No. 56351*

Luxembourg
and
Bulgaria

Agreement between the Government of the Grand Duchy of Luxembourg and the Government of the Republic of Bulgaria on exchange and mutual protection of classified information. Sofia, 29 January 2018

Entry into force: *1 May 2020, in accordance with article 14(1)*

Authentic texts: *Bulgarian, English and French*

Registration with the Secretariat of the United Nations: *Luxembourg, 22 September 2020*

*No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.

Luxembourg
et
Bulgarie

Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Bulgarie relatif à l'échange et à la protection réciproque d'informations classifiées. Sofia, 29 janvier 2018

Entrée en vigueur : *1er mai 2020, conformément au paragraphe 1 de l'article 14*

Textes authentiques : *bulgare, anglais et français*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Luxembourg, 22 septembre 2020*

*Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.

[BULGARIAN TEXT – TEXTE BULGARE]

СПОРАЗУМЕНИЕ

МЕЖДУ

ПРАВИТЕЛСТВОТО НА
ВЕЛИКОТО ХЕРЦОГСТВО ЛЮКСЕМБУРГ

И
ПРАВИТЕЛСТВОТО НА РЕПУБЛИКА БЪЛГАРИЯ

ЗА

ОБМЕН И ВЗАИМНА ЗАЩИТА НА

КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Правителството на Великото Херцогство Люксембург и Правителството на Република България (наричани по-нататък „Страните“),

Разбирайки, че ефективното сътрудничество в политическата, икономическата, военната, сигурността, разузнавателна и всяка друга сфера може да изисква обмен на класифицирана информация между Страните,

Разбирайки, че доброто сътрудничество може да изисква обмен на класифицирана информация между Страните,

Желаейки да създадат набор от правила, регламентиращи взаимната защита на класифицираната информация, обменяна между Страните, съгласно всички бъдещи споразумения за сътрудничество и/или класифицирани договори

Се договориха за следното:

Член 1
Цел и обхват

(1) Целта на това Споразумение е да гарантира защитата на класифицираната информация, която е съвместно създадена от или обменяна между Страните.

(2) Това Споразумение се прилага за всички дейности, договори или споразумения, включващи класифицирана информация, които ще бъдат изпълнявани или сключвани между Страните в бъдеще.

(3) Разпоредбите на това Споразумение се прилагат също за класифицираната информация, която вече е създадена или обменена в процеса на сътрудничество между Страните преди влизане в сила на това Споразумение.

Член 2
Определения

За целите на това Споразумение:

(1) **„Класифицирана информация“** означава информация, независимо от нейната форма, същност или метод на пренос, създадена или в процес на създаване, на която е определено ниво на класификация за сигурност и за която в интерес на националната сигурност и в съответствие с националното законодателство, се изисква защита срещу нерегламентиран достъп.

(2) **„Ниво на класификация за сигурност“** означава категория, която, според националното законодателство, характеризира значимостта на класифицираната информация, нивото на ограничаване на достъпа до нея и нивото на защитата ѝ от Страните, а също и категорията, на основата на която информацията е маркирана.

(3) **„Разрешение за достъп до класифицирана информация“** означава решение, издадено от съответния национален орган в резултат от процедура по проучване, което установява, че на определено физическо лице може да бъде предоставен достъп до класифицирана информация, в съответствие с националното законодателство.

(4) **„Удостоверение за сигурност“** означава решение, издадено от съответния национален орган в резултат от процедура по проучване, което установява, че по отношение на сигурността определено юридическо лице отговаря на физическите и организационните изисквания за създаване, обработване и съхраняване на класифицирана информация, в съответствие с националното законодателство.

(5) **„Необходимост да се знае“** означава необходимостта от достъп до класифицирана информация във връзка със служебни задължения и/или за изпълнение на конкретна служебна задача.

(6) **„Компетентен орган“** означава националният орган, който в съответствие с националното законодателство на съответната Страна, изпълнява държавната политика за защитата на класифицирана информация, упражнява цялостен контрол в тази сфера, както и ръководи прилагането на това Споразумение. Тези органи са описани в Член 3 на това Споразумение.

(7) **„Страна-източник“** означава Страната, която предава класифицираната информация.

(8) **„Страна-получател“** означава Страната, на която е предадена класифицираната информация.

(9) **„Трета страна“** означава държава или международна организация, която не е Страна по това Споразумение.

(10) **„Класифициран договор“** означава споразумение между два или повече Контрагента, което съдържа класифицирана информация или изисква достъп до класифицирана информация.

(11) **„Контрагент“** означава физическо или юридическо лице, което притежава юридическа правоспособност да сключва договори и/или е страна по класифициран договор.

(12) **„Подизпълнител“** означава Контрагент, на когото основният Контрагент възлага договор за подизпълнение.

(13) **„Нарушаване на мерките за сигурност“** означава всяко действие или бездействие, което е в противоречие с националното законодателство, резултатът от което води или може да доведе до нерегламентиран достъп до класифицирана информация.

(14) **„Нерегламентиран достъп до класифицирана информация“** означава всяка форма на разкриване на класифицирана информация, включително злоупотреба, изменение, увреждане, разкриване, унищожаване или неправилно класифициране на класифицирана информация, включително всяко друго действие, компрометиращо нейната защита или в резултат на което настъпва загуба на такава информация. За нерегламентиран достъп се смята също всяко действие или бездействие, в резултат на което такава информация е сведена до знанието на лице, което не притежава разрешение за достъп/ удостоверение за сигурност и което няма „необходимост да се знае“.

Член 3
Компетентни органи

Компетентните органи на Страните са:

За Великото Херцогство Люксембург:
- Държавна служба за разузнаване
Национален орган по сигурността
- (Service de renseignement de l’État
Autorité nationale de Sécurité (National Security Authority))

За Република България:
- Държавна комисия по сигурността на информацията
(State Commission on Information Security)

Член 4
Нива на класификация за сигурност

Страните се съгласяват, че следните нива на класификация за сигурност са еквивалентни и съответстват на нивата на класификация за сигурност, определени в националното законодателство на съответната Страна:

За Великото Херцогство Люксембург	**Еквивалент на английски език**	**За Република България**
TRES SECRET LUX	TOP SECRET	СТРОГО СЕКРЕТНО
SECRET LUX	SECRET	СЕКРЕТНО
CONFIDENTIEL LUX	CONFIDENTIAL	ПОВЕРИТЕЛНО
RESTREINT LUX	RESTRICTED	ЗА СЛУЖЕБНО ПОЛЗВАНЕ

Член 5
Мерки за защитата на класифицирана информация

(1) В съответствие със своето национално законодателство, Страните прилагат всички подходящи мерки за защита на класифицирана информация, която е съвместно създадена или обменяна по силата на това Споразумение. На такава класифицирана информация се осигурява същото ниво на защита каквото е осигурено за националната класифицирана информация със съответстващото ниво на класификация за сигурност.

