PERSONAL DATA PROCESSING AGREEMENT

FOR SAP SUPPORT AND PROFESSIONAL SERVICES

УГОДА ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

ДЛЯ ПОСЛУГ З ПІДТРИМКИ ТА ПРОФЕСІЙНИХ ПОСЛУГ SAP

1. BACKGROUND

1.1 Purpose and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between SAP and Customer. This DPA applies to Personal Data provided by Customer and each Data Controller in connection with the performance of the SAP services as set out in the relevant Agreement/Order Form ("SAP Service(s)") to which is attached the present DPA which may include:

(a) SAP Support as defined in the Software License and Support Agreement/Order Form; and/or

(b) Professional Services as described in the SAP Services Agreement/Order Form concluded between SAP and the Customer ("Services Agreement").

1.2 Structure. Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, the categories of data, the data subjects and the applicable technical and organizational measures.

1.3 GDPR. SAP and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.4 Governance. SAP acts as a Processor and Customer and those entities that it permits to include Personal Data in systems accessible by SAP when performing the SAP Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SAP as a Processor. Where authorizations, consent,

1. ЗАГАЛЬНА ІНФОРМАЦІЯ

1.1 Ціль та застосування. Умови, що містяться в цьому документі (далі – ««**Угода про обробку персональних даних**), є частиною Угоди та Договору в письмовій (в тому числі, в електронній)формі між SAP та Замовником. Ця Угода про обробку персональних даних застосовується до відносин Сторін з обробки Персональних даних у зв'язку з наданням послуг SAP, як зазначено у відповідній Угоді/Договорі (далі – «Послуги SAP»), до якої додається ця Угода про обробку персональних даних. Зазначені Послуги SAP можуть включати в себе:

(a) Послуги SAP з підтримки SAP відповідно до Угоди/Договору про надання прав на використання та надання послуг з підтримки програмного забезпечення та/або;

(b) професійні послуги, що описані в Угоді/Договорі про надання послуг SAP, укладенbv між SAP та Замовником (далі – «Договір про надання послуг»).

1.2 Структура. Додаток 1 та Додаток 2 включаються до складу цієї Угоди про обробку персональних даних та є її невід'ємною частиною. . У них визначається предмет, характер і мета обробки, тип Персональних даних, категорії суб'єктів даних та відповідні технічні й організаційні заходи.

1.3 Загальний регламент про захист даних (GDPR). SAP та Замовник погоджуються з тим, що кожна сторона несе відповідальність за перевірку та прийняття вимог, що пред'явлені до Операторів і Обробників згідно із Загальним регламентом про захист даних 2016/679 (далі – «**Загальний регламент про захист даних» «GDPR»**), зокрема у зв'язку з його статтями 28 і 32–36 зазначеного регламенту, якщо це застосовується (та в тій мірі, у якій вони застосовні) до Персональних даних Замовника або Операторів, які обробляються згідно з Угодою про обробку персональних даних. В якості іллюстрації в Додатку 3 перераховані відповідні вимоги Загального регламенту про захист даних і відповідні розділи цієї Угоди про обробку персональних даних.

1.4 Принципи правового регулювання. За цією Угодою про обробку персональних даних SAP виступає в ролі Обробника, а Замовник та ті юридичні особи, яким він дозволяє надавати Персональні дані в системи, доступні SAP під час надання Послуг SAP, виступають в якості Операторів. Замовник виступає в якості єдиної контактної особи та одноосібно несе відповідальність за отримання будь-яких відповідних повноважень, згод і дозволів на

instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to include Personal Data and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

обробку Персональних даних відповідно до цієї Угоди про обробку персональних даних, включаючи, у відповідних випадках, отримання згоди від Операторів на залучення SAP як Обробника. У випадку, коли Замовник надає повноваження, згоди, інструкції або дозволи, вони надаються не лише від імені самого Замовника, але також від імені всіх го іншихОператорів. У тих випадках, коли SAP інформує або повідомляє Замовникаа, така інформація або повідомлення вважаються отриманими тими Операторами, яким Замовник дозволив включати Персональні дані, і Замовник несе відповідальність за передачу такої інформації та повідомлень відповідним Операторам.

2. SECURITY OF PROCESSING

2. БЕЗПЕКА ОБРОБКИ

2.1 Appropriate Technical and Organizational Measures. SAP has implemented and will apply the technical and organizational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

Appendix 2 applies only to the extent that such SAP Services are performed on or from SAP premises. In the case where SAP is performing SAP Services on the Customer's premises and SAP is given access to Customer's systems and data, SAP shall comply with Customer's reasonable administrative, technical, and physical conditions to protect such data and guard against unauthorized access. In connection with any access to Customer's system and data, Customer shall be responsible for providing SAP personnel with user authorizations and passwords to access its systems and revoking such authorizations and terminating such access, as Customer deems appropriate from time to time. Customer shall not grant SAP access to Licensee systems or personal information (of Customer or any third party) unless such access is essential for the performance of SAP Services. Customer shall not store any Personal Data in non-production environments.

2.1 Належні технічні й організаційні заходи. Компанія SAP впровадила й застосовуватиме технічні та організаційні заходи, наведені в Додатку 2. Замовник перевірив такі заходи й погоджується, що вони є належними з урахуванням сучасного рівня розвитку науки та техніки, витрат на впровадження, характеру, обсягу, контексту та цілей обробки Персональних даних.

Додаток 2 застосовується лише у тих випадках, коли такі Послуги SAP надаються на території SAP або з території SAP. У тому випадку, коли SAP надає Послуги SAP на території Замовниката Клієнт надає SAP доступ до своїх систем і даних, SAP зобов'язується дотримуватися всіх розумних адміністративних, технічних і фізичних умов Замовника, щоб захистити такі дані й убезпечити їх від несанкціонованого доступу. У зв'язку з цим до обов'язків Замовника входить надання співробітникам SAP повноважень і паролів користувачів, котрі необхідні для доступу до своїх систем, а також відгук таких повноважень і припинення такого доступу в періоди , коли Замовник вважатиме це за потрібне. Замовник не надає компанії SAP право доступу до систем Ліцензіата та особистих відомостей (Замовника або будь-якої третьої особи), якщо такий доступ не є необхідним для надання Послуг SAP. Замовник не повинен зберігати жодних Персональних даних у непродуктивному середовищі.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base receiving the same SAP Service. SAP may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

2.2 Зміни. SAP застосовує технічні й організаційні заходи, викладені в Додатку 2, до всієї бази клієнтів SAP, що отримують таку Послугу SAP. SAP може в будь-який час без попереднього повідомлення змінити заходи, викладені в Додатку 2, якщо вони забезпечують щонайменше такий самий рівень захисту. Окремі заходи можуть бути замінені новими заходами, які слугують такій самій меті, не зменшуючи рівня захисту Персональних даних.

3. SAP OBLIGATIONS

3. ЗОБОВ'ЯЗАННЯ SAP

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented

3.1 Інструкції від Замовника. SAP оброблятиме Персональні дані лише відповідно до

instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and Customer may provide further instructions during the performance of the SAP Service. SAP will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the performance of the SAP Service. If any of the before-mentioned exceptions apply, or SAP otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SAP will immediately notify Customer (email permitted).

документально оформлених інструкцій від Замовника. Такою документально підтвердженою початковою інструкцією вважається Угода (зокрема ця Угода про обробку персональних даних). Замовник може надавати додаткові інструкції під час надання Послуги SAP. SAP докладе всіх розумних зусиль, щоб дотримуватися будь-яких інших інструкцій Замовника, якщо вони вимагаються Законом про захист даних, технічно припустимі та не вимагають змін у наданні Послуги SAP. Якщо застосовується будь-який із вищенаведених винятків або компанія SAP не може дотримуватись інструкції з іншої причини чи вважає, що інструкція порушує Закон про захист персональних даних, вона негайно сповістить про це Замовника (дозволено електронною поштою).

3.2 **Processing on Legal Requirement.** SAP may also process Personal Data where required to do so by applicable law. In such a case, SAP shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.2 **Обробка, що базується на вимогу законодавства.** SAP може також обробляти Персональні дані, якщо це вимагається, відповідно до чинного законодавства. У такому випадку компанія SAP повинна інформувати Замовника про таку законну вимогу перед обробкою, якщо відповідний закон не забороняє таке інформування з важливих причин, пов'язаних із суспільним інтересом.

3.3 **Personnel.** To process Personal Data, SAP and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. SAP and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

3.3 **Персонал.** Для обробки Персональних даних компанія SAP та її Субпідрядники з обробки даних мають дозволяти доступ тільки вповноваженому персоналу, який зобов'язаний зберігати конфіденційність даних. Компанія SAP та її Субпідрядники з обробки даних регулярно навчатимуть персонал, що має доступ до Персональних даних, застосуванню відповідних заходів із гарантування безпеки та захисту даних.

