

**Угода
між Україною та Королівством Іспанія
про взаємну охорону інформації з обмеженим доступом**

Україна та Королівство Іспанія (далі - Сторони),
бажаючи забезпечити охорону інформації з обмеженим доступом,
обмін якою здійснюється між Сторонами, або такої, що спільно
створюється Сторонами;

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

**Стаття 1
Визначення термінів**

У цій Угоді терміни вживаються у такому значенні:

«контракт з обмеженим доступом» – договір (контракт) у будь-якій
формі, який укладається між як державними органами, так і юридичними
особами Сторін, виконання якого пов'язано з інформацією з обмеженим
доступом;

«інформація з обмеженим доступом» - будь-який вид даних
незалежно від їхньої фізичної форми, характеристик, а також засобів
передачі, що відповідно до законодавства кожної Сторони визначені та
позначені як такі, що потребують забезпечення охорони від будь-якого
несанкціонованого доступу;

«компетентний орган безпеки» – державний орган, визначений
Стороною як відповідальний за здійснення нагляду за виконанням цієї
Угоди;

«дозвіл на провадження діяльності, пов'язаної з інформацією з
обмеженим доступом» - позитивне рішення компетентного органу безпеки
за результатами процедури перевірки відповідно до національного
законодавства про те, що державний орган або юридична особа має
необхідні умови для провадження діяльності, пов'язаної з інформацією з
обмеженим доступом;

«Сторона-джерело» – державний орган або юридична особа,
уповноважені Стороною передавати інформацію з обмеженим доступом;

«допуск» – позитивне рішення компетентного органу безпеки за
результатами процедури перевірки відповідно до національного
законодавства про те, що фізична особа має право на доступ до інформації
з обмеженим доступом;

«Сторона-одержувач» - державний орган або юридична особа,
уповноважені Стороною отримувати інформацію з обмеженим доступом.

Стаття 2

Компетентні органи безпеки

1. Компетентними органами безпеки Сторін є:

Для України:

Служба безпеки України

Україна, м. Київ, вул. Володимирська, 33;

Для Королівства Іспанія:

Державний секретар, Директор Національного центру розвідки

Національне управління безпеки

Avda. Padre Huidobro, s/n 28023, Madrid, Spain.

2. Сторони повідомляють одна одну дипломатичними каналами про будь-які зміни, що стосуються їх компетентних органів безпеки.

Стаття 3

Еквівалентність грифів обмеження доступу

1. Сторони погоджуються, що наступні грифи обмеження доступу є еквівалентними та відповідають ступеням обмеження доступу, визначеним їх законодавством:

В Україні	В Королівстві Іспанія
Особливої важливості	Secreto
Цілком таємно	Reservado
Таємно	Confidencial
Для службового користування	Difusión limitada

2. Сторони позначають всю інформацію з обмеженим доступом, отриману від іншої Сторони, національними грифами обмеження доступу того ж самого ступеня відповідно до пункту 1 цієї статті.

3. Сторона-одержувач може знижувати гриф обмеження доступу отриманої інформації з обмеженим доступом, а також розсекречувати таку інформацію лише за попереднім письмовим погодженням Сторони-джерела.

Стаття 4

Заходи безпеки

1. Сторони охороняють одержану і спільно створену інформацію з обмеженим доступом відповідно до їх законодавства і цієї Угоди.

2. Інформація з обмеженим доступом, обмін якою здійснюється між Сторонами, використовується лише для цілей, обумовлених перед її передачею.

3. До інформації з обмеженим доступом можуть мати доступ лише особи, яким згідно з національним законодавством надано допуск відповідного рівня, та яких з метою виконання їх службових обов'язків було уповноважено мати доступ до інформації з обмеженим доступом.

4. Доступ до інформації з обмеженим доступом з грифом «Для службового користування»/«Difusión limitada» дозволяється відповідно до законодавства Сторін.

5. Одержана інформація з обмеженим доступом не передається третій стороні без попередньої письмової згоди Сторони-джерела.

Стаття 5

Передача інформації з обмеженим доступом

1. Інформація з обмеженим доступом передається дипломатичними каналами.

2. В окремих випадках, коли використання таких каналів є неможливим або може призвести до надмірної затримки отримання інформації з обмеженим доступом, компетентні органи безпеки можуть визначити інші засоби її передачі.

