PERSONAL DATA PROCESSING AGREEMENT FOR SAP CLOUD SERVICES

UMOWA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH W ZWIĄZKU Z ROZWIĄZANIAMI W CHMURZE 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 processed by SAP and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SAP, and Customer shall not store Personal Data in such environments.

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, categories of 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 use the Cloud 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, 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 using the Cloud Service. Where SAP informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

1. INFORMACJE OGÓLNE

1.1 **Cel i zakres stosowania.** Niniejszy dokument („**DPA**") został włączony do Umowy i stanowi część pisemnej (dotyczy to również formy elektronicznej) umowy między SAP i Klientem. DPA odnosi się do Danych osobowych przetwarzanych przez firmę SAP i jej Podwykonawców przetwarzania danych w związku z udostępnianiem Rozwiązania w chmurze. DPA nie odnosi się do środowisk nieprodukty wnych Rozwiązania w chmurze, jeśli takie środowiska są udostępniane przez SAP, a Klient nie przechowuje w takich środowiskach Danych osobowych.

1.2 **Struktura.** Załączniki 1 i 2 zostały włączone do dokumentu DPA i stanowią jego część. Określono w nich przedmiot, charakter i cel przetwarzania, rodzaj Danych osobowych, kategorie osób, których dotyczą dane oraz odpowiedne środki techniczne i organizacyjne.

1.3 **RODO.** SAP i Klient uzgadniają, że każda ze stron ma obowiązek zweryfikować i wdrożyć wymagania, jakie na Administratorów i Podmiotów przetwarzających dane nakłada ogólne rozporządzenie o ochronie danych 2016/679 („**RODO**"), w szczególności w odniesieniu do art. 28 i 32-36 RODO, jeżeli i w stopniu, w jakim odnoszą się do Danych osobowych Klienta/Administratorów przetwarzanych na podstawie DPA. Dla celów ilustracyjnych w Załączniku 3 wymieniono istotne wymagania RODO oraz odpowiadające im punktu w niniejszym dokumencie DPA.

1.4 **Nadzór.** SAP występuje w roli Podmiotu przetwarzającego, a Klient i podmioty, którym zezwala na korzystanie z Rozwiązania w chmurze, występują w roli Administratorów (zgodnie z DPA). Klient pełni rolę jedynego punktu kontaktowego i jest wyłącznie odpowiedzialny za uzyskanie wszelkich odpowiednich upoważnień, zgód i pozwoleń dotyczących przetwarzania Danych osobowych zgodnie z niniejszym DPA, w tym - w odpowiednich wypadkach - zatwierdzenia Administratorów na wykorzystanie SAP jako podmiotu przetwarzającego. W przypadku gdy Klient dostarczy takie upoważnienia, zgodę, instrukcje lub pozwolenia, są one dostarczane nie tylko w imieniu Klienta, lecz także w imieniu każdego innego Administratora korzystającego z Rozwiązania w chmurze. W przypadku gdy SAP przekaże Klientowi informacje lub zawiadomienie, uznaje się, że Administratorzy uprawnieni przez Klienta do korzystania z Rozwiązania w chmurze

otrzymali takie informacje lub zawiadomienie. Za przekazanie takich informacji i zawiadomień odpowiada Klient.

2. SECURITY OF PROCESSING

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 as to the Cloud Service selected by Customer in the Order Form 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.

2.2 Changes. SAP applies the technical and organizational measures set forth in Appendix 2 to SAP's entire customer base hosted out of the same Data Center and receiving the same Cloud 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. BEZPIECZEŃSTWO PRZETWARZANIA

2.1 Odpowiednie środki techniczne i organizacyjne. Firma SAP wdrożyła i będzie stosować środki techniczne i organizacyjne określone w Załączniku 2. Klient zapoznał się z tymi środkami i zgadza się, że są one odpowiednie dla Rozwiązania w chmurze wybranego przez Klienta w Formularzu zamówienia, biorąc pod uwagę zaawansowanie techniczne, koszty wdrożenia, charakter, zakres, kontekst i cele przetwarzania Danych osobowych.