3.4 **Cooperation.** At Customer's request, SAP will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SAP's processing of Personal Data or any Personal Data Breach. SAP shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SAP will correct or remove any Personal Data in SAP´s possession (if any), or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.4 **Співпраця.** За запитом Замовника SAP надасть Замовнику або будь-якому Оператору сприяння в обробці запитів зі сторони Суб'єктів данних та контролюючих органів щодо обробки Персональних даних компанією SAP або будь-яких Порушень конфіденційності персональних даних. Компанія SAP зобов'язується якомога швидше повідомляти Замовника про будь-який запит, отриманий нею від Суб'єкта даних у зв'язку з обробкою Персональних даних, але не повинна відповідати на такий запит без подальших інструкцій Замовника,якщо це прийнятно. Компанія SAP буде виправляти або видаляти будь-які наявні в неї Персональні дані (за їх наявності) або обмежувати їх обробку відповідно до інструкцій Замовника та Закону про захист Персональних даних.

3.5 **Personal Data Breach Notification.** SAP will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SAP may provide such information in phases as it becomes

3.5 **Повідомлення про Порушення конфіденційності персональних даних.** Компанія SAP без зайвої затримки повідомлятиме Замовникаа про будь-які доведені до її відома Порушення конфіденційності персональних даних і (у межах розумного) надасть наявну в неї інформацію, щоб допомогти Замовнику виконати свої зобов'язання щодо повідомлення про

available. Such notification shall not be interpreted or construed as an admission of fault or liability by SAP.

Порушення конфіденційності персональних даних відповідно до Закону про захист персональних даних. SAP може надавати таку інформацію поступово, коли вона стає доступною. Таке повідомлення не може інтерпретуватись або тлумачитися як визнання помилки або відповідальності зі сторони SAP.

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SAP will provide such documents as are generally available for the SAP Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

3.6 Оцінка впливу на захист персональних даних. Якщо відповідно до Закону про захист персональних даних Замовник (або його Оператори) зобов'язаний здійснювати оцінку впливу на захист персональних даних або проводити попередню консультацію з регуляторним органом, компанія SAP на вимогу Замовника надасть відповідні документи, що зазвичай доступні для Послуги SAP (наприклад, цю Угода про обробку персональних даних, Угоду, аудиторські звіти чи сертифікати). Будь-яка додаткова допомога має взаємно узгоджуватися Сторонами.

4. DATA DELETION

Customer hereby instructs SAP to delete the Personal Data remaining with SAP (if any) within a reasonable time period in line with Data Protection Law (not to exceed six months) once Personal Data is no longer required for execution of the Agreement, unless applicable law requires retention.

4. ВИДАЛЕННЯ ДАНИХ

Цим Замовник поручає SAP видаляти наявні в неї залишкові Персональні дані (якщо вони є) протягом розумного періоду часу відповідно до Закону про захист персональних даних (не пізніше ніж через шість місяців) після того, як Персональні дані стануть непотрібними для виконання Угоди, за винятком випадків, коли вони мають зберігатися довше відповідно до чинного законодавства.

5. CERTIFICATIONS AND AUDITS

5.1 Customer Audit. Customer or its independent third party auditor reasonably acceptable to SAP (which shall not include any third party auditors who are either a competitor of SAP or not suitably qualified or independent) may audit SAP's service and support delivery centers and IT security practices relevant to Personal Data processed by SAP only if:

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures through providing a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate). Certifications are available under: https://www.sap.com/corporate/en/company/quality.html#certificates or upon request if the certification is not available online; or

(b) A Personal Data Breach has occurred; or

(c) An audit is formally requested by Customer's data protection authority; or

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any

5. СЕРТИФІКАТИ ТА АУДИТИ

5.1 Аудит Замовника. Замовник або його сторонній аудитор, який обґрунтовано задовольняє компанію SAP (жоден сторонній аудитор не може бути конкурентом SAP, не мати належної кваліфікації або не відповідати вимогам до незалежності), може проводити аудит Послуги й центрів надання підтримки SAP, а також перевіряти методи забезпечення інформаційної безпеки, що застосовуються до Персональних даних, які обробляються SAP, лише якщо:

(a) компанія SAP не надала достатніх доказів їх відповідності вимогам до технічних і організаційних заходів шляхом отримання сертифіката відповідності стандарту ISO 27001 або іншим стандартам (в обсязі, визначеному в сертифікаті); сертифікати доступні за адресою https://www.sap.com/corporate/en/company/quality.html#certificates або за запитом, якщо сертифікація через Інтернет недоступна;

(b) мало місце Порушення конфіденційності персональних даних;

(c) орган із захисту персональних даних на стороні Замовника надіслав офіційний запит на проведення аудиту;

(d) обов'язковий Закон про захист персональних даних надає Замовнику безпосереднє право на проведення аудиту та передбачає, що

twelve month period unless mandatory Data Protection Law requires more frequent audits.

Замовник має проводити аудиторську перевірку лише один раз протягом будь-якого дванадцятимісячного періоду, крім випадків, коли такий обов'язковий Закон про захист даних вимагає частішого проведення аудиту.

5.2 **Other Controller Audit.** Any other Controller may audit SAP's control environment and security practices relevant to Personal Data processed by SAP in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SAP on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.2 **Аудит іншим Оператором.** Будь-який інший Оператор може перевіряти середовище контролю та методи захисту SAP, що застосовуються для Персональних даних, які обробляє SAP, відповідно до розділу 5.1, лише якщо до цього іншого Оператора виконуються умови, викладені в розділі 5.1. Згідно з розділом 5.1 такий аудит має здійснюватися через Замовника та ним самим, крім випадків, коли цей інший Оператор має проводити його самостійно відповідно до Закону про захист персональних даних. Якщо проведення аудиту вимагають кілька Операторів , чиї Персональні дані обробляє компанія SAP на підставі Угоди, Замовник має зробити все можливе, щоб об'єднати такі аудити й уникнути їх багаторазового проведення.

5.3 **Scope of Audit.** Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency, time frame and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited to remote audits where possible. If an on-site audit is mandatory, it shall not exceed one business day. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to SAP.

5.3 **Об'єм аудиту.** Замовник має попередньо повідомляти про будь-який аудит щонайменше за шістдесят днів до його проведення, за винятком випадків, коли обов'язковий Закон про захист персональних даних або компетентний орган із захисту персональних даних вимагає коротшого часу сповіщення. Частота, період проведення й обсяги будь-яких аудитів мають взаємно узгоджуватися сторонами, що зобов'язані діяти розумно та сумлінно. За можливості Замовник має проводити аудит лише дистанційно. Якщо перевірка має обов'язково проводитися на місці, вона має тривати не довше одного робочого дня. Там, де ці обмеження не застосовуються, сторони використовуватимуть поточні сертифікати або інші звіти про аудит, щоб уникнути проведення повторюваних аудитів або зменшити їх кількість. Замовник повинен надати результати будь-якого аудиту компанії SAP.

5.4 **Cost of Audits.** Customer shall bear the costs of any audit unless such audit reveals a material breach by SAP of this DPA, then SAP shall bear its own expenses of an audit. If an audit determines that SAP has breached its obligations under the DPA, SAP will promptly remedy the breach at its own cost.

5.4 **Витрати на аудит.** Замовник несе витрати на будь-який аудит, за винятком випадків, коли під час такого аудиту виявлено серйозне порушення компанією SAP цієї Угоди про обробку персональних даних, у разі чого SAP оплачує свої витрати на проведення аудиту самостійно. Якщо під час аудиту виявлено, що компанія SAP порушила свої зобов'язання за Угодою про обробку персональних даних, SAP негайно виправить порушення за власний рахунок.

6. SUBPROCESSORS

6. СУБПІДРЯДНИКИ З ОБРОБКИ ДАНИХ

6.1 **Permitted Use.** SAP is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

6.1 **Дозволене використання.** SAP надається загальний дозвіл на укладання субдоговору про обробку Персональних даних із Субпідрядником з обробки даних за умови, що:

(a) SAP or SAP SE on its behalf shall engage Subprocessors under a written (including in

(a) SAP або SAP SE від свого імені залучає Субпідрядників з обробки даних на підставі

electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SAP shall be liable for any breaches by the Subprocessor in accordance with the terms of the Agreement;

(b) SAP will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA;

(c) For SAP Support SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP (under: https://support.sap.com/en/my-support/subprocessors.html) or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the SAP Service; and

(d) For Professional Services, SAP will, upon request of the Customer, make the list available or identify such subprocessors prior to the start of the applicable SAP Services.

6.2 New Subprocessors. SAP's use of Subprocessors is at its discretion, provided that:

(a) SAP will inform Customer in advance of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor (i) for SAP Support - by posting on the SAP Support Portal, or by email, upon Customer's registration on the SAP Portal and (ii) for Professional Services – by similar posting on the SAP Support Portal, or by e-mail, or in other written form;

(b) Customer may object to such changes as set out in Section 6.3.