3. Перед передачею інформації з обмеженим доступом Сторона-джерело попередньо отримує від компетентного органу безпеки держави Сторони-одержувача підтвердження того, що Стороні-одержувачу відповідно до національного законодавства було надано відповідний дозвіл на провадження діяльності, пов'язаної з інформацією з обмеженим доступом.

4. Сторона-одержувач повідомляє Сторону-джерело про отримання надісланої інформації.

Стаття 6

Переклад, відтворення та знищення

1. Інформація з обмеженим доступом з грифом «Особливої важливості»/«Secreto» перекладається або відтворюється лише за письмовим погодженням Сторони-джерела.

2. Переклади та відтворення інформації з обмеженим доступом здійснюються відповідно до наступних принципів:

а) особам, які здійснюють переклади чи відтворення інформації з обмеженим доступом, відповідно до національного законодавства повинно бути надано допуск, який надає право на доступ до такої інформації відповідного ступеня обмеження доступу;

б) переклади та відтворення позначаються такими ж самими грифами обмеження доступу та підлягають такій же охороні, як і оригінали;

с) переклади та кількість копій обмежуються необхідними для службових цілей;

д) на переклади наноситься відповідна позначка мовою перекладу, яка вказує, що вони містять інформацію з обмеженим доступом, отриману від Сторони-джерела.

3. Інформація з обмеженим доступом з грифом «Особливої важливості»/«Secreto» не знищується, а повертається Стороні-джерелу.

4. Інформація з обмеженим доступом з грифом «Цілком таємно»/«Reservado» або «Таємно»/«Confidencial» знищується за попереднім письмовим погодженням Сторони-джерела.

5. Інформація з обмеженим доступом з грифами «Для службового користування»/«Difusión limitada» знищується відповідно до національного законодавства.

Стаття 7

Візити

1. Доступ до інформації з обмеженим доступом надається відвідувачам лише у необхідному обсязі та за письмовим дозволом компетентного органу безпеки Сторони, що приймає, відповідно до національного законодавства.

2. Запит на візит подається установі, яку планується відвідати, а також компетентному органу безпеки Сторони, що приймає, щонайменше за 30 (тридцять) днів до візиту. У термінових випадках, у разі можливості, цей період може скорочуватись до 10 (десяти) днів до візиту.

3. Запити на візити повинні містити, зокрема:

- а) мету та заплановану дату візиту;
- б) ім'я та прізвище, дату та місце народження, громадянство та номер паспорту чи посвідчення відвідувача;
- с) посаду відвідувача та назву установи, яку він представляє;
- д) термін дії та рівень допуску відвідувача;
- е) назву, адресу, номер телефону, номер факсу та електронну адресу контактного пункту установи, яку планується відвідати;
- ф) дату запиту та підпис уповноваженої особи компетентного органу безпеки.

4. Термін дії дозволу на візит, що передбачає доступ до інформації з обмеженим доступом, не перевищує 12 (дванадцяти) місяців.

5. Охорона персональних даних, пов'язаних з візитами, здійснюється відповідно до законодавства Сторін.

6. Візити, що передбачають доступ до спільно створеної інформації з обмеженим доступом, особам третьої сторони дозволяються лише за спільним погодженням обох Сторін.

Стаття 8

Контракти з обмеженим доступом

1. Контракт з обмеженим доступом має містити розділ з питань безпеки та перелік грифів обмеження доступу.

2. В рамках підготовки або укладення контракту з обмеженим доступом компетентні органи безпеки інформують один одного за запитом про надання відповідного дозволу на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, або про започаткування належних процедур.

3. Компетентні органи безпеки невідкладно інформують один одного про будь-які зміни, що стосуються дозволів на провадження діяльності, пов'язаної з інформацією з обмеженим доступом, які підпадають під дію цієї Угоди, зокрема, про скасування або зниження рівня таких дозволів.

4. Вимоги з питань безпеки контракту з обмеженим доступом та перелік грифів обмеження доступу передається державним органам та юридичним особам, що беруть участь у виконанні контракту з обмеженим доступом, на основі принципу «необхідного знання».

Стаття 9

Консультації

1. У разі необхідності, компетентні органи безпеки Сторін можуть проводити консультації з питань охорони інформації з обмеженим доступом та виконання цієї Угоди.

2. З метою застосування рівноцінних заходів охорони інформації з обмеженим доступом, Сторони інформують одна одну щодо свого законодавства, а також про зміни до нього, що можуть вплинути на виконання цієї Угоди.