2.2 Zmiany. Firma SAP stosuje środki techniczne i organizacyjne wskazane w Załączniku 2 w przypadku całej bazy klientów firmy SAP obsługiwanych przy użyciu tego samego Centrum danych i korzystających z tego samego Rozwiązania w chmurze. Firma SAP może w każdej chwili i bez powiadomienia zmienić środki, o których mowa w Załączniku 2, o ile zapewni porównywalny lub wyższy poziom bezpieczeństwa. Poszczególne środki mogą zostać zastąpione nowymi, które pełnią tę sama funkcję, bez obniżania poziomu zabezpieczeń chroniących Dane osobowe.

3. SAP OBLIGATIONS

3.1 Instructions from Customer. SAP will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. 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 Cloud 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).

3. OBOWIĄZKI FIRMY SAP

3.1 Zalecenia otrzymane od Klienta. Firma SAP będzie przetwarzać Dane osobowe wyłącznie w sposób zgodny z udokumentowanymi zaleceniami przekazanymi przez Klienta. Umowa (obejmująca niniejszy dokument DPA) stanowi takie wstępne zalecenia, a każde wykorzystanie Rozwiązania w chmurze stanowi dalsze zalecenia. Firma SAP dołoży wszelkich starań, aby przestrzegać wszelkich innych zaleceń Klienta, o ile są one wymagane na podstawie Przepisów o ochronie danych osobowych, technicznie wykonalne i nie wymagają wprowadzenia zmian w Rozwiązaniu w chmurze. Jeśli zastosowanie ma którykolwiek z wspomnianych wcześniej wyjątków lub firma SAP z innych względów nie może wypełnić określonego zalecenia bądź uważa, że narusza ono Przepisy o ochronie danych osobowych, firma SAP niezwłocznie powiadomi Klienta (dozwolonym sposobem jest e-mail).

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 **Przetwarzanie w związku z wymogiem prawnym.** Firma SAP może również przetwarzać Dane osobowe, gdy taki obowiązek nakładają na nią obowiązujące przepisy. W takim przypadku firma SAP poinformuje Klienta o takim wymogu przed rozpoczęciem przetwarzania, chyba że prawo zabrania przekazywania takiej informacji ze względu na ważny interes publiczny.

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 **Personel.** Dla celów przetwarzania Danych osobowych firma SAP i jej Podwykonawcy przetwarzania danych zapewnią dostęp do danych wyłącznie upoważnionym członkom personelu, którzy zobowiązali się do zachowania poufności. Firma SAP i jej Podwykonawcy przetwarzania danych zadbają o regularne szkolenie personelu mającego dostęp do Danych osobowych w zakresie odpowiednich środków zapewniania bezpieczeństwa i prywatności danych.

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 shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service, or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SAP will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.4 **Współpraca.** Na wniosek Klienta firma SAP będzie współpracować (w uzasadnionym zakresie) z Klientem i Administratorami w ramach obsługi wniosków (od osób, których dotyczą dane, lub od organów regulacyjnych) odnoszących się do przetwarzania przez firmę SAP Danych osobowych lub do przypadków naruszenia bezpieczeństwa danych. Firma SAP powiadomi Klienta (tak szybko, jak to możliwe) o każdym otrzymanym wniosku od osoby, której dotyczą dane, dotyczącym przetwarzania Danych osobowych i nie udzieli samodzielnie odpowiedzi na taki wniosek bez dodatkowych zaleceń Klienta (odpowiednio do przypadku). Firma SAP zapewni funkcjonalność umożliwiającą Klientowi korygowanie lub usuwanie Danych osobowych z Rozwiązania w chmurze bądź ograniczenie ich przetwarzania zgodnie z Przepisami o ochronie danych osobowych. Jeśli taka funkcjonalność nie zostanie zapewniona, firma SAP skoryguje lub usunie odpowiednie Dane osobowe zgodnie z zaleceniem Klienta i Przepisami o ochronie danych osobowych.

