo a necessidade de as Partes garantirem a proteção da Informação Classificada trocada entre ambas através de qualquer tipo de contrato de cooperação celebrado ou a celebrar, e/ou produzida conjuntamente;

Desejando estabelecer normas sobre a proteção mútua da Informação Classificada trocada entre as Partes, e/ou produzida conjuntamente;

Confirmando que este Acordo não afeta os compromissos de ambas as Partes resultantes de outros acordos internacionais.

Acordam no seguinte:

ARTIGO 1.º
Objeto

1. O presente Acordo estabelece as regras de segurança aplicáveis a todo o tipo de contrato de cooperação celebrado ou a celebrar entre as entidades designadas de ambas as Partes que preveja a troca de Informação Classificada, bem como a produção conjunta desse tipo de informação.

2. Nenhuma das Partes pode invocar o presente Acordo com o objetivo de obter Informação Classificada que a outra Parte tenha recebido de uma terceira Parte.

ARTIGO 2.º
Definições

Para efeitos do presente Acordo entende-se por:

a) “Informação Classificada” a informação, qualquer que seja a sua forma, natureza e meio de transmissão, que, de acordo com o respetivo Direito em vigor, requeira proteção contra a divulgação não autorizada e à qual tenha sido atribuída um grau de classificação de segurança;

b) “Quebra de Segurança” uma ação ou omissão, deliberada ou accidental, contrária ao Direito das Partes, que comprometa ou possa comprometer a Informação Classificada;

c) “Comprometimento de Informação Classificada” situação em que ocorre uma Quebra de Segurança conducente à perda de confidencialidade, integridade ou disponibilidade da Informação Classificada;

d) “Autoridade Nacional de Segurança” a autoridade designada pela Parte para aplicar e fiscalizar o cumprimento do presente Acordo;

e) “Parte Transmissora” a Parte que transmite Informação Classificada à outra Parte;

f) “Parte Destinatária” a Parte que recebe a Informação Classificada transmitida pela Parte;

g) “Entidade Designada” a entidade pública ou privada autorizada, de acordo com o Direito em vigor nas Partes, a manusear Informação Classificada;

h) “Contrato Classificado” qualquer tipo de acordo entre as entidades designadas das Partes relativo à transmissão e produção de Informação Classificada;

i) “Credenciação de Segurança de Pessoal” ato pelo qual a Autoridade Nacional de Segurança determina que uma pessoa está habilitada a ter acesso a Informação Classificada, de acordo com o respetivo Direito em vigor;

j) “Credenciação de Segurança Industrial” ato pelo qual a Autoridade Nacional de Segurança determina que, sob o ponto de vista da segurança, uma entidade tem capacidade física e organizacional para manusear e armazenar Informação Classificada, de acordo com o respetivo Direito em vigor;

k) “Necessidade de Conhecer” o acesso à Informação Classificada restringido às pessoas que comprovadamente precisem de a conhecer ou possuir para desempenho das suas funções.

ARTIGO 3.º

Autoridades Nacionais de Segurança

1. As Autoridades Nacionais de Segurança designadas para aplicar e fiscalizar a aplicação do presente Acordo são:

Pela Ucrânia:

- Serviço de Segurança da Ucrânia

Pela República Portuguesa:

- Autoridade Nacional de Segurança;
Presidência do Conselho de Ministros

2. As Autoridades Nacionais de Segurança deverão trocar entre elas os respetivos contactos oficiais.

3. As Autoridades Nacionais de Segurança deverão trocar entre elas informação sobre a respetiva legislação que regula a proteção da Informação Classificada, bem como sobre as alterações que possam afetar a aplicação do presente Acordo.

4. As Autoridades Nacionais de Segurança podem realizar consultas, a pedido de uma delas, a fim de assegurar uma estreita cooperação na aplicação do presente Acordo.