Стаття 10

Порушення правил охорони інформації з обмеженим доступом

1. У разі порушення правил безпеки, за результатом чого відбулося розголошення інформації з обмеженим доступом, яка є предметом цієї Угоди, компетентний орган безпеки Сторони, відповідальної за охорону такої інформації, негайно інформує компетентний орган безпеки іншої Сторони та здійснює відповідні заходи згідно з національним законодавством.

2. У разі порушення правил безпеки під час передачі інформації з обмеженим доступом, що відбулась на території третьої сторони, компетентний орган безпеки Сторони, що надсилає таку інформацію, здійснює заходи, визначені у пункті 1 цієї статті.

3. Компетентний орган безпеки Сторони, який здійснює заходи, визначені у попередніх пунктах цієї статті, інформує компетентний орган безпеки іншої Сторони про їх результати.

Стаття 11

Витрати

1. Виконання цієї Угоди зазвичай не передбачає будь-яких витрат.
2. У разі виникнення можливих витрат, кожна Сторона самостійно несе витрати, пов'язанні з виконанням положень цієї Угоди.

Стаття 12

Вирішення спорів

1. Представники Сторін вирішують всі спори щодо тлумачення або виконання цієї Угоди шляхом переговорів і не звертаються до третьої сторони для їх вирішення.
2. Під час переговорів Сторони продовжують виконувати свої зобов'язання, що випливають з положень цієї Угоди.

Стаття 13

Зміни та доповнення

До цієї Угоди можуть бути внесені зміни та доповнення за взаємною згодою Сторін. Пропозиції про внесення змін та доповнень надсилаються дипломатичними каналами в письмовій формі і вони набирають чинності відповідно до положень пункту 1 статті 14 цієї Угоди.

Стаття 14

Прикінцеві положення

1. Ця Угода набирає чинності з дати отримання останнього письмового повідомлення, в якому Сторони дипломатичними каналами інформують одна одну про виконання відповідних внутрішньодержавних процедур, необхідних для набрання Угодою чинності.

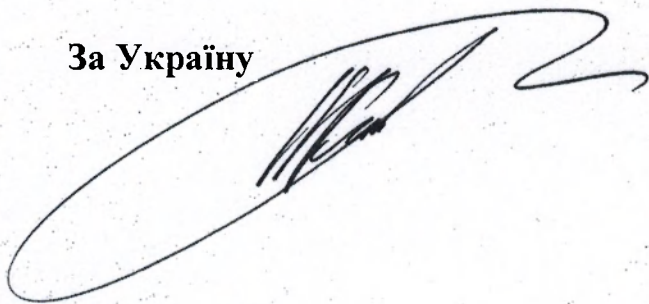
2. Ця Угода укладається на невизначений строк. Будь-яка Сторона може денонсувати цю Угоду шляхом направлення іншій Стороні повідомлення у письмовій формі. У такому випадку Угода припиняє дію через шість місяців після одержання такого письмового повідомлення.

3. У разі припинення дії цієї Угоди, Сторони продовжують забезпечувати охорону вже отриманої інформації з обмеженим доступом відповідно до положень цієї Угоди.

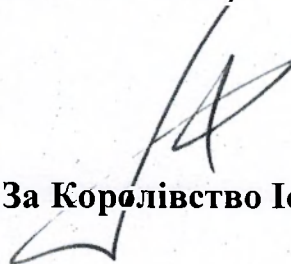
Вчинено у м. Київ «10» лютого 2015 року, у двох примірниках, кожний українською, іспанською та англійською мовами, при цьому всі тексти є автентичними.

На посвідчення чого ті, що підписалися нижче, належним чином на те вповноважені, підписали цю Угоду.