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

3.5 **Zawiadomienie o Naruszeniu danych osobowych.** Firma SAP bezzwłocznie powiadomi Klienta po uzyskaniu informacji o Naruszeniu danych osobowych i przekaże wszelkie posiadane informacje (w uzasadnionym zakresie) z myślą o ułatwieniu Klientowi wywiązania się ze spoczywających na nim obowiązków w zakresie zgłaszania Naruszenia danych osobowych, określonych w Przepisach o ochronie danych osobowych. Firma SAP może zapewniać takie informacje w kilku fazach, zależnie od ich dostępności. Takie zawiadomienie nie zostanie uznane za uznanie własnej winy lub przyjęcie odpowiedzialności przez firmę 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 Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

3.6 **Ocena skutków w zakresie ochrony danych.** Jeśli zgodnie z Przepisami o ochronie danych osobowych Klient (lub jego Administratorzy) są zobowiązani do przeprowadzenia oceny skutków w zakresie ochrony danych lub odbycia wcześniejszych konsultacji z przedstawicielami organów regulacyjnych, na wniosek Klienta firma SAP zapewni ogólnodostępne dokumenty dotyczące Rozwiązania w chmurze (na przykład niniejszy dokument DPA, Umowę, sprawozdania z audytu lub certyfikaty). Wszelka dodatkowa pomoc musi zostać uzgodniona przez obie strony.

4. DATA EXPORT AND DELETION

4. EKSPORT I USUWANIE DANYCH

4.1 **Export and Retrieval by Customer.** During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SAP and Customer will find a reasonable method to allow Customer access to Personal Data.

4.1 **Eksport i pobieranie przez Klienta.** W trakcie Okresu subskrypcji, Klient może w każdej chwili uzyskać dostęp do swoich Danych osobowych (zgodnie z postanowieniami Umowy). Klient może eksportować i pobierać swoje Dane osobowe w standardowym formacie. Eksport i pobieranie danych może podlegać ograniczeniom technicznym. W takim przypadku firma SAP i Klient określą odpowiednią metodę umożliwiającą Klientowi dostęp do Danych osobowych.

4.2 **Deletion.** Before the Subscription Term expires, Customer may use SAP's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SAP to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

4.2 **Usuwanie.** Przed upływem Okresu subskrypcji Klient może skorzystać z oferowanych przez firmę SAP samoobsługowych narzędzi do eksportu (w miarę ich dostępności) do wykonania eksportu Danych osobowych z Rozwiązania w chmurze (będzie on stanowił „zwrot" Danych osobowych). Po zakończeniu okres subskrypcji Klient niniejszym zaleca firmie SAP usunięcie Danych osobowych pozostałych na serwerach hostujących Rozwiązanie w chmurze w rozsądnym okresie zgodnym z Przepisami o ochronie danych (nie może on przekraczać sześciu miesięcy), chyba że obowiązujące przepisy wymagają ich zachowania.

5. CERTIFICATIONS AND AUDITS

5. CERTYFIKACJE I AUDYTY

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 control environment and security practices relevant to Personal Data processed by SAP only if:

5.1 **Audyty przeprowadzane przez Klienta.** Klient lub wyznaczony przez niego niezależny audytor zewnętrzny możliwy do zaakceptowania przez SAP (nie dotyczy to audytorów zewnętrznych, którzy są konkurentami firmy SAP, brak im koniecznych kwalifikacji lub nie są niezależni) może przeprowadzić audyt środowiska kontrolnego SAP i praktyk w zakresie bezpieczeństwa w odniesieniu do Danych osobowych przetwarzanych przez firmę SAP tylko wtedy, gdy:

(a) SAP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or SAP;