(2) Нивото на класификация за сигурност на съвместно създадената класифицирана информация съгласно това Споразумение се определя с общо съгласие на Страните.

(3) Страните своевременно се информират взаимно за всички промени в националното законодателство, засягащи защитата на класифицираната информация. В такива случаи, Страните се информират взаимно в писмена форма, за да обсъждат възможни изменения на това Споразумение. Междувременно, класифицираната информация трябва да бъде защитавана съгласно разпоредбите на Споразумението, освен ако не е договорено друго в писмена форма.

(4) Класифицираната информация трябва да е достъпна само за лица, които са упълномощени съгласно националното законодателство да имат достъп до класифицирана информация с еквивалентно ниво на класификация за

сигурност и които имат „необходимост да се знае“, и които са преминали през съответното обучение.

(5) Страната-получател е длъжна:

а) да не разкрива класифицирана информация на Трета страна без предварително писмено съгласие на Компетентния орган на Страната-източник;

б) да дава ниво на класификация за сигурност на класифицираната информация еквивалентно на даденото от Страната-източник;

в) да не използва класифицираната информация за други цели, различни от тези, за които е предоставена.

(6) Ако друго Споразумение, сключено между Страните, съдържа по-стриктни правила относно обмена или защитата на класифицирана информация, тези правила трябва да се прилагат.

Член 6
Сътрудничество за сигурност

(1) Компетентните органи взаимно се информират за действащото си национално законодателство в областта на защитата на класифицираната информация.

(2) За да осигурят тясно сътрудничество при прилагането на това Споразумение, Компетентните органи могат да провеждат консултации по искане, отправено от един от тях.

(3) За да постигнат и поддържат равностойни стандарти за сигурност, Компетентните органи, при поискване, предоставят един на друг информация за стандартите, практиките и процедурите за сигурност за защита на класифицирана информация, прилагани от съответната Страна.

(4) При поискване, Компетентните органи, в съответствие с националното си законодателство, си оказват взаимно съдействие при процедурите за издаване на разрешение за достъп до класифицирана информация и удостоверение за сигурност.

(5) Страните взаимно признават своите разрешения за достъп до класифицирана информация и удостоверения за сигурност, в съответствие с националното си законодателство.

(6) В рамките на обхвата на това Споразумение, Компетентните органи незабавно се информират взаимно за отнемане на разрешения за достъп и удостоверения за сигурност или за изменение на нивото на класификация за сигурност.

(7) Службите за сигурност и разузнаване на Страните могат директно да обменят класифицирана информация, в съответствие с националното законодателство.

(8) Страните взаимно се информират по дипломатически път за всички последващи промени в техните Компетентни органи.

Член 7
Пренасяне на класифицирана информация

(1) Класифицирана информация се пренася чрез дипломатически или военни куриери, или чрез други средства, одобрени предварително от Компетентните органи в съответствие с националното законодателство.

(2) Електронното предаване на класифицирана информация се осъществява чрез одобрени криптографски средства в съответствие с националното законодателство.

(3) Ако пренасяната класифицирана информация е маркирана с ниво на класификация SECRET LUX /SECRET/ СЕКРЕТНО и по-високо, Страната-получател трябва да потвърждава получаването писмено. Получаването на друга класифицирана информация се потвърждава при поискване.

Член 8
Размножаване, превод, унищожаване на класифицирана информация.
Промяна и премахване на ниво на класификация за сигурност.

(1) Класифицирана информация с ниво за класификация за сигурност TRES SECRET LUX /TOP SECRET/ СТРОГО СЕКРЕТНО се превежда или размножава само с предварителното писмено разрешение на Компетентния орган на Страната-източник.

(2) Всички преводи на класифицирана информация се правят от лица, които имат разрешение за достъп до подходящото ниво на класификация за сигурност. Такива преводи трябва да са със същото ниво на класификация в съответствие с член 4 на това Споразумение.

(3) Всички преводи трябва да имат обозначение, което показва, че съдържат класифицирана информация, получена от Страната-източник.

(4) Когато класифицирана информация е размножавана, нивото на класификацията за сигурност на оригинала трябва да се поставя на всяко копие. Такава размножена информация трябва да се намира под същия контрол както оригиналната информация. Броят на копията трябва да бъде ограничен до необходимия брой за служебни цели.

(5) Страната-получател не трябва да променя и/или премахва нивото на класификация на получената класифицирана информация без предварително писмено разрешение на Страната-източник.

(6) Класифицирана информация се унищожава по начин, непозволяващ нейното възстановяване изцяло или отчасти, в съответствие с националното законодателство.

(7) Страната-източник може изрично да забрани размножаването или унищожаването на класифицирана информация чрез поставяне на маркировка върху съответния носител на класифицирана информация или чрез изпращане на допълнително писмено уведомление. Ако унищожаването на класифицирана информация е забранено тя трябва да бъде върната на Страната-източник.

(8) Класифицирана информация с ниво на класификация за сигурност TRES SECRET LUX /TOP SECRET/ СТРОГО СЕКРЕТНО не се унищожава. Тя трябва да бъде върната на Страната-източник.

(9) Класифицирана информация маркирана SECRET LUX /SECRET/ СЕКРЕТНО се унищожава в съответствие с националното законодателство след като Страната-получател вече не я счита за необходима.

(10) В случай на кризисна ситуация, при която е невъзможно да се защити и върне обратно класифицирана информация, създадена или пренесена в съответствие с това Споразумение, класифицираната информация се унищожава незабавно. Страната-получател при първа възможност уведомява писмено Компетентния орган на Страната-източник за унищожаването на класифицираната информация.

Член 9
Класифицирани договори

(1) Класифицирани договори се сключват и изпълняват в съответствие с националното законодателство.

(2) При поискване, Компетентният орган на Страната-получател потвърждава, че на предложен Контрагент е издадено съответното разрешение за достъп до класифицирана информация или удостоверение за сигурност. Ако предложеният Контрагент не притежава съответното разрешение за достъп/удостоверение за сигурност, Компетентният орган на Страната-източник може да отправи искане до Компетентния орган на Страната-получател да издаде разрешение за достъп/удостоверение за сигурност.

(3) Компетентният орган в държавата, на чиято територия ще се изпълнява класифицираният договор, поема отговорността за определяне и администриране на мерките за сигурност за класифицирания договор при същите стандарти и изисквания, които регламентират защитата на неговите собствени класифицирани договори. Периодичните инспекции по сигурността могат да се извършват в съответствие с националното законодателство.