За Україну



За Королівство Іспанія



**Acuerdo
entre Ucrania y el Reino de España
para la protección recíproca de información clasificada**

Ucrania y el Reino de España (en lo sucesivo denominados las "Partes"),
Deseosos de garantizar la protección de la Información Clasificada que se
genere conjuntamente o se intercambie entre las Partes;

Confirmando que el presente Acuerdo no afectará a los compromisos de
ambas Partes derivados de otros acuerdos internacionales;

Han convenido en lo siguiente:

**Artículo 1
Definiciones**

A los efectos del presente Acuerdo, serán de aplicación las siguientes
definiciones:

Por "Contrato Clasificado" se entenderá todo contrato, de cualquier
naturaleza, suscrito entre autoridades estatales o entidades jurídicas de las
Partes, que suponga el acceso a Información Clasificada;

Por "Información Clasificada" se entenderá cualesquiera tipo de datos
con independencia de su forma material, sus características y su medio de
transmisión, que hayan sido así designados y marcados de conformidad con la
legislación de cada Parte a fin de protegerlos contra todo acceso no autorizado a
los mismos;

Por "Autoridad de Seguridad Competente" se entenderá la autoridad
estatal designada por cada Parte como responsable de supervisar la aplicación
del presente Acuerdo;

Por "Habilitación de Seguridad de Establecimiento" se entenderá la
determinación positiva, emitida por la Autoridad de Seguridad Competente tras
llevar a cabo un procedimiento de habilitación, de conformidad con la
legislación nacional, según la cual una autoridad estatal o entidad jurídica
cuenta con la capacidad para manejar Información Clasificada;

Por "Parte de Origen" se entenderá la autoridad estatal o entidad jurídica
designada por una Parte a efectos de cesión de Información Clasificada;

Por "Habilitación Personal de Seguridad" se entenderá una determinación
positiva, emitida por la Autoridad de Seguridad Competente tras llevar a cabo
un procedimiento de habilitación conforme a la legislación nacional, según la
cual una persona puede acceder a Información Clasificada;

Por "Parte Receptora" se entenderá una autoridad estatal o entidad
jurídica designada por cada Parte para recibir Información Clasificada.

Artículo 2

Autoridades de seguridad competentes

1. Las Autoridades de Seguridad Competentes de las Partes son:

Para Ucrania:

Servicio de Seguridad de Ucrania

Volodymyrska St. 33, Kiev, Ucrania;

Para el Reino de España:

Secretario de Estado, Director del Centro Nacional de Inteligencia

Oficina Nacional de Seguridad

Avda. Padre Huidobro, s/n 28023, Madrid, España.

2. Las Partes se informarán mutuamente, por conducto diplomático, sobre cualquier modificación que se produzca en relación con sus Autoridades de Seguridad Competentes.

Artículo 3

Equivalencias de las clasificaciones de seguridad

1. Las Partes convienen en que las siguientes marcas de clasificación de seguridad son equivalentes y corresponden a los grados de clasificación de seguridad especificados en su legislación:

En Ucrania	En el Reino de España
Особливої важливості	Secreto
Цілком таємно	Reservado
Таємно	Confidencial
Для службового користування	Difusión limitada

2. Cada Parte marcará la Información Clasificada recibida de la otra con una marca nacional de clasificación del mismo grado según lo dispuesto en el apartado 1 del presente artículo.

3. La Parte receptora sólo podrá reducir el grado de clasificación o desclasificar la Información Clasificada recibida con el previo consentimiento por escrito de la Parte de Origen.

Artículo 4

Disposiciones relativas a la seguridad

1. Las Partes protegerán la Información Clasificada recibida y generada conjuntamente de conformidad con su legislación y con lo previsto en el presente Acuerdo.
2. La Información Clasificada intercambiada entre las Partes sólo podrá utilizarse para los fines determinados antes de su transmisión.
3. Sólo podrán acceder a la Información Clasificada las personas que, conforme a la legislación nacional, hayan obtenido una Habilitación Personal de Seguridad del grado pertinente y hayan sido debidamente autorizadas a tal efecto para el desempeño de sus funciones oficiales.
4. El acceso a la Información Clasificada de grado “Для службового користування”/“Difusión limitada” sólo se autorizará conforme a lo dispuesto en la legislación de las Partes.
5. La Información Clasificada recibida no se divulgará a terceros sin el previo consentimiento por escrito de la Parte de Origen.

Artículo 5

Transmisión de la Información Clasificada

1. La Información Clasificada se transmitirá por conducto diplomático.
2. En casos específicos, cuando el empleo de este conducto no resulte factible o pudiera retrasar indebidamente la recepción de la Información Clasificada, las Autoridades de Seguridad Competentes podrán disponer que la transmisión se efectúe por otro medio.
3. Antes de transmitir la Información Clasificada, la Parte de Origen obtendrá de antemano de la Autoridad de Seguridad Competente del Estado de la Parte Receptora una confirmación de que esta última, de conformidad con su legislación nacional, ha recibido la pertinente Habilitación de Seguridad de Establecimiento.
4. La Parte Receptora notificará a la Parte de Origen la recepción de la información transmitida.