(a) Firma SAP nie dostarczyła wystarczających dowodów potwierdzających, że stosuje środki techniczne i organizacyjne zapewniające bezpieczeństwo systemów produktywnych Rozwiązania w chmurze poprzez dostarczenie: (i) certyfikatu potwierdzającego zgodność z normą ISO 27001 lub innymi standardami (ich zakres jest zdefiniowany w certyfikacie) lub (ii) ważnego dokumentu potwierdzającego zgodność ze standardem ISAE3402 i/lub ISAE3000 bądź innego raportu z atestacji SOC1-3. Na wniosek Klienta sprawozdania z audytu lub certyfikaty ISO są dostępne za pośrednictwem audytora zewnętrznego lub firmy SAP;

(b) A Personal Data Breach has occurred;

(b) Doszło do Naruszenia danych osobowych;

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

(c) Z formalnym wnioskiem o przeprowadzenie audytu wystąpił organ do spraw ochrony danych Klienta lub

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Protection Law requires more frequent audits.

(d) Przepisy o ochronie danych zapewniają Klientowi prawo do przeprowadzenia audytu; Klient może przeprowadzić audyt nie częściej niż raz na dwanaście miesięcy, chyba że w Przepisach o ochronie danych wymagana jest większa częstotliwość.

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 Audyt przeprowadzany przez innego Administratora. Każdy inny Administrator może przeprowadzić audyt środowiska kontrolnego SAP i praktyk w zakresie bezpieczeństwa Danych osobowych przetwarzanych przez firmę SAP zgodnie z punktem 5.1 tylko wtedy, gdy taki inny Administrator spełnia kryteria określone w punkcie 5.1. Taki audyt musi zostać przeprowadzony za pośrednictwem Klienta, zgodnie z punktem 5.1, chyba że zgodnie z Przepisami o ochronie danych inny Administrator musi przeprowadzić audyt samodzielnie. Jeśli przeprowadzenia audytu domaga się kilku Administratorów, których Dane osobowe są przetwarzane przez SAP na podstawie Umowy, Klient dołoży wszelkich starań, aby połączono je w ramach jednego audytu w celu uniknięcia konieczności przeprowadzania wielu audytów.

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 and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. 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 **Zakres audytu.** Klient zawiadomi firmę SAP o planowanym audycie na co najmniej sześćdziesiąt dni przed jego przeprowadzeniem, chyba że zgodnie z Przepisami o ochronie danych lub decyzją właściwego organu do spraw ochrony danych wymagany jest krótszy okres powiadomienia. Częstotliwość i zakres wszelkich audytów wymaga uzgodnienia przez obie strony działające w dobrej wierze. Audyty przeprowadzane przez Klienta nie mogą trwać dłużej niż trzy dni robocze. Niezależnie od tego rodzaju ograniczeń strony będą opierać się na aktualnych certyfikatach lub innych sprawozdaniach z audytu w celu uniknięcia lub ograniczenia konieczności wielokrotnego przeprowadzania audytu. Klient przekaże firmie SAP wyniki każdego audytu.

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 **Koszt audytów.** Koszty każdego audytu ponosi Klient, chyba że w wyniku audytu ujawnione zostanie istotne naruszenie postanowień niniejszego dokumentu DPA przez firmę SAP. W takim przypadku firma SAP pokryje własne koszty audytu. Jeśli audyt ujawni, że firma SAP naruszyła swoje obowiązki określone w dokumencie DPA, firma SAP niezwłocznie usunie naruszenie na własny koszt.