(4) Контрагентът е задължен да:

а) притежава удостоверение за сигурност за необходимото ниво на класификация за сигурност;

б) гарантира, че лицата, за които се изисква достъп до класифицирана информация, притежават разрешение за достъп до класифицирана информация до необходимото ниво на класификация за сигурност;

в) осигурява, че всички лица, на които е даден достъп до класифицирана информация, са информирани за своите отговорности да защитават класифицираната информация в съответствие с националното законодателство;

г) извършва периодични инспекции по сигурността на своите помещения.

(5) Подизпълнителите, наети по класифицирани договори, трябва да спазват изискванията за сигурност, прилагани за Контрагентите.

(6) Всеки класифициран договор, сключен в съответствие с това Споразумение, трябва да включва съответен анекс по сигурността, който е неразделна част от класифицирания договор, определящ следните аспекти:

а) ръководство за класифициране;

б) процедура за комуникация при промени в нивото на класификация за сигурност на информацията;

в) канали за комуникация и начини за електромагнитен пренос;

г) процедури за пренасяне на класифицирана информация;

д) данни за контакт на Компетентните органи, отговарящи за координацията на защитата на класифицираната информация, свързана с договора;

е) задължение за уведомяване за всяко нарушаване на мерките за сигурност или предположение за извършено такова.

(7) Копие на анекса по сигурността на всички класифицирани договори се изпраща до Компетентния орган на Страната, в която ще се изпълнява класифицираният договор, за да се позволи адекватен надзор и контрол върху стандартите, процедурите и практиките за сигурност, създадени от Контрагентите за защитата на класифицираната информация.

(8) Представители на Компетентните органи могат да извършват посещения един на друг, за да анализират ефективността на мерките, приети от Контрагента за защита на класифицираната информация, включена в класифициран договор. Уведомление за посещението следва да бъде предоставено най-малко 3 (три) седмици предварително.

Член 10
Посещения

(1) За посещения, включващи достъп до класифицирана информация, е необходимо предварително разрешение на Компетентния орган на приемащата Страна.

(2) Искането за посещение трябва да бъде изпратено най-малко 3 седмици преди посещението и да съдържа:

а) собствено и фамилно име на посетителя, дата и място на раждане, националност;

б) номер на паспорт или друг номер на лична карта на посетителя;

в) заеманата от посетителя длъжност и наименование на организацията, която представлява;

г) ниво на разрешението за достъп до класифицирана информация на посетителя, ако е приложимо;

д) цел, предложена работна програма и планирана дата на посещението;

е) наименования на организациите и структурите, за които е отправено искане да бъдат посетени;

ж) брой на посещенията и изисквания период;

з) данни за контакт на служителите по сигурността на структурите;

и) други данни, съгласувани от Компетентните органи.

(3) За прилагането на това Споразумение могат да се извършват многократни посещения. Компетентните органи на Страните одобряват списък с упълномощени лица, които да извършват многократни посещения. Тези списъци са валидни за първоначален период от дванадесет месеца. След като списъците бъдат одобрени от Компетентните органи на Страните, условията на конкретните посещения се уреждат директно между служителите по сигурността на структурите, които ще бъдат посетени от лицата.

(4) Всяка страна трябва да гарантира защитата на личните данни на посетителите в съответствие с националното законодателство.

Член 11
Нарушаване на мерките за сигурност

(1) Компетентният орган на Страната-получател незабавно информира Компетентния орган на Страната-източник за всяко предположение за или настъпило разкриване на нарушаване на мерките за сигурност.

(2) Компетентният орган на Страната-получател предприема всички възможни, подходящи мерки в съответствие със своето национално законодателство, за да ограничи последиците от нарушаването на мерките за сигурност и да предотврати по-нататъшни нарушения, както и да осигури съответно разследване. При отправено искане, Компетентният орган на Страната-източник предоставя съдействие в разследването. Компетентният орган на Страната-получател информира писмено Компетентния орган на Страната-източник за резултата от процедурата и коригиращите действия, предприети поради нарушението.

(3) В случаите, когато нарушаване на мерките за сигурност се извърши в трета държава, Компетентният орган на изпращащата Страна трябва да предприеме действията по ал. 2, когато това е възможно.

Член 12
Разходи

Всяка Страна поема разходите, възникнали в хода на изпълнение на задълженията ѝ по това Споразумение.

Член 13
Разрешаване на спорове

Всеки спор относно тълкуването или прилагането на това Споразумение се решава чрез консултации и преговори между Страните.

Член 14
Заключителни разпоредби

(1) Това Споразумение влиза в сила на първия ден от втория месец следващ датата на получаване по дипломатически път между Страните на последното писмено уведомление, с което Страните се информират, че националните правни изисквания за влизането в сила на това Споразумение са изпълнени.

(2) Това Споразумение може да се изменя на базата на взаимно писмено съгласие между Страните. Измененията следва да бъдат неразделна част от това Споразумение. Измененията влизат в сила в съответствие с ал. 1 на този член.

(3) Това Споразумение се сключва за неопределен период от време. Всяка Страна може да прекрати това Споразумение, като предостави на другата Страна писмено уведомление по дипломатически път. В такъв случай това Споразумение изтича шест месеца след датата на получаване на уведомлението за прекратяване от другата Страна.

(4) В случай на прекратяване на това Споразумение, всяка класифицирана информация, обменена в изпълнение на това Споразумение, продължава да бъде защитавана в съответствие с посочените в него разпоредби и при поискване се връща обратно на Страната-източник.

Подписано в София, на 29 януари 2018 г., в два оригинални екземпляра, всеки от които на френски, английски и български език, като трите текста имат еднаква сила. В случай на различия при тълкуването, меродавен е текстът на английски език.

За Правителството на Великото Херцогство Люксембург

Роналд Дофинг
Посланик на Великото Херцогство Люксембург в Република България

За Правителството на Република България

Борис Димитров
Председател на Държавната комисия по сигурността на информацията

[ENGLISH TEXT – TEXTE ANGLAIS]

AGREEMENT

BETWEEN

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG

AND

THE GOVERNMENT OF THE REPUBLIC OF BULGARIA

ON EXCHANGE AND MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Grand Duchy of Luxembourg and the Government of the Republic of Bulgaria (hereinafter referred to as the "Parties"),

Realising that effective co-operation in political, economic, military, security, intelligence and any other area may require exchange of Classified Information between the Parties,

Realising that good co-operation may require exchange of Classified Information between the Parties,

Desiring to create a set of rules regulating the mutual protection of Classified Information exchanged between the Parties under any future co-operation agreements and/or Classified contracts.