6.3 Objections to New Subprocessors.

(a) SAP Support: If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the SAP Support upon written notice to SAP, such notice to be provided to SAP no later than thirty days

письмового договору (зокрема, укладеного в електронній формі), який узгоджується з умовами цієї Угоди про обробку персональних даних, у зв'язку з обробкою Персональних даних таким Субпідрядником і несе відповідальність за будь-які порушення Субпідрядника з обробки даних відповідно до умов цієї Угоди;

(b) вибираючи Субпідрядника з обробки даних, SAP оцінюватиме його методи забезпечення недоторканності, безпеки та конфіденційності, щоб переконатися в його здатності забезпечити такий рівень захисту Персональних даних, який вимагає ця Угода про обробку особистих даних;

(c) У випадку Підтримки SAP компанія SAP публікує список Субпідрядників з обробки даних SAP, наявний на дату набуття чинності Угоди (за адресою https://support.sap.com/en/my-support/subprocessors.html), або надає його Замовнику на запит, зазначивши в ньому ім'я, адресу та роль кожного Субпідрядника з обробки даних, якого SAP залучає для надання Послуги SAP;

(d) у випадку Професійних послуг, перш ніж починати надання відповідних Послуг SAP, компанія SAP надасть на запит Замовника список Субпідрядників з обробки даних або зазначить їх іншим чином.

6.2 Нові Субпідрядники з обробки даних. SAP залучає Субпідрядників з обробки даних на свій розсуд за умови, що:

(a) SAP інформуватиме Замовника заздалегідь про будь-які передбачені доповнення або заміни до списку Субпідрядників з обробки даних, указуючи ім'я, адресу та роль нового Субпідрядника з обробки даних, 1) у випадку Підтримки SAP – шляхом публікації даних на Порталі SAP Support Portal або інформування електронною поштою після реєстрації Замовника на порталі; 2) у випадку Професійних послуг – також шляхом публікації даних на Порталі SAP Support Portal, інформування електронною поштою або сповіщення в іншій письмовій формі;

(b) Замовник може заперечувати проти таких змін, як зазначено в розділі 6.3.

6.3 Заперечення проти нових Субпідрядників з обробки даних.

(a) Підтримка SAP. Якщо згідно із Законом про захист Персональних даних Замовник має законну підставу, щоб заперечувати проти обробки Персональних даних новими Субпідрядниками з обробки даних, Замовник може припинити користуватися Підтримкою

from the date SAP informs the Customer of the new Subprocessor. If Customer does not provide SAP with a notice of termination within this thirty days period, Customer is deemed to have accepted the new Subprocessor. Within the thirty days period from the date of SAP informing the Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for providing SAP a notice of termination and does not affect SAP's right to use the new Subprocessor(s) after the thirty days period.

SAP, повідомивши про це SAP в письмовій формі не пізніше ніж через тридцять днів із дати, коли компанія SAP поінформувала його про нового Субпідрядника з обробки даних. Якщо Замовник не повідомить SAP про припинення протягом цього тридцятиденного періоду, то вважається, що Замовник погодився із залученням нового Субпідрядника з обробки даних. Протягом тридцятиденного періоду від дати, коли SAP поінформує Замовника про нового Субпідрядника з обробки даних, Замовник може вимагати сумлінного проведення спільної зустрічі сторін, на якій вони зможуть обговорити вирішення проблем, що спричинили заперечення. Такі обговорення не продовжують періоду, за який Замовник має повідомити SAP про припинення, і не впливають на право SAP залучати нових Субпідрядників з обробки даних після тридцятиденного періоду.

(b) Professional Services: If Customer has a legitimate reason under Data Protection Law that relates to the Subprocessors' processing of Personal Data, Customer may object to SAP's use of a Subprocessor, by notifying SAP in writing within five business days of SAP's information as per Section 6.2. If Customer objects to the use of the Subprocessor, the parties will come together in good faith to discuss a resolution. SAP may choose to: (i) not use the Subprocessor or (ii) take the corrective steps requested by Customer in its objection and use the Subprocessor. If none of these options are reasonably possible and Customer continues to object for a legitimate reason, either party may terminate the relevant services on five days' written notice. If Customer does not object within five days of receipt of the notice, Customer is deemed to have accepted the Subprocessor. If Customer's objection remains unresolved thirty days after it was raised, and SAP has not received any notice of termination, Customer is deemed to have accepted the Subprocessor.

(b) Професійні послуги. Якщо згідно із Законом про захист Персональних даних Замовник має законні підстави заперечувати проти залучення Субпідрядника з обробки даних компанією SAP для обробки Персональних даних, він може скористатися цим, сповістивши про це SAP в письмовій формі протягом п'яти робочих днів із моменту інформування компанією SAP відповідно до розділу 6.2. Якщо Замовник заперечує проти залучення Субпідрядника з обробки даних, Сторони мають добросовісно провести переговори , щоб обговорити способи вирішення цієї проблеми. SAP може на власний вибір 1) не залучати Субпідрядника з обробки даних або 2) ужити заходів для виправлення ситуації, що стала підставою для заперечення, відповідно до вимог Замовника та залучити Субпідрядника з обробки даних. Якщо жоден із цих варіантів неможливо реалізувати в межах розумного, а Замовник продовжує заперечувати на законних підставах, будь-яка сторона може припинити дію угоди про надання відповідних послуг, сповістивши про це письмово за п'ять днів. Якщо Замовник не заперечує протягом п'яти днів із моменту отримання сповіщення, вважається, що він погодився із залученням нового Субпідрядника з обробки даних. Якщо через тридцять днів після заперечення Замовником причину такого заперечення усунути не вдалося, а компанія SAP не отримала жодного повідомлення про припинення, то вважається, що Замовник погодився із залученням нового Субпідрядника з обробки даних.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 Emergency Replacement. SAP may replace a Subprocessor without advance notice where the reason for the change is outside of SAP's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SAP will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 Conditions for International Processing. SAP shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

(a) SAP and Customer enter into the Standard Contractual Clauses;

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by SAP or SAP SE and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by SAP) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when SAP has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section (c) or (d), or a notice to Customer; and/or

(c) При цьому вважається, що розірвання відповідно до цього розділу, відбувається не з вини однієї із Сторін та відбувається відповідно до умов Угоди.

6.4 Екстренна заміна. SAP може замінити Субпідрядника з обробки даних без попереднього сповіщення, якщо причина заміни не піддається розумному контролю SAP й така негайна заміна необхідна з міркувань безпеки або інших нагальних причин. У такому випадку SAP поінформує Замовника про заміну Субпідрядника з обробки даних якомога раніше після його призначення. Крім того, застосовуватимуться відповідні положення розділу 6.3.

7. МІЖНАРОДНА ОБРОБКА ДАНИХ

7.1 Умови міжнародної обробки даних. Компанія SAP вповноважена обробляти Персональні дані, зокрема із залученням Субпідрядників з обробки даних, відповідно до цієї Угоди про обробку персональних даних за межами країни перебування Замовника в межах дозволеного Законом про захист персональних даних.

7.2 Стандартні договірні умови. Якщо 1) Особисті дані Оператора з Європейської економічної зони або Швейцарії обробляються в країні за межами Європейської економічної зони або Швейцарії, а також будь-якої країни, організації чи території, визнаної Європейським Союзом безпечною країною з адекватним рівнем захисту даних відповідно до статті 45 Загального регламенту про захист даних, а також якщо 2) Персональні дані іншого Оператора обробляються на міжнародному рівні й така міжнародна обробка вимагає належних засобів відповідно до законодавства країни Оператора, забезпечити які можна шляхом підписання Стандартних договірних положень, застосовується зазначене нижче.

(a) SAP та Замовник підписують Стандартні договірні умови.

(b) Замовник підписує Стандартні договірні умови з кожним відповідним Субпідрядником з обробки даних в один із таких способів: 1) Замовник приєднується до Стандартних договірних положень, укладених компанією SAP або SAP SE та Субпідрядником з обробки даних, як незалежний власник прав і зобов'язань (далі – «Модель приєднання»); або 2) Замовник самостійно укладає Стандартні договірні умови з наданим SAP Субпідрядником з обробки даних (далі – «Модельдовіреності»). Модель довіреності застосовується, якщо та коли компанія SAP явно підтверджує, що Субпідрядник з обробки даних відповідає вимогам, включивши його до списку Субпідрядників з обробки даних, передбаченого розділом (c) або (d), або сповістивши про це Клієнта.

(c) Other Controllers who have been authorized by Customer to include Personal Data under the Agreement may also enter into Standard Contractual Clauses with SAP and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

9.1 "**Authorized Users**" means any individual to whom Customer grants access authorization in compliance with a SAP software license to use the SAP Service that is an employee, agent, contractor or representative of (i) the Customer, (ii) Customer's Affiliates, and/or (iii) Customer's and Customer's Affiliates' Business Partners (as defined under the Software License and Support Agreement).