Artículo 6

Traducción, reproducción y destrucción

1. La Información clasificada con el grado “Особливої важливості”/“Secreto” solo podrá traducirse o reproducirse previo consentimiento escrito de la Parte de Origen.
2. Las traducciones y reproducciones de Información Clasificada se llevarán a cabo conforme a los siguientes principios:
 - a) Las personas responsables de su traducción o reproducción deberán contar con la Habilitación Personal de Seguridad pertinente, conforme a la

legislación nacional, que les permita acceder a la Información del grado de clasificación correspondiente;

b) Toda reproducción y traducción llevará la marca de clasificación original y será objeto de la misma protección que los originales;

c) Las traducciones y el número de reproducciones se limitarán a lo requerido para fines oficiales;

d) En las traducciones figurará una anotación, en la lengua de traducción, en la que se haga constar que contiene Información Clasificada recibida de la Parte de Origen.

3. La Información clasificada con el grado “Особливої важливості”/”Secreto” no podrá destruirse, sino que se devolverá a la Parte de Origen.

4. La Información Clasificada marcada como “Цілком таємно”/”Reservado” o “Таємно”/”Confidencial” podrá destruirse con el previo consentimiento por escrito de la Parte de Origen.

5. La Información Clasificada marcada “Для службового користування”/”Difusión limitada” se destruirá según lo dispuesto en la legislación nacional.

Artículo 7

Visitas

1. Sólo se permitirá a los visitantes acceder a Información Clasificada en la medida en que resulte necesario y previa autorización escrita de la Autoridad de Seguridad Competente de la Parte anfitriona de conformidad con su legislación nacional.

2. Las solicitudes de visita se remitirán al establecimiento que vaya a ser visitado, así como a la Autoridad de Seguridad Competente de la Parte anfitriona, al menos treinta (30) días antes de la visita. En casos urgentes, el plazo podrá reducirse a diez (10) días antes de la visita, si fuera posible.

3. La solicitud de visita incluirá los siguientes datos:

- a) objeto y fecha propuesta para la visita;
- b) nombre y apellidos del visitante, fecha y lugar de nacimiento, nacionalidad y número de documento de identidad o pasaporte;
- c) cargo de los visitantes y establecimiento al que representan;
- d) grado y validez de la Habilitación Personal de Seguridad de los visitantes;
- e) nombre, dirección, número de teléfono y fax, dirección de correo electrónico y punto de contacto del establecimiento que vaya a visitarse;
- f) fecha de la solicitud y firma de la Autoridad de Seguridad Competente.

4. La validez de las autorizaciones de visita que impliquen el acceso a Información Clasificada no excederá de doce (12) meses.

5. La protección de los datos personales relativos a las visitas se llevará a cabo de conformidad con la legislación de las Partes.

6. Las visitas de representantes de terceros que impliquen el acceso a Información Clasificada generada conjuntamente producida exigirán el consentimiento de ambas Partes.

Artículo 8

Contratos clasificados

1. Todo Contrato Clasificado deberá contener disposiciones sobre los requisitos de seguridad y una guía de Clasificación.

2. En el contexto de la preparación o conclusión de un Contrato Clasificado, las Autoridades de Seguridad Competentes se informarán mutuamente, si así se solicita, de si se han emitido las pertinentes Habilitaciones de Seguridad de Establecimiento o se ha iniciado el procedimiento correspondiente para ello.

3. Las Autoridades de Seguridad Competentes se informarán mutuamente sin demora de cualquier modificación relativa a las Habilitaciones de Seguridad de Establecimiento a que se refiere el presente artículo, en particular sobre las posibles revocaciones o rebajas del grado de clasificación.

4. Los requisitos de seguridad de cada Contrato Clasificado y la guía de clasificación se comunicarán a las autoridades estatales y entidades jurídicas que vayan a ejecutar el Contrato siguiendo criterios de necesidad de conocer.

Artículo 9

Consultas

1. Si fuera preciso, las Autoridades de Seguridad Competentes de las Partes podrán celebrar consultas sobre la protección de la Información Clasificada y la aplicación del presente Acuerdo.