6. SUBPROCESSORS

6. PODWYKONAWCY PRZETWARZANIA DANYCH

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

6.1 **Dozwolone wykorzystanie** Firma SAP otrzymuje ogólne prawo do zlecania przetwarzania Danych osobowych Podwykonawcom, pod warunkiem że:

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

(a) Firma SAP lub SAP SE w jej imieniu zaangażuje Podwykonawców przetwarzania danych na podstawie pisemnej (dopuszczalna jest równie forma elektroniczna) umowy zgodnej z warunkami zawartymi w niniejszym dokumencie DPA, dotyczącymi przetwarzania Danych osobowych przez Podwykonawców. Firma SAP będzie odpowiadać za wszelkie naruszenia dokonane przez Podwykonawców przetwarzania danych zgodnie z warunkami niniejszej Umowy;

(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; and

(b) Firma SAP dokona oceny praktyk w zakresie bezpieczeństwa, prywatności i poufności stosowanych przez Podwykonawcę przed dokonaniem wyboru w celu ustalenia, czy jest on w stanie zapewnić poziom ochrony Danych osobowych wymagany w niniejszym dokumencie DPA; oraz

(c) SAP's list of Subprocessors in place on the effective date of the Agreement is published by SAP or SAP will make it available to Customer upon request, including the name, address and role of each Subprocessor SAP uses to provide the Cloud Service.

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

(a) SAP will inform Customer in advance (by email or by posting on the support portal available through SAP Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

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

6.3 Objections to New Subprocessors.

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SAP. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SAP's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

(b) Within the thirty day period from the date of SAP's notice to Customer informing 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 termination and do not affect SAP's right to use the new

(c) Lista Podwykonawców przetwarzania, z których usług firma SAP korzysta w dniu wejścia w życie Umowy, zostanie upubliczniona przez firmę SAP lub udostępniona Klientowi na żądanie. Lista musi zawierać nazwę (nazwisko), adres i rolę każdego z Podwykonawców przetwarzania wspierających firmę SAP w dostarczaniu Rozwiązania w chmurze.

6.2 Nowi Podwykonawcy przetwarzania danych. Firma SAP może korzystać z usług Podwykonawców przetwarzania wedle własnego uznania, pod warunkiem że:

(a) Firma SAP poinformuje Klienta z wyprzedzeniem (w emailu lub wiadomości na portalu pomocy technicznej dostępnym w ramach SAP Support) o zamiarze dodania do listy nowych Podwykonawców przetwarzania (lub zastąpienia dotychczasowego Podwykonawcy innym), podając nazwę (nazwisko), adres i rolę nowego Podwykonawcy; oraz

(b) Klient może nie wyrazić zgody na tego rodzaju zmiany zgodnie z punktem 6.3.

6.3 Zastrzeżenia wobec nowych Podwykonawców przetwarzania danych.

(a) Jeśli Klient ma uzasadnione powody (na podstawie Przepisów o ochronie danych), by nie wyrazić zgody na przetwarzanie Danych osobowych przez nowego Podwykonawcę przetwarzania danych, Klient może rozwiązać Umowę (dotyczy to wyłącznie Rozwiązania w chmurze, przy którym miałby zostać wykorzystany nowy Podwykonawca) za pisemnym powiadomieniem firmy SAP. Umowa zostanie rozwiązana w dniu wskazanym przez Klienta, nie później jednak niż trzydzieści dni od daty przekazania przez firmę SAP powiadomienia informującego Klienta o nowym Podwykonawcy. Jeśli Klient nie rozwiąże umowy w takim trzydziestodniowym okresie, uznaje się, że zaakceptował nowego Podwykonawcę.

(b) W ciągu trzydziestu dni od daty powiadomienia Klienta przez firmę SAP o zaangażowaniu nowego Podwykonawcy Klient może zażądać, aby strony spotkały się i, działając w dobrej wierze, omówiły możliwe rozwiązaniu problemu. Rozpoczęcie tego rodzaju rozmów nie wiąże się z wydłużeniem okresu, w którym Klient

Subprocessor(s) after the thirty day period.

(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

ma prawo rozwiązać umowę, i nie ma wpływu na przysługujące firmie SAP prawo do skorzystania z usług takiego nowego Podwykonawcy po upływie trzydziestodniowego okresu.

(c) Rozwiązanie umowy na podstawie niniejszego punktu 6.3 w każdym przypadku odbywa się bez winy żadnej ze stron i w sposób zgodny z warunkami Umowy.