ARTIGO 4.º

Regras de Segurança

A proteção e a utilização da Informação Classificada trocada entre as Partes regem-se pelas seguintes regras:

a) A Parte Destinatária deverá atribuir à Informação Classificada recebida um grau de proteção correspondente ao grau de classificação de segurança atribuído pela Parte Transmissora à Informação Classificada, de acordo com o artigo 5.º;

b) A Parte Destinatária não pode proceder à baixa de classificação ou desclassificação da Informação Classificada recebida sem prévia autorização escrita da Parte Transmissora;

c) O acesso à Informação Classificada deverá restringir-se às pessoas que, por força das suas funções, têm acesso a elas, segundo o princípio da "Necessidade de Conhecer", e possuem uma Credenciação de Segurança de Pessoal, de acordo com o respetivo Direito em vigor.

ARTIGO 5.º

Equivalência das classificações de segurança nacionais

As Partes acordam, em conformidade com o respetivo Direito em vigor, que a equivalência das suas classificações de segurança nacionais é a seguinte:

Para a Ucrânia	Para a República Portuguesa	Termos em língua inglesa
Особливої важливості	MUITO SECRETO	TOP SECRET
Цілком таємно	SECRETO	SECRET
Таємно	CONFIDENCIAL	CONFIDENTIAL
Для службового користування	RESERVADO	RESTRICTED

ARTIGO 6.º

Processo de credenciação de segurança

1. As Partes deverão reconhecer as Credenciações de Segurança de Pessoal e as Credenciações de Segurança Industrial concedidas de acordo com o Direito em vigor na outra Parte.

2. As Autoridades Nacionais de Segurança deverão informar-se mutuamente sobre quaisquer modificações relativas às Credenciações de Segurança de Pessoal e às Credenciações de Segurança Industrial.

3. As Autoridades Nacionais de Segurança das Partes, tendo em conta o respetivo Direito em vigor, deverão, a pedido, prestar-se assistência mútua na condução dos processos de credenciação de Segurança de Pessoal e de Segurança Industrial.

ARTIGO 7.º

Marcação

1. As Partes deverão marcar toda a Informação Classificada recebida da outra Parte com a marca de classificação nacional de segurança, em conformidade com o artigo 5º do presente Acordo.

2. As Partes deverão informar-se mutuamente sobre quaisquer alterações introduzidas posteriormente na classificação de segurança da Informação Classificada transmitida.

ARTIGO 8.º

Tradução, reprodução e destruição

1. As traduções e reproduções da Informação Classificada deverão obedecer aos seguintes procedimentos:

- a) As pessoas deverão estar devidamente credenciadas;
- b) As traduções e as reproduções deverão ser marcadas com o mesmo grau de classificação de segurança que o original;
- c) As traduções e o número de cópias deverão ser limitados ao número necessário para fins oficiais;
- d) Nos documentos traduzidos deverá ser aposta, na língua para a qual foram traduzidos, a indicação de que contêm Informação Classificada recebida da Parte Transmissora.

2. A Informação Classificada marcada como “ЦІЛКОМ ТАЄМНО” / SECRETO ou de grau superior apenas pode ser traduzida ou reproduzida mediante autorização escrita da Autoridade Nacional de Segurança da Parte Transmissora, de acordo com o respetivo Direito em vigor.

3. A Informação Classificada marcada como “ЦІЛКОМ ТАЄМНО” / SECRETO e de grau superior não pode ser destruída, devendo ser devolvida à Autoridade Nacional de Segurança da Parte Transmissora.

4. A Informação Classificada marcada com um grau até “Таємно” / CONFIDENCIAL deverá ser destruída de acordo com o respetivo Direito em vigor, de forma a impossibilitar a sua reconstrução total ou parcial.

5. No caso de não ser possível proteger e devolver a Informação Classificada produzida ou transmitida em conformidade com o presente Acordo, a Informação Classificada deverá ser imediatamente destruída. A Parte Destinatária deverá notificar a Autoridade Nacional de Segurança da Parte Transmissora, com a maior brevidade possível, da destruição da Informação Classificada.

ARTIGO 9.º

Transmissão da Informação Classificada

1. Antes da transmissão da Informação Classificada, a Parte Transmissora, através da Autoridade Nacional de Segurança, deverá obter da Autoridade Nacional de Segurança da Parte Destinatária, uma garantia escrita de que a Entidade Designada é titular de um Certificado de Credenciação de Segurança Industrial com o grau de classificação de segurança adequado, atribuído de acordo com o respetivo Direito em vigor.