Have agreed as follows:

Article 1
Objective and scope

(1) The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties.

(2) This Agreement shall be applicable to any activities, contracts or agreements involving Classified Information that will be conducted or concluded between the Parties in the future.

(3) The provisions of this Agreement shall also apply to the Classified Information already generated or exchanged in the process of cooperation between the Parties before entering into force of this Agreement.

Article 2
Definitions

For the purpose of this Agreement:

(1) "**Classified Information**" means information of whatever form, nature or method of transmission either manufactured or in the process of manufacture to which a security classification level has been attributed and which, in the interests of national security and in accordance with the national laws and regulations, requires protection against unauthorised access.

(2) **"Security classification level"** means category, according to the national laws and regulations, which characterises the importance of Classified Information, the level of restriction of access to it and the level of its protection by the Parties, and also the category on the basis of which information is marked.

(3) **"Personnel Security Clearance"** means determination, issued by the respective national authority as a result of a vetting procedure, which ascertains that a certain individual may be granted access to Classified Information in accordance with the national laws and regulations.

(4) **"Facility Security Clearance"** means determination, issued by the respective national authority as a result of a vetting procedure, which ascertains that, on the matters of security, a certain legal entity meets the physical and organisational requirements for generation, process and storing of Classified Information in accordance with the national laws and regulations.

(5) **"Need-to-know" principle"** means the necessity to have access to Classified Information in connection with official duties and/or for the performance of a concrete official task.

(6) **"Competent Authority"** means the national authority, which in compliance with the national laws and regulations of the respective Party, performs the state policy for the protection of Classified Information, exercises overall control in this sphere, as well as conducts the implementation of this Agreement. Such authorities are listed in Article 3 of this Agreement.

(7) **"Originating Party"** means the Party which transmits Classified Information.

(8) **"Receiving Party"** means the Party to which Classified Information is transmitted.

(9) **"Third Party"** means a state or international organisation, which is not a Party to this Agreement.

(10) **"Classified Contract"** means an agreement between two or more Contractors which contains Classified Information or requires access to Classified Information.

(11) **"Contractor"** means an individual or a legal entity possessing the legal capacity to conclude contracts and/or is a party to a classified contract.

(12) "**Sub-contractor**" means a Contractor to whom a prime Contractor lets a sub-contract.

(13) **"Breach of security"** means an act or an omission contrary to the national laws and regulations, which results or may result in an unauthorised access of Classified Information.

(14) **"Unauthorised access of Classified Information"** means any form of disclosure of Classified Information, including misuse, modification, damage, disclosure, destruction or incorrect classification of Classified Information, as well as any other action compromising its protection or resulting in the loss of such information. Unauthorised access shall be deemed to be also any action or omission resulting in knowledge of such information being acquired by any person who does not possess a Personnel Security Clearance/Facility Security Clearance and who does not have "the need to know".

Article 3
Competent Authorities

The Competent Authorities of the Parties are:

For the Grand Duchy of Luxembourg:

- Service de renseignement de l'État
  Autorité nationale de Sécurité (National Security Authority)

For the Republic of Bulgaria:

State Commission on Information Security;

Article 4
Security Classification Levels

The Parties agree that the following security classification levels are equivalent and correspond to the security classification levels specified in the national laws and regulations of the respective Party:

For the Grand Duchy of Luxembourg	Equivalent in English	For the Republic of Bulgaria
TRES SECRET LUX	TOP SECRET	СТРОГО СЕКРЕТНО
SECRET LUX	SECRET	СЕКРЕТНО
CONFIDENTIEL LUX	CONFIDENTIAL	ПОВЕРИТЕЛНО
RESTREINT LUX	RESTRICTED	ЗА СЛУЖЕБНО ПОЛЗВАНЕ

Article 5
Measures for the protection of Classified Information

(1) In compliance with their national laws and regulations, the Parties shall implement all appropriate measures for protection of Classified Information, which is commonly generated or exchanged under this Agreement. The same level of protection shall be ensured for such Classified Information as it is provided for the national Classified Information, with the corresponding security classification level.

(2) The Security classification level of the mutually generated Classified Information under this Agreement, is defined by mutual consent of the Parties.

(3) The Parties shall in due time inform each other about any changes in the national laws and regulations affecting the protection of Classified Information. In such cases, the Parties shall inform each other in written form in order to discuss possible amendments to this Agreement. Meanwhile, the Classified Information shall be protected according to the provisions of the Agreement, unless otherwise agreed in writing.

(4) Classified Information shall only be made accessible to individuals who are authorized in accordance with national laws and regulations to have access to Classified Information of the equivalent security classification level and who have a Need-to-know and who have been briefed accordingly.

(5) The Receiving Party is obligated:

a) not to disclose Classified Information to a Third Party without a prior written consent of the Competent Authority of the Originating Party;

b) to grant Classified Information a security classification level equivalent to that provided by the Originating Party;

c) not to use Classified Information for other purposes than those it has been provided for.

(6) If any other Agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these regulations shall apply.

Article 6
Security Co-operation

(1) The Competent Authorities shall inform each other of the national laws and regulations in force, regulating the protection of Classified Information.

(2) In order to ensure close co-operation in the implementation of this Agreement, the Competent Authorities may hold consultations at the request made by one of them.

(3) In order to achieve and maintain comparable standards of security, the Competent Authorities, on request, provide each other with information about the security standards, procedures and practices for protection of Classified Information, applied by the respective Party.

(4) On request, the Competent Authorities, in accordance with their national laws and regulations, assist each other throughout the procedures for issuance of a Personnel Security Clearance and Facility Security Clearance.

(5) The Parties mutually recognize their Personnel Security Clearances and Facility Security Clearances, in accordance with their national laws and regulations.

(6) Within the scope of this Agreement, the Competent Authorities shall inform each other without delay about revocation of Personnel and Facility Security Clearances or the alteration of the security classification level.

(7) The Security and Intelligence Services of the Parties may directly exchange Classified Information in accordance with national laws and regulations.

(8) The Parties notify each other through diplomatic channels of any subsequent changes of their Competent Authorities.

Article 7
Transfer of Classified Information

(1) Classified Information shall be transferred by means of diplomatic or military couriers or by other means, approved in advance by the Competent Authorities in accordance with national laws and regulations.

(2) Electronic transmission of Classified Information shall be carried out through certified cryptographic means in accordance with national laws and regulations.

(3) If transferred Classified Information is marked СЕКРЕТНО /SECRET/ SECRET LUX and above, the Receiving Party shall confirm the receipt in writing. The receipt of other Classified Information shall be confirmed on request.

Article 8
Translation, reproduction, destruction of Classified Information. Changing and removing of Security classification level.