6.4 Zastępstwo w nagłych sytuacjach. Firma SAP może zastąpić Podwykonawcę przetwarzania danych bez wcześniejszego powiadomienia, jeśli powód zmiany wynika z okoliczności, na które firma SAP nie ma wpływu i niezwłoczne zastępstwo jest wymagane ze względów bezpieczeństwa lub innych ważnych przyczyn. W takim przypadku firma SAP poinformuje Klienta o zastąpieniu Podwykonawcy przetwarzania danych niezwłocznie po jego wyznaczeniu. Zastosowanie mają odpowiednio postanowienia punktu 6.3.

7. PRZETWARZANIE W INNYM KRAJU

7.1 Warunki dotyczące przetwarzania w innych krajach. Firma SAP będzie uprawniona do przetwarzania Danych osobowych, również za pośrednictwem Podwykonawców, w sposób zgodny z niniejszym dokumentem DPA, poza krajem, w którym ma siedzibę Klient, zgodnie z Przepisami o ochronie danych.

7.2 Standardowe klauzule umowne. W przypadku gdy (i) Dane osobowe Administratora z siedzibą w EOG lub Szwajcarii są przetwarzane w kraju poza EOG, Szwajcarią oraz w kraju, organizacji lub regionie uznawanych przez Unię Europejską za bezpieczne, zapewniające odpowiedni poziom ochrony danych zgodnie z art. 45 RODO, lub gdy (ii) Dane osobowe innego Administratora są przetwarzane w innym kraju i takie przetwarzanie wymaga zastosowania odpowiednich środków, zgodnie z przepisami obowiązującymi w kraju Administratora; i tego rodzaju środki mogą zostać określone w Standardowych klauzulach umownych, wówczas:

(a) Firma SAP i Klient podpiszą umowę zawierającą takie Standardowe klauzule umowne;

(b) Klient zawrze umowę zawierająca Standardowe klauzule umowne z każdym odpowiednim Podwykonawcą przetwarzania w następujący sposób: albo (i) Klient przystąpi do umowy

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 6.1(c), or a notice to Customer; and/or

zawierającej Standardowe klauzule umowne zawartej przez firmę SAP lub SAP SE z Podwykonawcą przetwarzania jako niezależny „właściciel" obowiązków i praw („Model oparty na przystąpieniu"), albo (ii) Podwykonawca przetwarzania (reprezentowany przez SAP) zawrze z Klientem umowę zawierającą Standardowe klauzule umowne („Model oparty na pełnomocnictwie"). Model oparty na pełnomocnictwie ma zastosowanie, gdy firma SAP w sposób wyraźny potwierdziła, że Podwykonawca przetwarzania spełnia wymagane kryteria - został uwzględniony na liście Podwykonawców przetwarzania, o której mowa w punkcie 6.1(c), lub wskazany w powiadomieniu przesłanym Klientowi; i/lub

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer 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.

(c) Inni Administratorzy, których Klient upoważnił do korzystania z rozwiązań w chmurze na podstawie Umowy, mogą również zawrzeć z firmą SAP i/lub odpowiednimi Podwykonawcami przetwarzania umowę zawierającą Standardowe klauzule umowne w ten sam sposób jak Klient, zgodnie z postanowieniami powyższego punktu 7.2 (a) oraz (b). W takim przypadku Klient podpisze umowę zawierającą Standardowe klauzule umowne w imieniu innych Administratorów.

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.

7.3 Relacje między Standardowymi klauzulami umownymi i Umową. W przypadku konfliktu pomiędzy Umową a Standardowymi klauzulami umownymi Standardowe klauzule umowne mają pierwszeństwo przed Umową. Dla uniknięcia wątpliwości: określone w niniejszym dokumencie DPA postanowienia dotyczące audytu i Podwykonawców przetwarzania, zawarte w punkcie 5 oraz 6, obowiązują również w odniesieniu do Standardowych klauzul umownych.

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.