2. Entre as Partes, a Informação Classificada, normalmente, deverá ser transmitida por via diplomática.

3. Se a transmissão por via diplomática se revelar impraticável ou conduzir a atrasos indevidos na receção da Informação Classificada, esta pode ser transmitida por pessoal devidamente credenciado e devidamente autorizado pela Parte Transmissora.

4. A Informação Classificada pode ser transmitida por meios eletrónicos protegidos, aprovados pelas Partes, de acordo com o respetivo Direito em vigor.

5. A transmissão de um grande número ou de um volume considerável de Informação Classificada deverá ser aprovada, caso a caso, pelas duas Autoridades Nacionais de Segurança.

6. A Parte Destinatária deverá confirmar, por escrito, que recebeu a Informação Classificada.

ARTIGO 10.º

Utilização da Informação Classificada

1. A Informação Classificada transmitida só deverá ser utilizada para os fins para os quais foi transmitida.

2. Cada Parte deverá assegurar que todas as pessoas singulares e coletivas que recebem Informação Classificada cumprem devidamente as obrigações estabelecidas no presente Acordo.

3. A Parte Destinatária não pode transmitir Informação Classificada a uma Terceira Parte sem prévia autorização escrita da Parte Transmissora.

ARTIGO 11.º

Contratos Classificados

1. Antes da assinatura de um Contrato Classificado ou da sua execução no território da outra Parte, a Autoridade Nacional de Segurança de uma Parte deverá confirmar, por escrito, que a Entidade Designada proposta para o contrato é titular de um Certificado de Credenciação de Segurança Industrial com o grau de classificação de segurança adequado.

2. Qualquer entidade que celebre um contrato com uma Entidade Designada da Parte Destinatária, que inclua ou envolva o acesso a Informação Classificada relativa a um Contrato Classificado a ser executado pela Entidade designada, deverá respeitar as mesmas regras de segurança que a Entidade Designada.

3. A Autoridade Nacional de Segurança deverá fiscalizar o cumprimento pela Entidade Designada da Parte Destinatária das regras de segurança aplicáveis ao Contrato Classificado.

4. Qualquer Contrato Classificado celebrado entre as Entidades Designadas das Partes, nos termos do presente Acordo, deverá incluir regras de segurança que especifiquem os seguintes aspectos:

a) Compromisso da Entidade Designada da Parte Destinatária no sentido de garantir que as pessoas que tenham necessidade de ter acesso a Informação Classificada para o desempenho das suas funções foram devidamente credenciadas para o efeito;

b) Compromisso da Entidade Designada da Parte Destinatária no sentido de garantir que todas as pessoas que têm acesso a Informação Classificada foram informadas das responsabilidades que assumem na proteção da Informação Classificada, de acordo com o respetivo Direito em vigor;

c) Compromisso da Entidade Designada da Parte Destinatária no sentido de permitir a realização de inspeções de segurança às suas instalações;

d) Lista da Informação Classificada e dos respetivos graus de classificação de segurança;

e) Procedimento para a comunicação de alterações dos graus de classificação de segurança;

f) Canais de comunicação e meios de transmissão eletrónica;

g) Procedimento para a transmissão de Informação Classificada;

h) Obrigação da Entidade Designada da Parte Destinatária de comunicar à Parte Transmissora e à Autoridade Nacional de Segurança da Parte Destinatária qualquer Comprometimento, ou suspeita de Comprometimento, da Informação Classificada.

5. As instruções de segurança de qualquer Contrato Classificado deverão ser remetidas à Autoridade Nacional de Segurança da Parte Destinatária a fim de garantir a fiscalização de segurança adequada.

6. Os representantes das Autoridades Nacionais de Segurança podem efetuar visitas mútuas com o objetivo de analisar a eficácia das medidas adotadas pela Entidade Designada da Parte Destinatária tendentes a assegurar a proteção da Informação Classificada envolvida num Contrato Classificado.