2. A fin de aplicar medidas equivalentes para la protección de la Información Clasificada conforme al presente Acuerdo, las Partes se informarán mutuamente de los pormenores de su legislación y de las modificaciones de la misma que puedan afectar a la aplicación del Acuerdo.

Artículo 10

Infracción de seguridad de la Información Clasificada

1. Si se produce una infracción de seguridad que comprometa la Información Clasificada a que se refiere el presente Acuerdo, la Autoridad de Seguridad Competente de la Parte responsable de protegerla informará inmediatamente a su homóloga de la otra Parte y adoptará las medidas pertinentes de acuerdo con su legislación nacional.

2. Si la infracción se produce durante el transporte de la Información Clasificada a través del territorio de un tercero, la Autoridad de Seguridad

Competente de la Parte que la haya enviado adoptará las medidas mencionadas en el apartado 1 del presente artículo.

3. La Autoridad de Seguridad Competente de la Parte que adopte las medidas mencionadas en los anteriores apartados del presente artículo informará de sus resultados a su homóloga de la otra Parte.

Artículo 11

Gastos

1. Como norma general, la aplicación del presente Acuerdo no generará gasto alguno.

2. En caso de producirse, cada una de las Partes sufragará sus propios gastos ocasionados durante la aplicación del presente Acuerdo.

Artículo 12

Solución de controversias

1. Los representantes de las Partes resolverán mediante negociaciones cualquier controversia relativa a la interpretación o aplicación del presente Acuerdo y no la someterán a terceros para su solución.

2. Durante las negociaciones, las Partes continuarán vinculadas al cumplimiento de las obligaciones dimanantes de lo dispuesto en el presente Acuerdo.

Artículo 13

Enmiendas

El presente Acuerdo podrá enmendarse por mutuo consentimiento entre las Partes. Las enmiendas se propondrán por escrito y por conducto diplomático y surtirán efecto a tenor de lo dispuesto en el apartado 1 del artículo 14 del mismo.

Artículo 14

Disposiciones finales

1. El presente Acuerdo entrará en vigor en la fecha de recepción de la última notificación escrita por la que las Partes se informen recíprocamente, por conducto diplomático, de que se han completado sus requisitos jurídicos internos necesarios para su entrada en vigor.

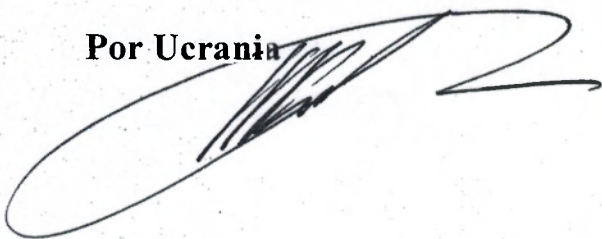
2. El presente Acuerdo permanecerá en vigor por un periodo indefinido. Cualquiera de las Partes podrá denunciarlo mediante notificación escrita enviada a la otra Parte. En tal caso, el presente Acuerdo terminará seis (6) meses después de la fecha de recepción de dicha notificación escrita.

3. En caso de terminación del presente Acuerdo, las Partes seguirán otorgando su protección a toda la Información Clasificada ya recibida de conformidad con lo previsto en el mismo.

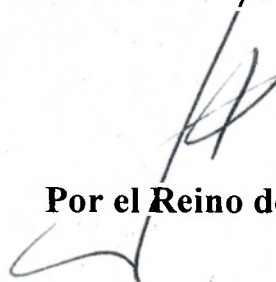
Hecho en Kyiv, el 10 de febrero de 2015 en dos originales en ucraniano, español e inglés, siendo todos los textos igualmente auténticos.

En fe de lo cual, los abajo firmantes, debidamente autorizados, firman el presente Acuerdo.

Por Ucrania



Por el Reino de España



Agreement
between Ukraine and the Kingdom of Spain
on the mutual protection of classified information

Ukraine and the Kingdom of Spain (hereinafter referred to as "the Parties"),

Willing to ensure the protection of the Classified Information exchanged between or mutually produced by the Parties;

Confirming that this Agreement shall not affect the commitments of both Parties stemming from other international agreements;

Have agreed as follows:

Article 1
Definitions

For the purpose of this Agreement, the term:

"Classified Contract" means a contract in any form between either a state authorities or legal entities of the Parties involving access to Classified Information;

"Classified Information" means any kind of data regardless of its physical form, characteristics as well as of the means of transmission that has been designated and marked as such in accordance with the legislation of either Party in order to ensure its protection against any unauthorized access;