9.2 "Controller" means the natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as Processor for another Controller, it shall in relation to

(c) Інші Оператори, яким Замовник дозволив включати Персональні дані відповідно до Угоди, також можуть підписати Стандартні договірні умови з SAP та/або відповідними Субпідрядниками з обробки даних так само, як Замовник, відповідно до розділів 7.2 (a) і (b) вище. У такому випадку Замовник підписує Стандартні договірні умови від імені інших Операторів.

7.3 Зв'язок між Стандартними договірними умовами та Угодою. Жодне положення Угоди не може тлумачитися як пріоритетніше в разі конфлікту з положенням Стандартних договірних умов. Щоб уникнути непорозумінь, слід уточнити, що в тих пунктах, де в цій Угоді про обробку персональних даних додатково визначено правила проведення аудиту та залучення Субпідрядників з обробки даних (розділи 5 і 6), такі визначення також застосовуються до Стандартних договірних умов.

7.4 Застосовне законодавство в Стандартних договірних положень. Стандартні договірні умови регулюються законодавством країни, де зареєстрований відповідний Оператор.

8. ДОКУМЕНТАЦІЯ ТА ВЕДЕННЯ ОБЛІКУ ОБРОБКИ

Кожна сторона несе відповідальність за дотримання вимог до ведення документації, зокрема щодо ведення обліку про обробку, якщо цього вимагає Закон про захист персональних даних. Кожна сторона зобов'язана в межах розумного допомагати іншій стороні в дотриманні вимог до документації, зокрема надавати іншій стороні необхідну їй інформацію на її обґрунтований запит (наприклад, за допомогою електронної системи), щоб вона мала можливість виконати будь-які свої зобов'язання щодо ведення обліку про обробку.

9. ВИЗНАЧЕННЯ

Всі терміни, написані з великої літери, але не визначені в цьому документі, застосовуються в значеннях, що встановлені в Угоді.

9.1. «Авторизовані користувачі» – це будь-якафізична особа, яка уповноважена Замовником відповідно до ліцензії на програмне забезпечення SAP для використання Послуги SAP, а саме: працівника, агента, підрядника або представника 1) Замовника, 2) його Афілійованих компаній і/або 3) Бізнес- партнерів Замовника та його Афілійованих осіб (відповідно до Договору про надання прав на використання та надання послуг з підтримки програмного забезпечення).

9.2. «Оператор» – це фізична або юридична особа, державний орган, заклад або інша організація, яка самостійно або спільно з іншими визначає цілі та засоби обробки Персональних даних. Для цілей цієї Угоди про обробку персональних даних у випадках, коли Замовник виступає в ролі Обробника для

SAP be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

іншого Оператора, у відносинах з SAP він має вважатися додатковим і незалежним Оператором із відповідними правами та обов'язками Оператора відповідно до цієї Угоди про обробку персональних даних.

9.3 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SAP on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

9.3. **«Законодавство про захист персональних даних»** – це застосовне законодавство, яке захищає основні права та свободи осіб і їхнє право на конфіденційність у зв'язку з обробкою Персональних даних відповідно до Угоди (і, тією мірою, у якій, воно стосується відносин між сторонами у зв'язку з обробкою Персональних даних компанією SAP від імені Замовника, враховує Загальний регламент про захист даних як мінімальний стандарт, незалежно від того, чи поширюється дія цього регламенту на такі Персональні дані).

9.4 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

9.4. **«Суб'єкт даних»** – це фізична особа, особу якої встановлено чи можна встановити відповідно до Закону про захист персональних даних.

9.5 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is supplied to or accessed by SAP or its Subprocessors in order to provide the SAP Service under the Agreement.

9.5. **«Персональні дані»** – це будь-яка інформація, що стосується Суб'єкта даних і захищена Законом про захист персональних даних. Для цілей Угоди про обробку персональних даних вона поширюється лише на Персональні дані, які надаються компанії SAP або її Субпідрядникам з обробки чи використовуються ними для надання Послуги SAP відповідно до Угоди.

9.6 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

9.6. **«Порушення конфіденційності персональних даних»** – це підтверджена подія такого характеру: 1) випадкове або незаконне знищення, утрата, змінення, несанкціоноване розголошення або несанкціонований доступ сторонніх осіб до Персональних даних; 2) подібний інцидент, пов'язаний з Персональними даними, у разі якого згідно із Законом про захист персональних даних Оператор зобов'язаний повідомити компетентні органи із захисту персональних даних або Суб'єктів даних.

9.7 **"Professional Services"** means implementation services, consulting services and/or services such as SAP Premium Engagement Support Services, Innovative Business Solutions Development Services, Innovative Business Solutions Development Support Services.

9.7. **«Професійні послуги»** – це послуги з впровадження, консультаційні послуги та/або такі послуги, як послуги підтримки SAP Premium Engagement, послуги розробки Innovative Business Solutions, послуги підтримки Innovative Business Solutions.

9.8 **"Processor"** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, be it directly as Processor of a Controller or indirectly as Subprocessor of a Processor which processes Personal Data on behalf of the Controller.

9.8. **«Обробник»** – це фізична або юридична особа, державний орган, заклад чи інша організація , яка обробляє Персональні дані від імені Оператора, виконуючи безпосередньо роль Обробника Оператора або опосередковано роль Субпідрядника з обробки даних Обробника, який обробляє Персональні дані від імені Замовника.

9.9 **"Standard Contractual Clauses"** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The

9.9. **«Стандартні договірні умови»**, що іноді також називаються «Типовими умовами ЄС», – це документ «Стандартні договірні умови (Обробники)» або будь-яка наступна їхня версія, опублікована Європейською комісією (що

Standard Contractual Clauses current as of the effective date of the Agreement are attached hereto as Appendix 4.

9.10 "Subprocessor" means SAP Affiliates, SAP SE, SAP SE Affiliates and third parties engaged by SAP , SAP SE or SAP SE's Affiliates in connection with the SAP Service and which processes Personal Data in accordance with this DPA.

застосовуватиметься автоматично). Стандартні договірні умови, дійсні на дату набуття чинності Угоди, наведені в Додатку 4.

9.10. «Субпідрядник з обробки даних» – це Афілійовані особи SAP, SAP SE, Афілійовані особи SAP SE та треті сторони, залучені компанією SAP, SAP SE або Афілійованими особами SAP SE у зв'язку з Послугами SAP, що обробляють Персональні дані відповідно до цієї Угоди про обробку персональних даних.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer who concluded a Software License and Support Agreement and/or Services Agreement with SAP under which it benefits from SAP Service as described under the relevant Agreement. The Data Exporter allows other Controllers to also use the SAP Service, these other Controllers are also Data Exporters.

Data Importer

SAP and its Subprocessors provide the SAP Service as defined under the relevant Agreement concluded by the Data Exporter that includes the following SAP Service:

- Under the Software License and Support Agreement: SAP and/or its Subprocessors provide support when a Customer submits a support ticket because the Software is not available or not working as expected. They answer phone calls and perform basic troubleshooting, and handles support tickets in a tracking system
- under the applicable Services Agreement for Professional Services: SAP and/or its Subprocessors provide Services subject to the Order Form Services and the applicable Scope Document.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, Business Partners or other individuals having Personal Data transmitted to, made available or accessed by the Data Importer.

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data and/or data fields which could be transferred per SAP Service as stated in the relevant Agreement. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, plus any application-specific data transferred by Authorized Users and may include financial data such as bank account data, credit or debit card data.

Додаток 1 до Угоди про обробку персональних даних і, якщо застосовується, Стандартних договірних умов

Експортер даних

Експортер даних – цеЗамовник, який уклав з SAP Договір про надання прав на використання та надання послуг з підтримки програмного забезпечення та/або Договір про надання послуг, згідно з яким він користується Послугами SAP як описано у відповідному Договорі. Експортер даних дозволяє іншим Операторам також використовувати Послуги SAP, а ці інші Оператори також вважаються Експортерами даних.

Імпортер даних

Компанія SAP та її Субпідрядники з обробки даних надають Послуги SAP, як визначено у відповідній Угоді, укладеній Експортером даних, зокрема зазначені нижче.

- За Договором про надання прав на використання та надання послуг з підтримки програмного забезпечення. Компанія SAP та/або її Субпідрядники з обробки даних надають підтримку, коли Замовник надсилає звернення до служби підтримки у зв'язку з тим, що Програмне забезпечення недоступне або не працює належним чином. Вони відповідають на телефонні дзвінки, виконують базові процедури з виправлення помилок і обробляють звернення до служби підтримки в системі відстеження
- За відповідною Угодою про надання Професійних послуг Компанія SAP та/або її Субпідрядники з обробки даних надають Послуги, що регулюються Договором і відповідним Регламентом надання послуг.

Суб'єкти даних

Якщо Експортер даних не вказав інше, передані Персональні дані стосуються таких категорій Суб'єктів даних: працівників, підрядників, Бізнес-партнерів або інших фізичних осіб, яким Імпортер даних передав чи надав Персональні дані або доступ до них.