ARTIGO 12.º

Visitas

1. As visitas de nacionais da Parte Transmissora à Parte Destinatária que envolvam o acesso a Informação Classificada estão sujeitas à prévia autorização escrita das Autoridades Nacionais de Segurança, de acordo com o respetivo Direito em vigor.

2. O pedido de visita deverá ser apresentado à Autoridade Nacional de Segurança da Parte Destinatária, com uma antecedência mínima de 30 dias em relação à data da ou das visitas.

3. Nas situações urgentes, o pedido de visita deverá ser apresentado com a antecedência mínima de sete dias.

4. A autorização para as visitas que envolvam o acesso a Informação Classificada só é concedida pela Parte Destinatária aos visitantes da Parte Transmissora se estes:

a) Tiverem sido devidamente credenciados pela Autoridade Nacional de Segurança da Parte Transmissora requerente; e

b) Estiverem autorizados a receber ou a ter acesso a Informação Classificada, segundo o princípio da “Necessidade de Conhecer”, de acordo com o respetivo Direito em vigor.

5. A Autoridade Nacional de Segurança da Parte que recebe o pedido de visita deverá informar, o mais rapidamente possível, a Autoridade Nacional de Segurança da Parte requerente sobre a decisão.

6. Uma vez aprovada a visita, a Autoridade Nacional de Segurança da Parte Destinatária deverá fornecer uma cópia do pedido de visita à Entidade Designada a ser visitada.

7. A autorização da visita é válida por um período máximo de doze meses.

8. As Partes podem acordar em elaborar listas de pessoas autorizadas a efetuar visitas recorrentes. Essas listas são válidas por um período de doze meses.

9. Após aprovação das listas pelas Autoridades Nacionais de Segurança, as condições das visitas concretas deverão ser definidas diretamente, em conjunto com as Entidades Designadas a visitar.

10. O pedido de visita deverá incluir a seguinte informação:

a) O nome e o apelido do visitante, o local e a data de nascimento, a nacionalidade, o número do passaporte ou do documento de identificação;

b) O nome da Entidade Designada que o visitante representa ou à qual pertence;

c) O nome e endereço da Entidade Designada a ser visitada;

- d) Confirmação do certificado da Credenciação de Segurança de Pessoal do visitante e respetiva validade;
- e) Objeto e propósito da ou das visitas;
- f) A data e duração previstas da ou das visitas pedidas e, em caso de visitas recorrentes, a duração total das visitas;
- g) O contacto da entidade a ser visitada, contactos anteriores e qualquer outra informação útil para determinar a justificação da ou das visitas;
- h) A data, a assinatura e a aposição do selo oficial da Autoridade Nacional de Segurança.

ARTIGO 13.º

Quebra de Segurança

1. Em caso de Quebra de Segurança de Informação Classificada recebida ou conjuntamente produzida, a Autoridade Nacional de Segurança da Parte Destinatária deverá informar a Autoridade Nacional de Segurança da Parte Transmissora e proceder à adequada investigação, de acordo com o respetivo Direito em vigor.

2. Se a Quebra de Segurança ocorrer, durante a transmissão, num território que não está sob a jurisdição de uma das Partes, a Autoridade Nacional de Segurança da Parte Transmissora deverá proceder de acordo com o previsto no número 1.

3. A Autoridade Nacional de Segurança da Parte Transmissora deverá, se necessário, cooperar na investigação.

4. Em qualquer caso, os resultados da investigação, incluindo as razões da Quebra de Segurança, a dimensão dos prejuízos e as conclusões da investigação, deverão ser comunicados, por escrito, à Autoridade Nacional de Segurança da Parte Transmissora.

ARTIGO 14.º

Encargos

Cada Parte deverá suportar as despesas incorridas por ela com a aplicação e supervisão de todos os aspectos do presente Acordo.

ARTIGO 15.º

Resolução de conflitos

Qualquer conflito relativo à interpretação ou aplicação do presente Acordo será resolvido através de negociação.

ARTIGO 16.º

Entrada em vigor

O presente Acordo entra em vigor no trigésimo (30.º) dia após a receção da última notificação, por escrito e por via diplomática, informando que foram cumpridos todos os requisitos de Direito interno das duas Partes necessários para o efeito.