"Competent Security Authority" means a state authority designated by a Party as being responsible for the supervision on implementation of this Agreement;

"Facility Security Clearance" means a positive decision of the Competent Security Authority stemming from a vetting procedure in accordance with the national legislation that a state authority and/or legal entity has the capability to handle Classified Information;

"Originating party" means a state authority or legal entity designated by the Party to release Classified Information;

"Personnel Security Clearance" means a positive decision of the Competent Security Authority stemming from a vetting procedure in accordance with the national legislation that an individual is eligible to have access to Classified Information;

"Receiving party" means a state authority or legal entity designated by the Party to receive Classified Information.

Article 2
Competent Security Authorities

1. The Competent Security Authorities of the Parties are:

For Ukraine:

Security Service of Ukraine
Volodymyrska St. 33, Kyiv, Ukraine;

For the Kingdom of Spain:
Secretary of State, Director of the National Intelligence Centre
National Office of Security
Avda. Padre Huidobro, s/n 28023, Madrid, Spain.

2. The Parties shall inform each other, through diplomatic channels, of any modification concerning their Competent Security Authorities.

Article 3

Equivalency of classification markings

1. The Parties agree that the following classification markings are equivalent and correspond to the classification levels specified in their legislations:

In Ukraine	In the Kingdom of Spain
Особливої важливості	Secreto
Цілком таємно	Reservado
Таємно	Confidencial
Для службового користування	Difusión limitada

2. The Parties shall mark all the Classified Information received from the other Party with a national classification marking of the same level according to paragraph 1 of this Article.

3. The Receiving party shall either downgrade or declassify the received Classified Information only with the prior written approval of the Originating party.

Article 4

Security measures

1. The Parties shall protect the received and mutually produced Classified Information in accordance with their legislation and this Agreement.

2. Classified Information exchanged between the Parties shall only be used for the purposes determined before its transmission.

3. Only those individuals who according to the national legislation have been granted a Personnel Security Clearance at the appropriate level and, in order to perform their official duties, were duly authorized, may have access to Classified Information.

4. Access to Classified Information marked with “Для службового користування”/“Difusión limitada” shall be authorized in accordance with the legislation of the Parties.

5. Received Classified Information shall not be disclosed to a third

party without the prior written consent of the Originating party.

Article 5

Transmission of Classified Information

1. Classified Information shall be transmitted through diplomatic channels.

2. In specific cases, when the use of such channels would be impractical or unduly delay the receipt of Classified Information the Competent Security Authorities may define other means for its transmission.

3. Before the transmission of Classified Information, the Originating party shall in advance obtain from the Competent Security Authority of the State of the Receiving party a confirmation that the Receiving party according to the national legislation has been granted the appropriate Facility Security Clearance.

4. The Receiving party shall notify the Originating party of the reception of the transmitted information.

Article 6

Translation, Reproduction and Destruction

1. Classified Information marked "Особливої важливості"/"Secreto" shall be translated or reproduced only upon the written approval of the Originating party.

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

a) The individuals who perform translations and reproductions of Classified Information shall be granted a Personnel Security Clearance, in accordance with the national legislation, enabling them access to Classified Information of relevant classification level;

b) The translations and the reproductions shall be marked and placed under the same protection as the original;

c) The translations and the number of copies shall be limited to that required for official purposes;

d) The translations shall bear an appropriate note in the language into which they are translated indicating that they contain Classified Information received from the Originating party.

3. Classified Information marked "Особливої важливості"/"Secreto" shall not be destroyed but shall be returned to the Originating party.

4. Classified Information marked "Цілком таємно"/"Reservado" or "Таємно"/"Confidential" shall be destroyed with prior written approval of the Originating party.

5. Classified Information marked "Для службового користування"/"Difusión limitada" shall be destroyed in accordance with the national legislation.

Article 7

Visits

1. Visitors shall be granted access to Classified Information only to the extent necessary and with the written authorisation of the Competent Security Authority of the host Party in accordance with the national legislation.

2. Requests for visits shall be submitted to the facility to be visited as well as the Competent Security Authority of the host Party at least thirty days (30) prior to the visit. In urgent cases, if possible, such period of time may be reduced to ten (10) days prior to the visit.