Категорії даних

Під переданими Персональними даними слід розуміти зазначені нижче категорії даних.

Замовник визначає категорії даних і/або поля даних, які можуть передаватися в рамках надання Послуг SAP згідно з відповідною Угодою. Під переданими Персональними даними зазвичай слід розуміти такі категорії даних: ім'я, номери телефонів, адреса електронної пошти, часовий пояс, дані адреси, дані для доступу до системи, її використання та авторизації в ній, назва компанії, дані договорів, дані рахунків-фактур, а також будь-які специфічні для застосунку дані, передані Авторизованими користувачами. Вони, зокрема, можуть містити фінансові дані, як-от дані про банківські рахунки та кредитні або дебетові картки.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form), if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the basic processing activities as set out in the Agreement which may include:

- use of Personal Data to provide the SAP Service
- storage of Personal Data
- computer processing of Personal Data for data transmission
- execution of instructions of Customer in accordance with the Agreement.

Спеціальні категорії даних, якщо застосовується

Під переданими Персональними даними зазвичай слід розуміти зазначені нижче особливі категорії даних, визначені в Угоді за її наявності (зокрема, у Договорі).

Операції обробки або цілі

З переданими Персональними даними виконуються базові операції обробки відповідно до Угоди, зокрема:

- використання Персональних даних для надання Послуг SAP;
- зберігання Особистих даних;
- комп'ютерна обробка Персональних даних для передачі даних;
- виконання інструкцій Замовника відповідно до Угоди.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organizational Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SAP's current technical and organizational measures. SAP may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- SAP protects its assets and facilities using the appropriate means based on the SAP Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SAP buildings must register their names at reception and must be accompanied by authorized SAP personnel.
- SAP employees and external personnel must wear their ID cards at all SAP locations.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

Додаток 2 до Угоди про обробку персональних даних і, якщо застосовується Стандартних договірних умов – технічні й організаційні заходи

1. ТЕХНІЧНІ Й ОРГАНІЗАЦІЙНІ ЗАХОДИ

У наступних розділах нижче визначаються поточні технічні й організаційні заходи SAP. SAP може в будь-який час змінити їх без повідомлення за умови забезпечення аналогічного чи більш вищого рівня захисту. Індивідуальні заходи можуть бути замінені новими заходами, що слугують такій самій меті, не зменшуючи рівня захисту Персональних даних.

1.1 Контроль фізичного доступу. Неавторизовані особи не мають змоги отримувати фізичний доступ до приміщень, будівель або кабінетів, де розташовані системи обробки даних, які обробляють і/або використовують Персональні дані.

Заходи:

- SAP захищає свої активи та об'єкти, використовуючи відповідні засоби відповідно до Політики безпеки SAP
- Загалом будівлі захищені системами контролю доступу (наприклад, системою доступу за допомогою смарт-картки).
- Згідно з мінімальними вимогами найвіддаленіші точки входу в будівлю мають бути оснащені сертифікованою системою ключів із підтримкою сучасних засобів керування активними ключами.
- Залежно від категорії захисту, будівлі, окремі території та прилеглі приміщення можуть бути захищені додатковими засобами. Зокрема, можуть застосовуватися спеціальні профілі доступу, відеоспостереження, системи тривожної сигналізації та системи біометричного контролю доступу.
- Права доступу надаються уповноваженим особам на індивідуальній основі залежно від ужитих заходів для Контролю доступу до систем і даних (див. розділи 1.2 та 1.3 нижче). Це також стосується доступу відвідувачів. Гості та відвідувачі будівель SAP повинні зареєструватися на стійці адміністратора та мають супроводжуватися вповноваженим персоналом SAP.
- Співробітники SAP та зовнішній персонал повинні носити бейджі на всій території SAP.

Додаткові заходи для Центрів обробки даних:

- Усі Центри обробки даних дотримуються строгих процедур із безпеки, за виконанням яких слідкують охоронці, камери відеоспостереження, детектори руху, механізми контролю доступу, та інших заходів для запобігання зламу обладнання та проникнення на об'єкти Центру обробки даних. До систем та інфраструктури на об'єктах Центру обробки даних мають доступ тільки вповноважені представники. Для забезпечення належного функціонування обладнання для фізичного захисту безпеки (наприклад, датчики

руху, камери тощо) регулярно проходить технічне обслуговування та ремонт.

- SAP and all third-party Data Center providers log the names and times of authorized personnel entering SAP's private areas within the Data Centers.

- SAP та всі сторонні постачальники Центру обробки даних записують до журналу імена вповноважених працівників, які входять на приватні території SAP в Центрах обробки даних, а також час такого входу.

1.2 System Access Control. Data processing systems used to provide the SAP Service must be prevented from being used without authorization.

1.2 Контроль доступу до систем. Мають бути створені такі умови, за яких системами обробки даних, що використовуються для надання Послуги SAP, неможливо скористатися без дозволу.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the SAP Security Policy

- All personnel access SAP's systems with a unique identifier (user ID).

- SAP has procedures in place to so that requested authorization changes are implemented only in accordance with the SAP Security Policy (for example, no rights are granted without authorization). In case personnel leaves the company, their access rights are revoked.

- SAP has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

- The company network is protected from the public network by firewalls.

- SAP uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.

- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SAP's corporate network and critical infrastructure is protected by strong authentication.

Заходи:

- Для надання доступу до систем, що обробляють конфіденційні дані, зокрема тих, які застосовуються для зберігання та обробки Персональних даних, використовується кілька рівнів повноважень. Для керування повноваженнями застосовуються визначені процеси, передбачені Політикою безпеки SAP.

- Увесь персонал отримує доступ до систем SAP за унікальним ідентифікатором (ІД користувача).

- SAP має процедури, за якими запити на змінення повноважень виконуються лише відповідно до Політики безпеки SAP (наприклад, права не надаються без повноважень). У випадку, якщо працівник звільняється з компанії, його права доступу відкликаються.

- Компанія SAP запровадила політику паролів, яка забороняє спільне використання паролів, регулює правила реагування на розголошення пароля, а також вимагає регулярної зміни паролів і змінення усталених паролів. Для автентифікації присвоюються персоналізовані ідентифікатори користувача. Усі паролі повинні відповідати визначеним мінімальним вимогам і зберігатись у зашифрованому вигляді. У випадку паролів користувача в домені система вимагає змінювати пароль кожні шість місяців відповідно до вимог до складних паролів. Кожен комп'ютер має зберігач екрана, захищений паролем.

- Мережа компаній захищена від загальнодоступної мережі за допомогою брандмауерів.

- У точках доступу до мережі компанії (для облікових записів електронної пошти), а також на всіх файлових серверах і всіх робочих станціях SAP використовує найновіше антивірусне програмне забезпечення.

- Для регулярного та періодичного розгортання відповідних оновлень безпеки запроваджена система керування програмними вставками. Повний віддалений доступ до корпоративної мережі та критично важливої інфраструктури SAP захищений за допомогою системи строгої автентифікації.

1.3 Data Access Control. Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal

1.3 Контроль доступу до даних. Особи, які мають право використовувати системи обробки даних, отримують доступ лише до тих Персональних

Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

даних, на використання яких вони мають право. Вони не мають право без дозволу читати, копіювати, змінювати або видаляти Особисті дані під час обробки, використання та зберігання.

Measures:

Заходи:

- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- У рамках Політики безпеки SAP особисті дані вимагають щонайменше такого ж рівня захисту, як і «конфіденційна» інформація, відповідно до стандарту класифікації інформації SAP.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. SAP uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SAP Security Policy.
- Доступ до Персональних даних надається за принципом необхідності. Персонал Замовника має доступ до інформації, яка потрібна для виконання його обов'язків. Компанія SAP використовує концепції повноважень, які являють собою документи з описом процесів надання прав і призначення ролей для кожного облікового запису (ідентифікатор користувача). Усі дані клієнта захищені відповідно до Політики безпеки SAP.
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SAP conducts internal and external security checks and penetration tests on its IT systems.
- Усі продуктивні сервери працюють у Центрах обробки даних або в захищених серверних. Заходи безпеки, що використовуються для захисту застосунків, які обробляють Персональні дані, регулярно перевіряються. З цією метою SAP проводить внутрішні та зовнішні перевірки безпеки та тести на проникнення у своїх інформаційних системах.
- SAP does not allow the installation of software that has not been approved by SAP.
- SAP не дозволяє інсталювати програмне забезпечення, не схвалене SAP.
- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
- Стандарт безпеки SAP регулює видалення та знищення даних і їхніх носіїв після того, як вони стають непотрібними.

1.4 Data Transmission Control. Except as necessary for the provision of the SAP Services in accordance with the relevant Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at SAP to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

1.4 Контроль передачі даних. За винятком тих випадків, коли це необхідно для надання Послуг SAP згідно з відповідною Угодою, під час передавання заборонено без дозволу читати, копіювати, змінювати чи видаляти Персональні дані. У випадку фізичного переміщення носіїв даних в SAP застосовуються відповідні заходи для забезпечення узгоджених рівнів обслуговування (наприклад, шифрування та вкриті свинцем контейнери).