ARTIGO 17.º

Revisão

1. O presente Acordo pode ser objeto de revisão por mútuo consentimento escrito das Partes.
2. As emendas entram em vigor nos termos previstos no artigo 16.º.

ARTIGO 18.º

Vigência e denúncia

1. O presente Acordo permanece em vigor por um período de tempo ilimitado.
2. Qualquer das Partes pode, a qualquer momento, denunciar o presente Acordo mediante notificação escrita e por via diplomática, o qual cessa a sua vigência seis meses após a data da receção da respetiva notificação.
3. Não obstante a denúncia, a Informação Classificada transmitida ao abrigo do presente Acordo deverá continuar a ser protegida em conformidade com as disposições do mesmo enquanto a Parte Transmissora não isentar a Parte Destinatária dessa obrigação.

ARTIGO 19.º

Registo

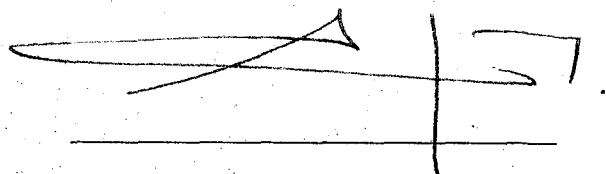
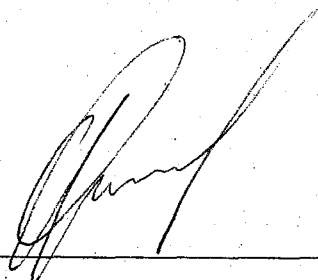
A Parte em cujo território o presente Acordo for assinado deverá submetê-lo para registo junto do Secretariado das Nações Unidas nos termos do artigo 102.º da Carta das Nações Unidas, devendo, igualmente, notificar a outra Parte da conclusão deste procedimento e indicar-lhe o número de registo atribuído.

Em fé do que, os representantes das Partes, devidamente autorizados, assinaram o presente Acordo.

Feito em Kiev, a 22 de maio de 2017, em dois originais, nas línguas ucraniana, portuguesa e inglesa, sendo todos os textos igualmente autênticos. Em caso de divergência de interpretação, o texto na língua inglesa deverá prevalecer.

Pela Ucrânia

Pela República Portuguesa



**Agreement
between Ukraine and the Portuguese Republic
on Mutual Protection of Classified Information**

Ukraine and the Portuguese Republic

Hereinafter referred to as the "Parties",

Recognizing the need of the Parties to guarantee the protection of the Classified Information exchanged between them, under co-operation contracts concluded or to be concluded in any forms, as well as jointly created;

Desiring to create rules on the mutual protection of Classified Information exchanged between the Parties, as well as jointly created,

Confirming that this Agreement shall not affect the commitments of both Parties which stem from other international agreements,

Agree as follows:

**ARTICLE 1
Object**

1. This Agreement sets out the security rules applicable to all co-operation contracts in any forms, concluded or to be concluded between the designated entities of both Parties, which envisage an exchange of Classified Information, as well as the joint creation of such information.

2. Either Party may not invoke this Agreement in order to obtain Classified Information that the other Party has received from a third party.

**ARTICLE 2
Definitions**

For the purposes of this Agreement:

a) "Classified Information" means an information, regardless of its form, nature, and means of transmission, determined in accordance with the national legislation to require protection against unauthorized disclosure and which has been classified with an appropriate level of classification;

b) "Breach of Security" means an act or an omission, deliberate or accidental, contrary to the national legislation of the Parties, which results in the actual or possible Compromise of Classified Information;

c) "Compromise of Classified Information" means a situation when, due to a Breach of Security, Classified Information has lost its confidentiality, integrity or availability;

d) "National Security Authority" means the authority designated by the Party for the implementation and the supervision of the application of this Agreement;

e) "Originating Party" means the Party which releases Classified Information to the other Party;

f) "Receiving Party" means the Party which receives the Classified Information from the other Party;