(1) Classified Information with a security classification level СТРОГО СЕКРЕТНО / TOP SECRET / TRES SECRET LUX shall be translated or reproduced only by written permission of the Competent Authority of the Originating Party.

(2) All translations of Classified Information shall be made by individuals who have a security clearance up to the appropriate security classification level. Such translations shall bear an equal security classification level in accordance with Article 4 of this Agreement.

(3) All translations shall bear a designation which shows that they contain Classified Information received by the Originating Party.

(4) When Classified Information is reproduced, the security classification level of the original shall also be marked on each copy. Such reproduced information shall be placed under the same control as the original information. The number of copies shall be limited to that required for official purposes.

(5) The Receiving Party shall not change and/or remove the security classification level of the received Classified Information without prior written permission of the Originating Party.

(6) Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part in accordance with national laws and regulations.

(7) The Originating Party may explicitly prohibit the reproduction or destruction of Classified Information by marking the relevant carrier of Classified Information or sending subsequent written notice. If destruction of the Classified Information is prohibited, it shall be returned to the Originating Party.

(8) Classified Information of СТРОГО СЕКРЕТНО / TOP SECRET / TRES SECRET LUX security classification level shall not be destroyed. It shall be returned to the Originating Party.

(9) Information classified as СЕКРЕТНО/SECRET/SECRET LUX shall be destroyed in accordance with the national laws and regulations after it is no longer consider necessary by the Receiving Party.

(10) In case of a crisis situation which makes it impossible to protect and return Classified Information, generated or transferred according to this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Authority of the Originating Party in writing about the destruction of the Classified Information as soon as possible.

Article 9
Classified Contracts

(1) Classified Contracts shall be concluded and implemented in accordance with national laws and regulations.

(2) Upon request the Competent Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security

clearance, the Competent Authority of the Originating Party may request the Competent Authority of the Receiving Party to issue the appropriate security clearance.

(3) The Competent Authority in which state's territory the Classified Contract is to be performed, shall assume the responsibility for prescribing and administering security measures for the Classified Contract under the same standards and requirements that govern the protection of its own Classified Contracts. Periodical security inspections may be carried out in accordance with national laws and regulations.

(4) The Contractor shall be obliged to:

a) hold a Facility Security Clearance at the appropriate security classification level;

b) ensure that the individuals requiring access to Classified Information hold a Personnel Security Clearance at the appropriate security classification level;

c) ensure that all individuals, granted access to Classified Information, are informed of their responsibilities to protect Classified Information in accordance with national laws and regulations;

d) perform periodic security inspections of its premises.

(5) Sub-contractors engaged in Classified Contracts shall comply with the security requirements applied to the Contractors.

(6) Every Classified Contract concluded in accordance with this Agreement shall include an appropriate security annex which is an integral part of the Classified Contract identifying the following aspects:

a) a classification guide;

b) a procedure for the communication of changes in the security classification level of the information;

c) communication channels and means for electromagnetic transmission;

d) procedures for the transportation of Classified Information;

e) contact details of the Competent Authorities responsible for the co-ordination of the protection of Classified Information related to the Contract;

f) an obligation to notify any actual or suspected Breach of Security.

(7) A copy of the security annex of all Classified Contracts shall be forwarded to the Competent Authority of the Party where the Classified Contract is to be performed, to allow an adequate supervision and control of the security standards, procedures and practices established by the Contractors for the protection of Classified Information.

(8) Representatives of the Competent Authorities may visit each other in order to analyse the efficiency of the measures adopted by a Contractor for the protection of the Classified Information involved in a Classified Contract. Notice of the visit shall be provided, at least, three (3) weeks in advance.

Article 10
Visits

(1) Visits that involve access to Classified Information shall be subject to prior permission by the Competent Authority of the host Party.

(2) The request for visit shall be submitted at least 3 weeks prior to the visit and shall contain:

a) visitor's name and surname, date and place of birth, nationality;
b) passport number or another identification card number of the visitor;
c) position of the visitor and name of the organization represented;
d) level of the Personnel Security Clearance of the visitor, if applicable;
e) purpose, proposed working program and planned date of the visit;
f) names of organizations and facilities requested to be visited;
g) number of visits and period required;
h) contact details of the Security Officers of the facilities;
i) other data, agreed upon by the Competent Authorities.

(3) For the implementation of this Agreement recurring visits may be executed. The Competent Authorities of the Parties approve a list of authorised individuals to make recurring visits. Those lists are valid for an initial period of twelve months. Once the lists have been approved by the Competent Authorities of the Parties, the terms of the concrete visits shall be directly arranged with the Security Officers of the facilities to be visited by the individuals.

(4) Each Party shall guarantee the protection of personal data of the visitors in accordance with national laws and regulations.

Article 11
Breach of Security

(1) The Competent Authority of the Receiving Party shall immediately notify the Competent Authority of the Originating Party of any suspicion or discovery of a Breach of Security.

(2) The Competent Authority of the Receiving Party shall undertake all possible appropriate measures in accordance with its national laws and regulations so as to limit the consequences of the Breach of Security and to prevent further violations and ensure the appropriate investigation. On request, the Competent Authority of the Originating Party shall provide investigative assistance. The Competent Authority of the Receiving Party shall inform in writing the Competent Authority of the Originating Party of the outcome of the proceedings and the corrective measures undertaken due to the violation.

(3) If a Breach of security occurs in a third country, the Competent Authority of the dispatching Party shall take the actions under paragraph 2, where possible.

Article 12
Costs

Each Party shall bear the costs incurred in the course of implementing its obligations under this Agreement.

Article 13
Settlement of Disputes

Any dispute regarding the interpretation or application of this Agreement shall be settled by consultations and negotiations between the Parties.

Article 14
Final Provisions

(1) This Agreement shall enter into force on the first day of the second month after the date of the receipt of the latest written notification by which the Parties have notified each other, through diplomatic channels, that their national legal requirements necessary for its entry into force have been fulfilled.

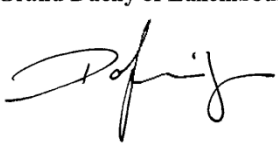
(2) This Agreement may be amended by mutual written consent of the Parties. The amendments shall be the integral part of this Agreement. Such amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

(3) This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party written notice through diplomatic channels. In that case, this Agreement shall terminate six months from the date on which the other Party has received the denunciation notice.