Measures:

Заходи:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.
- Під час передачі через внутрішні мережі SAP Персональні дані захищаються відповідно до Політики безпеки SAP.
- When data is transferred between SAP and its customers, the protection measures required for data transfer are hereby mutually agreed upon between SAP and its customer and included as a part of the Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SAP-controlled systems (e.g. data being transmitted outside the firewall of the SAP Data Center).
- Коли дані передаються між компанією SAP та її клієнтами, вони узгоджують між собою заходи захисту, необхідні для такого передавання. Перелік узгоджених заходів занесено до складу Угоди. Це стосується як фізичного перенесення даних, так і передавання їх через мережу. У будь-якому випадку Замовник бере на себе відповідальність за передавання будь-яких даних, коли він перебуває за межами систем управління SAP (наприклад,

передавання даних за межами брандмауера Центру обробки даних SAP).

1.5 Data Input Control. It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SAP data processing systems.

1.5 Контроль введення даних. У системах можна перевірити дані за минулий період і визначити, де та ким були введені, змінені чи вилучені Персональні дані в системах обробки даних SAP.

Measures:

Заходи:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- Компанія SAP дозволяє доступ до Персональних даних лише вповноваженому персоналу, якщо це потрібно для виконання обов'язків.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the SAP Service to the extent technically possible.
- Компанія SAP впровадила систему реєстрації в журналі для введення, змінення та видалення або блокування Персональних даних нею самою або її Субпідрядниками з обробки даних у рамках надання Послуги SAP (тією мірою, у якій це технічно можливо).

1.6 Job Control. Job Control is required to ensure that personal data processed on behalf of others are processed strictly in compliance with the Customer's instructions

1.6 Контроль завдань. Контроль завдань вимогається для того, щоб гарантувати, що обробка Пероснальних даних, що обробляються від імені інших осіб, здійснюється суворо відповідно до інструкцій Замвоника.

Measures:

Заходи:

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
- Компанія SAP використовує засоби управління та обробки, щоб стежити за відповідністю договорів, укладених між компанією SAP та її Замовниками, Субпідрядниками з обробки даних або іншими постачальниками послуг.
- As part of the SAP Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SAP Information Classification standard.
- У рамках Політики безпеки SAP особисті дані вимагають щонайменше такого ж рівня захисту, як і «конфіденційна» інформація відповідно до стандарту класифікації інформації SAP.
- All SAP employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SAP customers and partners.
- Усі співробітники SAP, Субпідрядники з обробки даних, що уклали договір з SAP, або інші постачальники послуг зобов'язані дотримуватися договірних зобов'язань щодо забезпечення конфіденційності всієї таємної інформації, зокрема комерційних таємниць клієнтів і партнерів SAP.

For Support Services, SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer system without the knowledge and consent of the customer. For Support Services, SAP provides a specially designated, secure support ticket facility in which SAP provides a special access-controlled and monitored security area for transferring access data and passwords. SAP customers have control over their remote support connections at all times. SAP employees cannot access a customer on premise system without the knowledge and active participation of the customer.

Клієнти SAP завжди контролюють свої віддалені підключення до служб підтримки. Співробітники SAP не можуть отримати доступ до системи клієнтів без їхнього відома та згоди. Для служб підтримки компанія SAP надає окрему спеціалізовану безпечну платформу обробки запитів підтримки, на якій вона створює окрему зону безпеки з контролем доступу та можливістю відстеження, що використовується для передавання даних доступу та паролів. Клієнти SAP постійно контролюють свої віддалені підключення. Співробітники SAP не можуть отримати доступ до локальної системи Замовника в системі без його відома та активної участі.

1.7 Availability Control. Personal Data will be protected against accidental or unauthorized destruction or loss.

1.7 Контроль доступності. Необхідно захищати Пероснальні дані від випадкового або несанкціонованого знищення або втрати.

Measures:

Заходи:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- SAP has defined business continuity plans for business-critical processes;
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control. Personal Data collected for different purposes can be processed separately.

Measures:

- SAP uses appropriate technical controls to achieve Customer Data separation at all times.
- Customer (including its approved Controllers) will have access only to their own Data based on secure authentication and authorization.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control. Personal Data will remain intact, complete and current during processing activities.

Measures:

SAP has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

In particular, SAP uses the following to implement the control and measure sections described above. In particular:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

- Компанія SAP використовує процеси регулярного резервного копіювання, щоб забезпечити відновлення критично важливих для бізнесу систем у разі необхідності.
- SAP застосовує системи безперервного енергопостачання (наприклад, ДБЖ, акумулятори, генератори тощо), щоб гарантувати доступність джерел живлення для Центрів обробки даних.
- Компанія SAP визначила плани забезпечення безперервності бізнесу для критично важливих для бізнесу процесів.
- Вона регулярно перевіряє аварійні процеси та системи.

1.8 Контроль відокремлення даних. Персональні дані, зібрані для різних цілей, можуть оброблятись окремо.

Заходи:

- Компанія SAP постійно використовує належні технічні засоби контролю для відокремлення Даних Замовника.
- Замовник (зокрема, його затверджені Оператори) матиме доступ лише до власних Даних за умови проходження захищеної автентифікації та авторизації.
- Якщо для обробки інциденту підтримки потрібні Персональні дані Замовника , дані призначаються цьому конкретному повідомленню та використовуються лише для його обробки. Вони не застосовуються для обробки будь-яких інших повідомлень. Ці дані зберігаються в спеціальних системах підтримки.

1.9 Контроль цілісності даних. Під час обробки Персональні дані залишаються незмінними, повними та актуальними.

Заходи:

Компанія SAP впровадила багаторівневу стратегію захисту від несанкціонованих змін.

Зокрема, для реалізації положень розділів, що стосуються контролю та вимірювання, наведених вище, вона використовує:

- брандмауери;
- центр моніторингу безпеки;
- антивірусне програмне забезпечення;
- резервне копіювання та відновлення;
- перевірку на зовнішнє та внутрішнє проникнення;
- регулярні зовнішні аудити для підтвердження адекватності заходів безпеки.

Appendix 3 to the DPA

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Article of GDPR	Section of DPA	Click on link to see Section
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(2), 28(3) (d) and 28 (4)	6	SUBPROCESSORS
28 (3) sentence 1	1.1and Appendix 1, 1.2	Purpose and Aplication, Appendix 1 Structure.
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organizational Measures.
28(3) (e)	3.4	Cooperation.
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organizational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2 and Appendix 4	Standard Contractual Clauses. and Appendix 4 Standard Contractual Clauses (Processors)

Додаток 3 до Угоди про обробку особистих даних

У таблиці нижче наведені відповідні статті Загального регламенту про захист даних і відповідні умови Угоди про обробку особистих даних. Вони призначені лише для ілюстрації.

Стаття Загального регламенту про захист даних (GDPR)	Розділ Угоди про обробку особистих даних	Натисніть на посилання для перегляду розділу
28(1)	2 і Appendix 2	Security of Processing і Додаток 2 «Технічні та організаційні заходи».
28(2), 28(3) (d) і 28 (4)	6	SUBPROCESSORS
28 (3) пункт 1	1.1і Appendix 1, 1.2	Призначення та застосування, Appendix 1 Structure.
28(3) (a) і 29	3.1 і 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel.
28(3) (c) і 32	2 і Appendix 2	Security of Processing і Додаток 2 «Технічні та організаційні заходи».
28(3) (e)	3.4	Cooperation.
28(3) (f) і 32–36	2 і Appendix 2, 3.5, 3.6	Security of Processing і Appendix 2, «Технічні та організаційні заходи». Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data Deletion
28(3) (h)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) (c)	7.2 і Appendix 4	Standard Contractual Clauses. і Appendix 4 Standard Contractual Clauses (Processors)

Appendix 4 to the DPA

Standard Contractual Clauses (Processors)*

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

[…]

(in the Clauses hereinafter referred to as the '**data exporter'**)

and

[…]

(in the Clauses hereinafter referred to as the **'data importer'**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for

Додаток 4 до Угоди про обробку Персональних даних

Стандартні договірні умови (Обробники)*

Для цілей статті 26(2) Директиви 95/46/ЕС (а після 25 травня 2018 р. – статті 44 та наступних Постанови 2016/79) для передачі Персональних даних обробникам, зареєстрованим у сторонніх країнах, які не забезпечили належний рівень захисту даних

[…]

(далі в цих Положеннях – **експортер даних**)

і

[…]

(далі в цих Положеннях – **імпортер даних**)

кожна сторона, а разом сторони,

УЗГОДИЛИ викладені далі договірні положення (далі – Положення), щоб забезпечити адекватні засоби захисту конфіденційності та основних прав і свобод фізичних осіб у зв'язку з передачею Особистих даних, зазначених у Додатку 1, експортером імпортеру.