g) "Designated Entity" means the public or private entity authorized in accordance with national legislation of the Parties to handle Classified Information;

h) "Classified Contract" means an arrangement in any forms between the designated entities of the Parties concerning transmission of Classified Information or its creation;

i) "Personnel Security Clearance" means a determination by the National Security Authority that an individual is eligible to have access to Classified Information, in accordance with the respective national legislation;

j) "Facility Security Clearance" means a determination by the National Security Authority that, from a security point of view, a facility has the physical and organizational capability to handle and store Classified Information, in accordance with the respective national legislation;

k) "Need-to-know" means that access to Classified Information may only be granted to a person who has a verified requirement for knowledge of or possession of it in order to perform their duties.

ARTICLE 3

National Security Authorities

1. The National Security Authorities designated for the implementation and supervision of the application of this Agreement are:

For Ukraine:

Security Service of Ukraine

For the Portuguese Republic:

National Security Authority

Presidency of the Council of Ministers

2. The National Security Authorities shall provide each other with their official contact data.

3. The National Security Authorities shall inform each other of the respective national legislation regulating the protection of Classified Information as well as amendments affecting the implementation of this Agreement.

4. In order to ensure close co-operation in the implementation of this Agreement, National Security Authorities may hold consultations at request of one of them.

ARTICLE 4

Security Rules

The protection and use of the Classified Information exchanged between the Parties is ruled by the following rules:

a) the Receiving Party shall afford to the received Classified Information a level of protection equivalent to the security classification level given to the Classified Information by the Originating Party, in accordance with Article 5;

b) the Receiving Party shall neither downgrade nor cancel the security classification level of the received Classified Information without the prior written consent of the Originating Party;

c) the access to Classified Information shall be limited to persons who, in order to perform their duties, have access to the Classified Information, on a Need-to-know basis and hold a Personnel Security Clearance in accordance with the respective national legislation.

ARTICLE 5

Equivalence of the National Security Classifications

The Parties shall, with regard to their national legislation, adopt the following equivalency for their national security classifications:

For Ukraine	For the Portuguese Republic	Equivalent in English
Особливої важливості	MUITO SECRETO	TOP SECRET
Цілком таємно	SECRETO	SECRET
Таємно	CONFIDENCIAL	CONFIDENTIAL
Для службового користування	RESERVADO	RESTRICTED

ARTICLE 6

Security Clearance Procedure

1. The Parties shall recognize the Personnel Security Clearances and Facility Security Clearances issued in accordance with the respective national legislation of the other Party.

2. The National Security Authorities shall inform each other about any modifications regarding the Personnel Security Clearances and Facility Security Clearances.

3. On request, the National Security Authorities of the Parties, taking into account their respective national legislation, shall assist each other during the Personnel and Facility Security Clearance procedures.

ARTICLE 7

Marking

1. The Parties shall mark all the classified information received from the other Party with a national security classification of the same level according to the Article 5 of this Agreement.

2. The Parties shall inform each other about all subsequent security classification alterations to the released Classified Information.

ARTICLE 8

Translation, Reproduction and Destruction

1. Translations and reproductions of Classified Information shall be made in accordance with the following procedures:

- a) the individuals shall be appropriately security cleared;
- b) the translations and the reproductions shall be marked with the same security classification as the original;
- c) the number of copies of translations and reproductions shall be limited to that required for official purposes;
- d) the translations shall bear an appropriate note in the language of translation indicating that they contain Classified Information received from the Originating Party.

2. Classified Information marked as "ЦІЛКОМ ТАЄМНО" / SECRETO and above shall be translated or reproduced only upon written permission of the National Security Authority of the Originating Party in accordance with the respective national legislation.

3. Classified Information marked as "ЦІЛКОМ ТАЄМНО" / SECRETO and above shall not be destroyed but shall be returned to the National Security Authority of the Originating Party.

4. Classified Information marked up to "Таємно" / CONFIDENTIAL shall be destroyed in accordance with the respective national legislation, in such a manner as to eliminate its partial or total reconstruction.