(4) In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

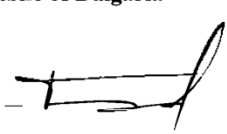
Done at Sofia on 29 January 2018 in 2 original copies, each in the French, English and Bulgarian languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the
Grand Duchy of Luxembourg



Ronald DOFING
Ambassador
of the Grand Duchy of Luxembourg
to the Republic of Bulgaria

For the Government of the
Republic of Bulgaria



Boris DIMITROV
Chairperson
of the State Commission
on Information Security

[FRENCH TEXT – TEXTE FRANÇAIS]

ACCORD

ENTRE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

ET

LE GOUVERNEMENT DE LA RÉPUBLIQUE DE BULGARIE

RELATIF À L'ÉCHANGE ET À LA PROTECTION RÉCIPROQUE D'INFORMATIONS CLASSIFIÉES

Le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement de la République de Bulgarie, ci-après dénommés les «Parties»,

Reconnaissant qu'une coopération efficace dans les domaines politique, économique, militaire, de la sécurité ou de l'intelligence, et dans tout autre domaine, peut exiger l'échange d'informations classifiées entre les Parties,

Reconnaissant qu'une coopération satisfaisante peut exiger l'échange d'informations classifiées entre les Parties,

Désirant créer un ensemble de règles régissant la protection réciproque d'informations classifiées échangées entre les Parties dans le cadre de tout futur accord de coopération et/ou contrat classifié.

Conviennent ce qui suit :

Article premier
Objet et champ d'application

(1) Le présent Accord a pour but de garantir la protection des informations classifiées généralement produites ou échangées entre les Parties.

(2) Le présent Accord est applicable à l'ensemble des activités, contrats ou accords impliquant des informations classifiées qui seront menés ou conclus entre les Parties à l'avenir.

(3) Les dispositions du présent Accord s'appliquent également aux informations classifiées déjà produites ou échangées dans le cadre d'une coopération entre les Parties avant l'entrée en vigueur des présentes.

Article 2
Définitions

Aux fins du présent Accord :

(1) les « **informations classifiées** » désignent les informations, quel qu'en soit la forme, la nature ou le mode de transmission, qu'elles soient élaborées ou en cours d'élaboration, auxquelles un degré de classification de sécurité a été attribué et qui, dans l'intérêt de la sécurité nationale et conformément aux lois et réglementations nationales, nécessitent une protection contre tout accès non autorisé.

(2) le « **niveau de classification de sécurité** » désigne la catégorie qui, conformément aux lois et réglementations nationales, caractérise l'importance des informations classifiées, le niveau de restriction dont leur accès fait l'objet et le degré de protection dont elles doivent bénéficier de la part des Parties, ainsi que la catégorie sur la base de laquelle les informations sont identifiées.

(3) une « **habilitation de sécurité pour une personne physique** » renvoie à une décision rendue par l'autorité nationale pertinente à l'issue d'une procédure de vérification, selon laquelle une personne peut se voir accorder l'accès à des informations classifiées conformément aux lois et réglementations nationales.

(4) une « **habilitation de sécurité pour une personne morale** » renvoie à une décision rendue par l'autorité nationale pertinente à l'issue d'une procédure de vérification, selon laquelle, eu égard à la sécurité, une personne morale donnée satisfait aux exigences matérielles et organisationnelles applicables à l'élaboration, au traitement et au stockage d'informations classifiées, conformément aux lois et réglementations nationales.

(5) le « **principe du besoin d'en connaître** » renvoie à la nécessité d'accéder à des informations classifiées dans le cadre de devoirs officiels et/ou d'une mission officielle concrète.

(6) une « **autorité compétente** » désigne l'autorité nationale qui, conformément aux lois et réglementations nationales de la Partie concernée, mène les travaux relatifs à la politique de l'État en matière de protection des informations classifiées, exerce un contrôle global dans ce domaine et assure la mise en œuvre des modalités du présent Accord. Ces autorités sont énumérées à l'article 3 du présent Accord.

(7) la « **Partie d'origine** » désigne la Partie qui transmet les informations classifiées.

(8) la « **Partie destinataire** » désigne la Partie à laquelle sont transmises les informations classifiées.

(9) une « **tierce partie** » désigne tout État ou toute organisation internationale qui n'est pas l'une des Parties au présent Accord.

(10) un « **contrat classifié** » désigne un accord entre deux contractants ou plus, lequel contient des informations classifiées ou requiert un accès aux informations classifiées.

(11) un « **contractant** » désigne toute personne physique ou morale dotée de la capacité juridique de conclure des contrats et/ou étant partie à un contrat classifié.

(12) un « **sous-traitant** » désigne tout contractant avec lequel le premier contractant conclut un contrat de sous-traitance.

(13) une « **infraction à la sécurité** » désigne tout acte ou toute omission contraire aux lois et réglementations nationales et se traduisant ou étant susceptible de se traduire par un accès non autorisé aux informations classifiées.

(14) un « **accès non autorisé aux informations classifiées** » désigne toute forme de divulgation d'informations classifiées, en ce compris toute utilisation inappropriée, modification, détérioration, divulgation, destruction ou classification incorrecte d'informations classifiées, ainsi que toute autre action compromettant leur protection ou se traduisant par leur perte. Un accès non autorisé désigne par ailleurs toute action ou omission entraînant l'acquisition de telles informations par toute personne ne disposant pas d'une habilitation de sécurité individuelle/d'établissement et n'ayant pas « besoin d'en connaître ».

Article 3
Autorités compétentes

Les autorités compétentes des Parties sont :

Pour le Grand-Duché de Luxembourg :

- Le service de renseignement de l'État
  L'Autorité nationale de Sécurité (National Security Authority)

Pour la République de Bulgarie :

- La Commission d'État chargée de la Sécurité de l'information ;

Article 4
Niveaux de classification de sécurité

Les Parties reconnaissent que les niveaux de sécurité suivants sont équivalents et correspondent aux niveaux de sécurité spécifiés dans les lois et réglementations nationales de la Partie concernée :

Pour le Grand-Duché de Luxembourg	Équivalent en anglais	Pour la République de Bulgarie
TRÈS SECRET LUX	TOP SECRET	СТРОГО СЕКРЕТНО
SECRET LUX	SECRET	СЕКРЕТНО
CONFIDENTIEL LUX	CONFIDENTIAL	ПОВЕРИТЕЛНО
RESTREINT LUX	RESTRICTED	ЗА СЛУЖЕБНО ПОЛЗВАНЕ

Article 5
Mesures applicables à la protection d'informations classifiées

(1) Conformément à leurs lois et réglementations nationales, les Parties mettent en œuvre toutes les mesures appropriées afin de protéger les informations classifiées généralement produites ou échangées en vertu du présent Accord. Elles garantissent auxdites informations classifiées un niveau de protection équivalent à celui qui est accordé à leurs informations classifiées nationales assorties du niveau de classification de sécurité correspondant.