Пункт 1

Визначення

Для цілей пунктів:

(а) терміни «персональні дані», «спеціальні категорії даних», «обробляти або обробка», «оператор персональних даних», «обробник», «суб'єкт даних» і «контролюючий орган» мають таке ж значення, як у Директиві 95/46/ЕС Європейського парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних і вільне переміщення таких даних від 24 жовтня 1995 року(1);

(б) термін «експортер даних» означає оператора, який передає персональні дані;

(в) термін «імпортер даних» означає обробника, який погоджується отримувати від експортера персональні дані, призначені для обробки від його імені після передачі відповідно до його інструкцій і умов цих Положень, і на якого не поширюється вимога забезпечення адекватного захисту в сторонній країні в розумінні Статті 25(1) Директиви 95/46/ЕС;

(г) термін «субпідрядник з обробки даних» означає будь-якого обробника, залученого імпортером даних або будь-яким іншим субпідрядником з обробки даних імпортера даних, який погоджується одержувати від імпортера даних або від будь-якого

* Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)
Відповідно до Рішення Комісії від 5 лютого 2010 року (2010/87/EU)

processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7,Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party

іншого субпідрядника імпортера даних персональні дані, призначені виключно для операцій обробки, які повинні здійснюватися від імені експортера даних після передачі відповідно до його інструкцій, умов цих Положень і умов письмового субдоговору;

(д) термін «застосовний закон про захист даних» означає законодавство, яке захищає основні права й свободи фізичних осіб і, зокрема, їхнє право на конфіденційність у зв'язку з обробкою персональних даних, що застосовується до контролера даних у країні – члені ЄС, де перебуває зареєстрований експортер даних;

(е) «технічні й організаційні заходи безпеки» – це заходи, спрямовані на захист особистих даних від випадкового або незаконного знищення чи випадкової втрати, зміни, несанкціонованого розголошення або доступу, зокрема, коли обробка передбачає передачу даних через мережу, а також від усіх інших незаконних форм обробки.

Пункт 2

Відомості про передачу даних

Докладні відомості про передачу та, зокрема, спеціальні категорії персональних даних, якщо такі застосовуються, зазначені в Додатку 1, який є невід'ємною частиною цього Пункту.

Пункт 3

Положення щодо сторонніх бенефіціарів

1. Суб'єкт даних може вимагати застосування до експортера даних цього Пункту, Пункт 4(б)–(з), Пункту 5(а)–(д) і (є)–(и), Пункту 6(1) і (2), Пункт 7, Пункту 8(2) і Пунктів 9–12 як до стороннього бенефіціара.

2. Суб'єкт даних може вимагати застосування до імпортера даних цього Пункту, Пункту 5(а)–(д) і (є), Пункту 6, Пункту 7, Пункту 8(2) і Пунктів 9–12 у випадках, коли експортер даних фактично зник або припинив існування де-юре, крім випадків, коли всі юридичні зобов'язання експортера даних за договором або в силу закону взяв на себе його наступник, унаслідок чого він прийняв на себе права й обов'язки експортера даних. У такому випадку суб'єкт даних може вимагати застосування таких положень до цього наступника.

3. Суб'єкт даних може вимагати застосування до субпідрядника з обробки даних цього Пункту,Пункту5(а)–(д) і (є), Пункту 6, Пункту 7, Пункту 8(2) і Пунктів 9–12 у випадках, коли експортер та імпортер даних фактично зникли, припинили існувати де-юре або стали неплатоспроможними, крім випадків, коли всі юридичні зобов'язання експортера даних за договором або в силу закону взяв на себе його наступник, унаслідок чого він прийняв на себе права й обов'язки експортера даних. У такому випадку

liability of the subprocessor shall be limited to its own processing operations under the Clauses.

суб'єкт даних може вимагати застосування таких положень до цього наступника. Така відповідальність субпідрядника як третьої сторони з обробки даних обмежується власними операціями обробки відповідно до Умов.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Сторони не заперечують проти того, щоб суб'єкта даних представляла асоціація чи інший орган, якщо суб'єкт даних чітко висловив таке бажання й це дозволено національним законодавством.

Clause 4

Obligations of the data exporter

Пункт 4

Обов'язки експортера даних

The data exporter agrees and warrants:

Експортер даних погоджується та гарантує:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(а) що обробка, зокрема саме передавання персональних даних, виконувалась і продовжує виконуватися згідно з відповідними положеннями застосовного закону про захист даних (і, у відповідних випадках, про неї повідомляється відповідним органам країни – члена ЄС, де зареєстровано експортера даних) і не порушує відповідних нормативних положень цієї країни;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(б) що він вимагав і протягом усього терміну надання послуг з обробки особистих даних вимагатиме від імпортера даних обробляти передані персональні дані лише від імені експортера даних і відповідно до застосовного закону про захист даних і Умовами;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(в) що імпортер даних надасть достатні гарантії застосування технічних і організаційних заходів безпеки, зазначених у Додатку 2 до цього договору;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(г) що після оцінки вимог застосовного закону про захист даних установлено, що заходи безпеки є прийнятними для захисту персональних даних від випадкового або незаконного знищення або випадкової втрати, зміни, несанкціонованого розголошення або доступу, зокрема, якщо обробка передбачає передачу даних через мережу, а також від усіх інших незаконних форм обробки й що ці заходи забезпечують належний рівень безпеки з урахуванням ризиків, що виникають унаслідок обробки, і характеру даних, що підлягають захисту, з огляду на сучасний рівень розвитку технологій і витрат на впровадження;

(e) that it will ensure compliance with the security measures;

(д) що він забезпечить дотримання вимог до заходів безпеки;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(е) що у випадках передачі даних спеціальних категорій суб'єкт даних був або буде поінформований заздалегідь або якомога раніше після передачі про те, що його дані можуть бути передані в сторонню країну, яка не забезпечує адекватний захист у розумінні Директиви 95/46/ЕС;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory

(є) що він пересилатиме всі сповіщення, отримані від імпортера даних або будь-якого субпідрядника з обробки даних відповідно до Пунктів 5(б) і Пунктів 8(3), до контролюючого органу із захисту

authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

даних, якщо експортер даних вирішить продовжити передачу або скасувати призупинення;

(ж) що він за запитом надаватиме суб'єктам даних копію цих Умов , за винятком Додатку 2, і стислий опис заходів безпеки, а також копію будь-якого договору про послуги обробки даних за субпідрядом, які мають бути надані відповідно до Умов , крім випадків, коли в договорі міститься комерційна інформація, у разі чого він може її видалити;

(з) що в разі обробки даних за субпідрядом операція обробки виконується субпідрядником з обробки даних відповідно до Пункту 11 із забезпеченням щонайменше такого самого рівня захисту особистих даних і прав суб'єкта даних, який має гарантувати й імпортер даних відповідно до Умов;

(и) що він забезпечить дотримання Пунктів 4(а)–(з).

Clause 5

Obligations of the data importer [(2)]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

Пункт 5

Обов'язки імпортера даних [(2)]

Імпортер даних погоджується та гарантує:

(а) що він оброблятиме особисті дані лише від імені експортера даних і відповідно до його інструкцій і Умов ; якщо він не може забезпечити дотримання цих вимог із будь-яких причин, він погоджується негайно сповістити експортера даних про неможливість виконання вимог, у разі чого експортер даних має право призупинити передачу даних і/або розірвати договір;

(б) що немає підстав вважати, що законодавство, яке до нього застосовується, перешкоджає виконанню інструкцій, отриманих від експортера даних, і його обов'язків за договором, а також що в разі зміни в цьому законодавстві, яка може мати суттєвий негативний вплив на виконання гарантій і обов'язків, передбачених цими Умовами, він негайно сповістить про цю зміну експортера даних, щойно йому про неї стане відомо, у разі чого експортер даних має право призупинити передачу даних і/або розірвати договір;

(в) що він упровадив технічні й організаційні заходи безпеки, зазначені в Додатку 2, перед обробкою переданих персональних даних;

(г) що він негайно сповістить експортера даних про:

1) будь-який обов'язковий за законом запит на розголошення персональних даних від правоохоронних органів, якщо це не заборонено на інших підставах, наприклад на підставі кримінального права, що вимагає збереження конфіденційності розслідування правоохоронними органами;

2) будь-який випадковий чи несанкціонований доступ;

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by

3) будь-який запит, отриманий безпосередньо від суб'єктів даних, без відповіді на цей запит, крім випадків, коли це дозволено на інших підставах;

(д) що він оперативно та належним чином реагує на всі запити експортера даних у зв'язку з обробкою особистих даних, що підлягають передачі, і дотримуватиметься рекомендацій контролюючого органу стосовно обробки переданих даних;

(е) що на вимогу експортера даних він надаватиме свої засоби обробки даних для перевірки передбачених Умовами операцій обробки, яка має проводитись експортером даних або інспекційним органом, що складається з незалежних членів із необхідною професійною кваліфікацією, які взяли на себе зобов'язання дотримуватися конфіденційності й (у відповідних випадках) обрані експортером даних за згодою контролюючого органу;

(є) що він надаватиме за запитом суб'єкта даних копію цих Умов або будь-якого наявного договору про обробку даних за субпідрядом, крім випадків, коли в договорі міститься комерційна інформація, у разі чого він може її видалити, за винятком Додатку 2, який замінюється стислим описом заходів безпеки в тих випадках, коли суб'єкт даних не може отримати копію від експортера даних;

(ж) що, у випадку обробки даних за субпідрядом, він попередньо повідомив експортера даних і отримав його попередню письмову згоду;

(з) що послуги обробки, які надає субпідрядник з обробки даних, надаватимуться відповідно до Пункту 11;

(и) що він негайно надішле експортеру даних копію будь-якої угоди із субпідрядником з обробки даних, яку він укладе відповідно до Умов.