5. If it is impossible to protect and return Classified Information transferred or created in accordance with this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

ARTICLE 9

Transmission of Classified Information

1. The Originating Party, through the National Security Authority, shall obtain from the National Security Authority of the Receiving Party a written assurance that the Designated Entity holds an appropriate Facility Security Clearance granted in accordance with the respective national legislation before the transmission of Classified Information.

2. Classified Information shall normally be transmitted between the Parties through diplomatic channels.

3. If the use of the diplomatic channels would be impractical or unduly delay receipt of the Classified Information, transmission may be carried out by appropriately security cleared personnel, duly authorized by the Originating Party.

4. Classified Information may be transmitted via protected electronic means approved by the Parties in accordance with the respective national legislation.

5. The transmission of large items or quantities of Classified Information shall be approved on a case-by-case basis by both National Security Authorities.

6. The Receiving Party shall confirm in writing the receipt of the Classified Information.

ARTICLE 10

Use of Classified Information

1. The transmitted Classified Information shall be used only for the purpose it has been transmitted for.

2. Either Party shall ensure that all individuals and legal entities that receive Classified Information duly comply with the obligations established in this Agreement.

3. The Receiving Party shall not release the Classified Information to a third party without prior written permission from the Originating Party.

ARTICLE 11

Classified Contracts

1. The National Security Authority of one Party shall confirm in writing before conclusion of a Classified Contract or its carrying out in the territory of the other Party, that the Designated Entity of the Receiving Party proposed for the contract participation holds an appropriate Facility Security Clearance certificate granted in accordance with the respective national legislation.

2. Any entity that concludes a contract with a Designated Entity of the Receiving Party that includes or involves access to Classified Information related to a given Classified Contract to be performed by the Designated Entity must fulfill the same security obligations as the Designated Entity.

3. The National Security Authority shall supervise the compliance by the Designated Entity of the Receiving Party with the security rules applicable to the Classified Contract.

4. Every Classified Contract concluded between Designated Entities of the Parties, under the provisions of this Agreement, shall include security rules identifying the following aspects:

a) commitment of the Designated Entity of the Receiving Party to ensure that persons that require access to Classified Information to perform their duties have been appropriately security cleared;

b) commitment of the Designated Entity of the Receiving Party to ensure that all persons with access to Classified Information are informed of their responsibility related to protection of Classified Information, in accordance with the respective national legislation;

c) commitment of the Designated Entity of the Receiving Party to allow security inspections of its premises;

d) list of Classified Information and the respective security classifications;

e) procedure for communication of alterations in the security classifications;

f) communication channels and means of electronic transmission;

g) procedure for transmission of Classified Information;

h) an obligation of the Designated Entity of the Receiving Party to notify the Originating Party and the National Security Authority of the Receiving Party of any actual or suspected Compromise of Classified Information.

5. Security rules of any Classified Contract shall be forwarded to the National Security Authority of the Receiving Party to allow adequate security supervision.

6. Representatives of the National Security Authorities may visit each other in order to control over the efficiency of the measures adopted by a Designated Entity of the Receiving Party for the protection of Classified Information involved in a Classified Contract.

ARTICLE 12

Visits

1. Visits entailing access to Classified Information by nationals from the Originating Party to the Receiving Party are subject to prior written permission of the National Security Authorities in accordance with the respective national legislation.

2. The request for visit shall be submitted to the National Security Authority of the Receiving Party and has to be received at least thirty days before the visit or visits take place.

3. In urgent cases, the request for visit shall be submitted at least seven days in advance.

4. Visits entailing access to Classified Information shall be allowed by Receiving Party to visitors from the Originating Party only if they have been:

a) appropriately security cleared by the National Security Authority of the requesting Originating Party; and

b) authorized to receive or to have access to Classified Information on a Need-to-Know basis, in accordance with the respective national legislation.

5. The National Security Authority of the Party that receives the request for visit shall inform, as soon as possible, the National Security Authority of the requesting Party about the decision.

6. Once the visit has been approved, the National Security Authority of the Receiving Party shall provide a copy of the request for visit to the Designated Entity to be visited.