3. Requests for visits shall state in particular the following:

- a) purpose and proposed date of the visit;
- b) first name and family name, date and place of birth, nationality and passport or ID card number of the visitor;
- c) position of the visitors and name of the facility represented;
- d) validity and level of the Personnel Security Clearance of the visitors;
- e) name, address, phone, fax number and e-mail address of the point of contact of the facility to be visited;
- f) date of the request and signature of the Competent Security Authority.

4. The validity of authorizations for visits, involving access to Classified Information, shall not exceed twelve (12) months.

5. Protection of the personnel data related to the visits shall be performed in accordance with the legislation of the Parties.

6. Visits by individuals from a third party entailing access to Classified Information mutually produced shall only be authorized by the common approval of both Parties.

Article 8

Classified Contracts

1. A Classified Contract shall contain security section and a classification guide.

2. In the context of the preparation or conclusion of Classified Contracts, the Competent Security Authorities shall inform each other upon request whether an appropriate Facility Security Clearance has been issued or the relevant proceedings have been initiated.

3. The Competent Security Authorities shall inform each other without delay about any alteration with regard to Facility Security Clearances falling under this Article, in particular about a revocation or a downgrading of the classification level.

4. Security requirements of the Classified Contract and the classification guide shall be communicated to state authorities and legal entities performing Classified Contract on a "need-to-know" basis.

Article 9

Consultations

1. If needed, the Competent Security Authorities of the Parties may have consultations on the protection of Classified Information and the implementation of this Agreement.

2. In order to apply equivalent measures for the protection of Classified Information under this Agreement, the Parties shall inform each other of their legislation and its changes that may affect the implementation of this Agreement.

Article 10

Breach of security of Classified Information

1. In case of a breach of security that results in a compromise of Classified Information pursuant to this Agreement, the Competent Security Authority of the Party responsible for the protection of such information shall immediately inform the Competent Security Authority of the other Party and adopt the appropriate measures in accordance with its national legislation.

2. If the breach of security occurs during the transportation of the Classified Information through the territory of a third party, the Competent Security Authority of the sending Party shall adopt the measures established under the paragraph 1 of this Article.

3. The Competent Security Authority of the Party adopting measures mentioned on previous paragraphs of this Article shall inform of their results to the Competent Security Authority of the other Party.

Article 11

Expenses

1. The implementation of this Agreement will not normally bear any cost.

2. In case of eventual costs, each Party shall bear their own expenses incurred in connection with the implementation of the provisions of this Agreement.

Article 12

Settlement of disputes

1. The representatives of the Parties shall settle all the disputes arising from the interpretation or implementation of this Agreement by negotiation and shall not refer to a third party for its settlement.

2. Pending the negotiations, the Parties shall continue to fulfill their obligations stemming from the provisions of this Agreement.

Article 13

Amendments

This Agreement may be amended by mutual consent of the Parties. Amendments shall be proposed through diplomatic channels in writing and shall enter into force in accordance with the provisions of paragraph 1 of Article 14 of this Agreement.

Article 14

Final provisions

1. This Agreement shall enter into force from the date of receipt of the last written notification by which the Parties notify each other, through diplomatic channels, that their respective internal legal requirements for the entry into force of this Agreement have been fulfilled.

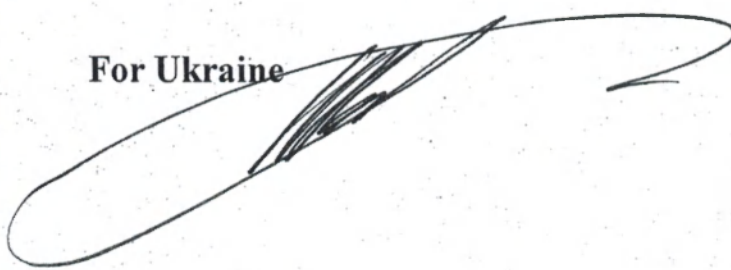
2. This Agreement shall remain in effect for an indefinite period. Either Party may denounce the Agreement by giving the other Party notice in writing. In such case, the Agreement shall be terminated six months after the receipt of such written notice.

3. In case of termination of this Agreement, the Parties shall continue to provide protection of the Classified Information already received according to the provisions of this Agreement.

Done at Kyiv on the 10 of february 2015, in two originals, each in Ukrainian, Spanish and English languages, all texts being equally authentic.

In witness whereof, the undersigned, duly authorized, have signed this Agreement.

For Ukraine



For the Kingdom of Spain