Пункт 6

Відповідальність

1. Сторони погоджуються з тим, що будь-який суб'єкт даних, який постраждав у результаті будь-якого невиконання обов'язків, зазначених у Пункті 3 або в Пункті 11, будь-якою стороною або субпідрядником з обробки даних, має право отримати компенсацію від експортера даних за завданий збиток.

2. Якщо суб'єкт даних не може подати проти експортера даних позов із вимогою компенсації згідно з параграфом 1 внаслідок порушення імпортером даних або його субпідрядником з обробки даних будь-якого зі своїх зобов'язань, зазначених у Пункті 3 або Пункті 11, оскільки експортер даних фактично зник, припинив своє існування де-юре або став неплатоспроможним, імпортер даних погоджується, що суб'єкт даних може подати позов проти імпортера даних так, ніби він і був експортером даних, крім випадків, коли всі юридичні зобов'язання експортера даних за

operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an

договором або в силу закону взяв на себе його наступник, у разі чого суб'єкт даних може вимагати дотримання його прав цим наступником.

Імпортер даних не може посилатися на порушення субпідрядником з обробки даних своїх зобов'язань, щоб самому уникнути відповідальності.

3. Якщо суб'єкт даних не може подати позов проти експортера даних або імпортера даних, згаданого в параграфах 1 і 2, у зв'язку з порушенням субпідрядником з обробки даних будь-якого зі своїх зобов'язань, зазначених у Пункті 3 або в Пункті 11, оскільки експортер та імпортер даних фактично зникли, припинили своє існування де-юре або стали неплатоспроможними, субпідрядник з обробки даних погоджується, що суб'єкт даних може подавати позов проти субпідрядника з обробки даних у зв'язку з власними операціями обробки згідно з цими Пунктами так, ніби він сам був експортером чи імпортером даних, крім випадків, коли всі юридичні зобов'язання експортера даних за договором або в силу закону взяв на себе його наступник, у разі чого суб'єкт даних може вимагати дотримання його прав цим наступником. Відповідальність субпідрядника з обробки даних обмежується його власними операціями обробки відповідно до Умов.

Пункт 7

Посередництво та юрисдикція

1. Імпортер даних погоджується, що якщо суб'єкт даних вимагає від нього дотримання прав стороннього бенефіціара та/або виплати компенсації за збитки відповідно до Умов, імпортер даних прийме рішення суб'єкта даних:
   (а) передати вирішення спору шляхом урегулювання незалежною особою або (у відповідних випадках) контролюючим органом;
   (б) передати спір до судів країни – члена ЄС, де зареєстровано експортера даних.
2. Сторони погоджуються, що вибір, зроблений суб'єктом даних, не позбавляє його суттєвих чи процесуальних прав на застосування засобів захисту відповідно до інших положень національного чи міжнародного права.

Пункт 8

Співпраця з контролюючими органами

1. Експортер даних погоджується надати копію цього договору контролюючому органу, якщо він цього вимагає або якщо це необхідно зробити відповідно до чинного закону про захист даних.
2. Сторони погоджуються, що контролюючий орган має право проводити аудит імпортера даних і будь-якого субпідрядника з обробки даних у таких самих обсягах і на таких самих умовах, як у випадку аудиту

audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

експортера даних відповідно до чинного закону про захист даних.

3. Імпортер даних повинен негайно поінформувати експортера даних про наявність законодавства, що застосовується до нього або будь-якого субпідрядника з обробки даних і перешкоджає проведенню аудиту імпортера даних або будь-якого субпідрядника з обробки даних відповідно до параграфа 2. У такому випадку експортер даних має право вжити заходів, передбачених у Пункті 5(б).

Пункт 9

Застосовне законодавство

Ці Умови регулюються законодавством країни – члена ЄС, де зареєстровано експортера даних.

Пункт 10

Змінення договору

Сторони зобов'язуються не змінювати Умови. Це не заважає сторонам у разі потреби додавати положення, пов'язані з діловими питаннями, за умови, що вони не суперечать Умовам.

Пункт 11

Обробка за субпідрядом

1. Імпортер даних не має права передавати в субпідряд будь-які операції обробки, що виконуються від імені експортера даних згідно з Умовами , без попередньої письмової згоди експортера даних. Якщо імпортер даних передає в субпідряд свої зобов'язання за цими Умовами за згодою експортера даних, він робитиме це лише шляхом укладання письмової угоди із субпідрядником з обробки даних, яка накладає на субпідрядника з обробки даних ті ж зобов'язання, які накладаються й на імпортера даних відповідно до Пунктів (3). Якщо субпідрядник з обробки даних не виконує свої зобов'язання щодо захисту даних за такою письмовою угодою, імпортер даних несе перед експортером даних усю відповідальність за виконання субпідрядником з обробки даних своїх обов'язків за такою угодою.

2. Попередній письмовий договір між імпортером даних і субпідрядником з обробки даних також повинен включати положення про права стороннього бенефіціара, передбачене в Пункті 3. Це необхідно у випадках, коли суб'єкт даних не може пред'явити експортеру або імпортеру даних вимогу щодо компенсації, передбачену параграфом 1 Положення 6, оскільки вони фактично зникли, припинили своє існування де-юре або стали неплатоспроможними, і жоден правонаступник не взяв на себе всі юридичні зобов'язання експортера даних чи імпортера даних за договором чи в силу закону. Така відповідальність субпідрядника як

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

третьої сторони з обробки даних обмежується власними операціями обробки відповідно до Умов.

3. Положення договору, що стосуються аспектів захисту даних для обробки за субпідрядом, зазначені в параграфі 1, регулюються законодавством країни – члена ЄС, у якій зареєстровано експортера даних.

4. Експортер даних зобов'язаний вести список угод про обробку даних за субпідрядом, укладених згідно з Положеннями, і заносити їх до такого списку, коли про них повідомить імпортер даних відповідно до Пункту 5(и), щонайменше один раз на рік. Цей список має бути доступним контролюючому органу із захисту даних експортера даних.

Пункт 12

Зобов'язання після припинення надання послуг, що передбачають обробку персональних даних

1. Сторони погоджуються, що в разі припинення надання послуг, які передбачають обробку даних імпортер даних і субпідрядник з обробки даних за вибором експортера даних повернуть усі передані особисті дані та їхні копії експортеру даних або знищать усі персональні дані та письмово підтвердять експортеру даних, що це зроблено, за винятком випадків, коли законодавство, що діє для імпортера даних, забороняє повернення або знищення всіх переданих персональних даних або їхньої частини. У цьому випадку імпортер даних гарантує конфіденційність переданих персональних даних і не буде активно обробляти передані особисті дані в подальшому.

2. Імпортер даних і субпідрядник з обробки даних гарантують, що на вимогу експортера даних і/або контролюючого органу вони нададуть свої засоби обробки даних для перевірки заходів, зазначених у параграфі 1.

---

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(3) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

(1) Сторони можуть відтворити визначення та значення, що містяться в Директиві 95/46/ЄС, у цьому Положенні, якщо вони вважають за краще вказати їх окремо в договорі.

(2) Обов'язкові вимоги національного законодавства, що застосовуються до імпортера даних і не виходять за рамки того, що необхідно в демократичному суспільстві згідно з одним з інтересів, перелічених у Статті 13(1) Директиви 95/46/ЕС, тобто, якщо їх достатньо для захисту національної безпеки, оборони, громадської безпеки, попередження, розслідування, виявлення та переслідування у зв'язку з кримінальними злочинами або порушеннями етичних принципів для регульованих професій, важливих економічних або фінансових інтересів держави або захист суб'єкта даних чи прав та свобод інших людей, не суперечать стандартним договірним положенням. Прикладами таких обов'язкових вимог, які не виходять за межі того, що необхідно в демократичному суспільстві, можуть, зокрема, слугувати міжнародно визнані санкції, вимоги до податкової звітності та вимоги до звітування в рамках боротьби з відмиванням грошей.

(3) Ця вимога може бути виконана субпідрядником з обробки даних шляхом укладання договору між експортером та імпортером даних відповідно до цього Рішення.