(2) Le niveau de classification de sécurité des informations classifiées mutuellement produites en vertu des présentes est établi d'un commun accord entre les Parties.

(3) Chaque Partie s'engage à informer l'autre en temps opportun de toute évolution des lois et réglementations nationales affectant la protection des informations classifiées. Dans un tel cas, la Partie concernée informera l'autre par écrit afin de discuter des modifications éventuelles à apporter aux présentes. Dans l'intervalle, les informations classifiées seront protégées conformément aux dispositions des présentes, sauf accord contraire des Parties formulé par écrit.

(4) L'accès aux informations classifiées est exclusivement réservé aux personnes autorisées, en vertu des lois et réglementations nationales, à accéder à des informations classifiées d'un niveau de classification de sécurité équivalent, qui ont besoin de connaître de telles informations et ont été informées en conséquence.

(5) La Partie destinataire s'engage :

a) à ne délivrer aucune information classifiée à une tierce partie sans l'accord écrit de l'autorité compétente de la Partie d'origine ;

b) à octroyer aux informations classifiées un niveau de classification de sécurité équivalent à celui que leur a octroyé la Partie d'origine ;

c) à ne pas utiliser d'informations classifiées à d'autres fins que celles auxquelles elles lui ont été transmises.

(6) Si tout autre Accord conclu entre les Parties comporte des règles plus strictes eu égard à l'échange ou à la protection des informations classifiées, de telles règles s'appliquent.

Article 6
Coopération à des fins de sécurité

(1) Les autorités compétentes se tiennent mutuellement informées des lois et réglementations nationales en vigueur en matière de protection des informations classifiées.

(2) Afin de garantir une coopération efficace dans l'exécution des présentes, les autorités compétentes peuvent organiser des consultations si l'une d'entre elles en formule la demande.

(3) En vue d'appliquer et de maintenir des normes de sécurité similaires, les autorités compétentes se tiennent, sur demande, mutuellement informées des normes, procédures et pratiques de sécurité appliquées par chaque Partie en matière de protection des informations classifiées.

(4) Sur demande, les autorités compétentes, conformément à leurs lois et réglementations nationales, s'assistent mutuellement dans le cadre des procédures visant à établir une habilitation de sécurité du personnel ou une habilitation de sécurité d'installation.

(5) Les Parties reconnaissent mutuellement leurs habilitations de sécurité du personnel et d'installation, conformément à leurs lois et réglementations nationales.

(6) Dans le cadre du présent Accord, les autorités compétentes se tiennent mutuellement informées sans délai de toute révocation d'habilitation de sécurité du personnel et d'installation ou de toute modification apportée au niveau de classification de sécurité.

(7) Les services de sécurité et d'intelligence des Parties peuvent directement échanger des informations classifiées conformément aux lois et réglementations nationales.

(8) Les Parties se tiennent mutuellement informées, par la voie diplomatique, de toute modification apportée à leurs autorités compétentes.

Article 7
Transfert d'informations classifiées

(1) Les informations classifiées seront transférées par des coursiers diplomatiques ou militaires ou par tout autre moyen approuvé préalablement par les autorités compétentes conformément aux lois et réglementations nationales.

(2) La transmission électronique d'informations classifiées est effectuée par le biais de méthodes cryptographiques certifiées conformément aux lois et réglementations nationales.

(3) Si des informations classifiées transmises sont identifiées comme étant de niveau СЕКРЕТНО /SECRET/ SECRET LUX ou d'un niveau supérieur, la Partie destinataire en confirmera la réception par écrit. La réception des autres informations classifiées sera confirmée sur demande.

Article 8
Traduction, reproduction, destruction d'informations classifiées. Modification et suppression d'un niveau de classification de sécurité.

(1) Les informations classifiées identifiées comme étant de niveau СТРОГО СЕКРЕТНО / TOP SECRET / TRÈS SECRET LUX seront exclusivement traduites ou reproduites sur autorisation écrite de l'autorité compétente de la Partie d'origine.

(2) Toutes les traductions d'informations classifiées seront effectuées par des personnes disposant d'une habilitation de sécurité correspondant au niveau de classification de sécurité approprié. Les traductions ainsi produites seront assorties d'un niveau de classification de sécurité équivalent à celui des informations d'origine, conformément à l'article 4 des présentes.

(3) Toutes les traductions porteront une mention indiquant qu'elles contiennent des informations classifiées reçues par la Partie d'origine.

(4) Lors de la reproduction d'informations classifiées, le niveau de classification de sécurité des informations originales sera également indiqué sur chaque exemplaire. Les informations ainsi reproduites sont placées sous le même niveau de contrôle que les informations originales. Le nombre de copies est limité à celui requis pour un usage officiel.

(5) La Partie destinataire ne pourra modifier et/ou supprimer le niveau de classification de sécurité des informations classifiées reçues sans l'accord écrit préalable de la Partie d'origine.

(6) Les informations classifiées seront détruites dans la mesure requise pour empêcher leur reconstruction en tout ou partie, conformément aux lois et réglementations nationales.

(7) La Partie d'origine pourra explicitement interdire la reproduction ou la destruction d'informations classifiées en apposant sur le conteneur des informations concernées le marquage correspondant, ou au moyen d'une notification écrite envoyée par la suite. Les informations classifiées dont la destruction est interdite doivent être restituées à la Partie d'origine.

(8) Les informations classifiées assorties du niveau de classification de sécurité СТРОГО СЕКРЕТНО / TOP SECRET / TRÈS SECRET LUX ne doivent pas être détruites. Celles-ci doivent être renvoyées à la Partie d'origine.

(9) Les informations classifiées СЕКРЕТНО/SECRET/SECRET LUX seront détruites conformément aux lois et réglementations nationales dès lors que la Partie destinataire n'en a plus l'utilité.

(10) Dans le cas d'une situation de crise rendant impossible la protection et le renvoi des informations classifiées produites ou échangées en vertu du présent Accord, les informations classifiées sont détruites immédiatement. La Partie destinataire informera dès que possible l'autorité compétente de la Partie d'origine de la destruction des informations classifiées.

Article 9
Contrats classifiés

(1) Les contrats classifiés seront conclus et exécutés conformément aux lois et réglementations nationales.

(2) Sur demande, l'autorité compétente de la Partie destinataire confirmera qu'un Contractant proposé s'est vu octroyer une habilitation de sécurité. Si le Contractant proposé ne détient pas l'habilitation de sécurité appropriée, l'autorité compétente de la Partie d'origine peut demander à celle de la Partie destinataire d'établir une telle habilitation.