7. The validity of the visit permission shall not exceed twelve months.

8. Parties may agree to set up lists of authorized persons to make recurring visits. Those lists are valid for a period of twelve months.

9. After the lists have been approved by the National Security Authorities the conditions of the specific visits shall be directly arranged with the Designated Entities to be visited.

10. The request for visit shall entail the following information:

a) visitor's first and last name, place and date of birth, nationality, passport or identification card number;

b) name of the Designated Entity the visitor represents or to which the visitor belongs;

c) name and address of the Designated Entity to be visited;

d) confirmation of the visitor's Personnel Security Clearance and its validity;

- e) object and purpose of the visit or visits;
- f) expected date and duration of the requested visit or visits, and in case of recurring visits, the total period covered by the visits;
- g) contact of the entity to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;
- h) the date, signature and stamping of the official seal of the National Security Authority.

ARTICLE 13

Breach of Security

1. In case of Breach of Security related to Classified Information received or jointly created Classified Information, the National Security Authority of the Receiving Party shall inform the National Security Authority of the either Originating Party, as soon as possible, and ensure the appropriate investigation in accordance with the respective national legislation.
2. If a Breach of Security occurs during transmission on a territory which is not under the jurisdiction of one of the Parties, the National Security Authority of the Originating Party shall take the actions prescribed in Paragraph 1.
3. The National Security Authority of the Originating Party shall, if required, co-operate in the investigation.
4. In any case, the National Security Authority of the Originating Party shall be informed of the results of the investigation, in writing, including the reasons for the Breach of Security, the extent of the damage and the conclusions of the investigation.

ARTICLE 14

Expenses

Either Party shall bear its own expenses incurred in connection with the application and supervision of all aspects of this Agreement.

ARTICLE 15

Settlement of Disputes

Any dispute concerning the interpretation or application of this Agreement shall be settled through negotiations.

ARTICLE 16

Entry into Force

This Agreement shall enter into force on the thirtieth (30) day following the receipt of the last notification, in writing and through diplomatic channels, stating that all necessary internal requirements of both Parties for the entry into force have been fulfilled.

ARTICLE 17

Amendments

1. This Agreement may be amended on the basis of mutual written consent of the Parties.
2. The amendments shall enter into force according to Article 16.

ARTICLE 18

Duration and Termination

1. This Agreement is concluded for an indefinite period of time.
2. Either Party may terminate this Agreement at any time, by written notification through diplomatic channels, producing its effects six months after the date of its receipt by the other Party.
3. Notwithstanding the termination, all Classified Information transmitted according to this Agreement shall continue to be protected in compliance with the provisions set forth herein, until the Originating Party dispenses the Receiving Party from this obligation.

ARTICLE 19

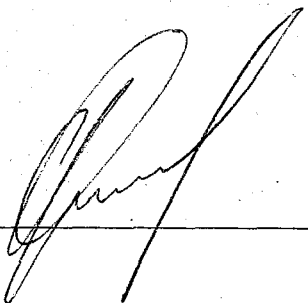
Registration

The Party in whose territory this Agreement is signed shall transmit it for registration to the Secretariat of the United Nations, in accordance with Article 102 of the Charter of the United Nations, and shall notify the other Party of the conclusion of the proceeding, indicating the respective registration number.

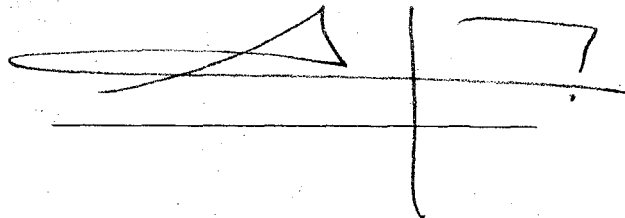
In witness whereof, the duly authorized representatives of the Parties, have signed this Agreement.

Done at Kyiv on the 22 of May 2017 in two originals, each one in the Ukrainian, Portuguese and English languages, all texts being authentic. In case of any difference of interpretation the English text shall prevail.

For Ukraine


A stylized, cursive signature in black ink, written over a horizontal line.

For the Portuguese Republic


A stylized, cursive signature in black ink, written over a horizontal line.