(3) Il incombe à l'autorité compétente dont le territoire est visé par l'exécution du Contrat classifié de prescrire et d'administrer les mesures de sécurité applicables audit contrat selon les mêmes normes et les mêmes exigences que celles qui régissent la protection de ses propres Contrats classifiés. Des inspections périodiques de la sécurité pourront être effectuées conformément aux dispositions des lois et réglementations nationales.

(4) Le Contractant sera tenu de :

a) détenir une habilitation de sécurité d'un niveau de classification de sécurité approprié ;

b) garantir que les personnes demandant à accéder à des informations classifiées disposent d'une habilitation de sécurité du d'un niveau approprié ;

c) s'assurer que toutes les personnes qui se voient octroyer l'accès à des informations classifiées sont tenues informées de leurs responsabilités en matière de protection des informations, conformément aux lois et réglementations nationales ;

d) réaliser des inspections périodiques de la sécurité sur ses installations.

(5) Les sous-traitants engagés au titre de Contrats classifiés se conformeront aux exigences de sécurité applicables aux contractants.

(6) Chaque contrat classifié conclu conformément aux dispositions des présentes comportera une annexe relative à la sécurité appropriée, laquelle fera partie intégrante du contrat en question et répertoriera les aspects suivants :

a) un guide de classification ;

b) une procédure relative à la communication des modifications apportées aux niveaux de classification de sécurité des informations ;

c) des voies de communication et des moyens de transmission électromagnétique ;

d) les procédures relatives au transport d'informations classifiées ;

e) les coordonnées des autorités compétentes en charge de la coordination de la protection des informations classifiées liées au contrat ;

f) une obligation de signaler toute infraction à la sécurité avérée ou suspectée.

(7) Une copie de l'annexe relative à la sécurité de tous les contrats classifiés sera transmise à l'autorité compétente de la Partie visée par l'exécution du contrat classifié en question, afin de lui permettre d'exercer une surveillance et un contrôle appropriés eu égard aux normes, procédures et pratiques de sécurité mises en œuvre par le contractant pour garantir la protection des informations classifiées.

(8) Les représentants des autorités compétentes peuvent effectuer des visites réciproques afin d'analyser l'efficacité des mesures adoptées par un contractant pour garantir la protection des informations classifiées impliquées dans un contrat classifié. Toute visite doit être notifiée au moins trois (3) semaines à l'avance.

Article 10
Visites

(1) Les visites impliquant l'accès à des informations classifiées sont soumises à l'autorisation préalable de l'autorité compétente de la Partie hôte.

(2) Toute demande de visite doit être soumise au minimum 3 semaines avant la visite et contenir :

a) le nom, le prénom, la date et le lieu de naissance, et la nationalité du visiteur ;
b) le numéro du passeport ou de la carte d'identité du visiteur ;
c) la qualité du visiteur et le nom de l'organisation représentée ;
d) le niveau de l'habilitation de sécurité individuelle du visiteur, le cas échéant ;
e) le but de la visite ainsi que le programme de travail proposé et la date prévue ;
f) les noms des organisations et des établissements objet de la visite ;
g) le nombre de visites requises et la période concernée ;
h) les coordonnées des agents affectés à la sécurité des installations concernées ;
i) toutes autres données convenues par les autorités compétentes.

(3) Aux fins de l'exécution des présentes, des visites récurrentes pourront être organisées. Les autorités compétentes des Parties approuvent une liste de personnes autorisées à effectuer des visites récurrentes. Ces listes sont valides pour une période initiale de douze mois. Une fois les listes approuvées par les autorités compétentes des Parties, les modalités des visites concrètes seront directement déterminées en collaboration avec les Agents affectés à la sécurité des sites concernés.

(4) Chacune des Parties garantit la protection des données personnelles des visiteurs conformément à ses lois et réglementations nationales.

Article 11
Infraction à la sécurité

(1) L'autorité compétente de la Partie destinataire informera sans délai l'autorité compétente de la Partie d'origine de toute infraction à la sécurité avérée ou suspectée.

(2) L'autorité compétente de la Partie destinataire prendra toutes les mesures appropriées possibles, conformément à ses lois et réglementations nationales, afin de limiter les conséquences de toute infraction à la sécurité et d'empêcher toute violation ultérieure, et veillera à mener une enquête appropriée. Sur demande, l'autorité compétente de la Partie d'origine apportera son aide dans le cadre d'une telle enquête. Sur demande, l'autorité compétente de la Partie destinataire informera par écrit l'autorité compétente de la Partie d'origine du résultat des procédures mises en œuvre et des mesures correctives entreprises à la suite de la violation.

(3) En cas d'infraction à la sécurité survenant dans un pays tiers, l'autorité compétente de la Partie à l'origine de la diffusion des informations prendra, dans la mesure du possible, les mesures visées par le paragraphe 2.

Article 12
Frais

Chacune des Parties assume les frais engagés du fait de l'exécution de ses obligations en vertu du présent Accord.

Article 13
Règlement des litiges

Tout litige quant à l'interprétation ou l'application du présent Accord est exclusivement résolu par voie de consultation et négociation entre les Parties.

Article 14
Dispositions finales

(1) Le présent Accord prend effet le premier jour du deuxième mois qui suit la réception de la dernière des notifications écrites par lesquelles les Parties se sont tenues mutuellement informées, par la voie diplomatique, de l'accomplissement des exigences légales nationales requises pour son entrée en vigueur.

(2) Le présent Accord peut être modifié d'un commun accord par écrit entre les Parties. Les modifications apportées aux présentes font partie intégrante du présent Accord. Ces modifications entrent en vigueur conformément aux dispositions du paragraphe 1 du présent article.

(3) Le présent Accord est conclu pour une durée indéterminée. Chaque Partie pourra mettre fin au présent Accord en informant l'autre Partie par écrit via les voies diplomatiques. Dans un tel cas, l'Accord prendra fin au terme d'un délai de six mois à partir de la date de réception de la résiliation par l'autre Partie.

(4) En cas de résiliation du présent Accord, toutes les informations classifiées échangées en vertu des présentes resteront protégées conformément aux clauses des présentes et seront, sur demande, restituées à la Partie d'origine.

Fait à Sofia, le 29 janvier 2018 en deux exemplaires originaux, chacun en langues française, anglaise et bulgare, tous les textes faisant également foi. Dans le cas d'un désaccord quant à l'interprétation des dispositions du présent Accord, le texte anglais prévaut.

Pour le Gouvernement du Grand-Duché de Luxembourg

Ronald DOFING
Ambassadeur
du Grand-Duché de Luxembourg
en République de Bulgarie

Pour le Gouvernement de la République de Bulgarie

Boris DIMITROV
Président
de la Commission d'état pour
la sécurité des informations