7.4 Prawo właściwe dla Standardowych klauzul umownych. Standardowe klauzule umowne będą podlegać przepisom prawa kraju, w którym odpowiedni Administrator jest zarejestrowany.

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

8. DOKUMENTACJA; REJESTRY DOTYCZĄCE PRZETWARZANIA

Każda ze stron jest odpowiedzialna za wypełnienie obowiązków w zakresie dokumentacji, w szczególności dotyczących prowadzenia rejestrów dotyczących przetwarzania, gdy jest to wymagane zgodnie z Przepisami o ochronie danych. Każda ze

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.

stron zapewni drugiej stronie konieczne wsparcie (w uzasadnionym zakresie) w spełnieniu obowiązków dotyczących dokumentacji; obejmuje to między innymi przekazywanie informacji, których potrzebuje druga strona, w sposób określony przez taką drugą stronę (np. za pomocą systemu elektronicznego), tak aby owa druga strona mogła spełnić spoczywające na niej obowiązki związane z prowadzeniem rejestrów dotyczących przetwarzania.

9. EU ACCESS

9.1 Optional Service. EU Access is an optional service that may be offered by SAP. If agreed in the Order Form for the eligible Cloud Service expressly identified there as being subject to EU Access, SAP shall provide the Cloud Service solely for production instances in accordance with this Section 9. Where EU Access is not agreed in the Order Form, this Section 9 shall not apply.

9.2 EU Access. SAP will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and SAP shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4.

9.3 Data Center Location. Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. SAP will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If SAP plans to migrate the Customer instance to a Data Center within the EEA or to Switzerland, SAP will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

9. DOSTĘP NA TERENIE UE

9.1 Usługa opcjonalna. Dostęp na terenie UE to opcjonalna usługa oferowana przez SAP. Jeśli uzgodniono to w Formularzu zamówienia dotyczącym spełniającego kryteria Rozwiązania w chmurze w sposób wyraźny wskazanego jako objętego usługą dostępu na terenie UE, firma SAP zapewni Rozwiązanie w chmurze wyłącznie dla instancji produktywnych zgodnie z postanowieniami niniejszego punktu 9. W przypadku gdy usługa dostępu na terenie UE nie została uzgodniona w Formularzu zamówienia, niniejszy punkt 9 nie ma zastosowania.

9.2 Dostęp na terenie UE. Dla celów świadczenie pomocy technicznej wymagającej dostępu do Danych osobowych w Rozwiązaniu w chmurze firma SAP będzie korzystać wyłącznie z usług europejskich Podwykonawców przetwarzania i nie będzie eksportować Danych osobowych poza EOG lub Szwajcarię, chyba że uzyska od Klienta wyraźne zezwolenie na piśmie (dopuszczalne jest również wykorzystanie poczty elektronicznej) osobno dla każdego przypadku; lub zgodnie z wyjątkami opisanymi w punkcie 9.4.

9.3 Lokalizacja Centrum danych. Po wejściu w życie Umowy Centra danych wykorzystywane do przechowywania Danych osobowych w Rozwiązaniu w chmurze będą zlokalizowane na terenie EOG lub Szwajcarii. Firma SAP nie dokona migracji instancji Klienta do Centrum danych zlokalizowanych poza EOG lub Szwajcarią bez uzyskania wcześniejszej pisemnej zgody Klienta (dopuszczalne jest również wykorzystanie poczty elektronicznej). Jeśli firma SAP będzie planować migrację instancji Klienta do Centrum danych zlokalizowanego na terenie EOG lub Szwajcarii, firma SAP powiadomi o tym Klienta na piśmie (dopuszczalne jest również wykorzystanie poczty elektronicznej) nie później niż trzydzieści dni przed planowaną migracją.

9.4 **Exclusions.** The following Personal Data is not subject to 9.2 and 9.3:

(a) Contact details of the sender of a support ticket; and

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymize that Personal Data before any transmission of the incident message to SAP.

9.4 **Wyłączenia.** Poniższe Dane osobowe nie podlegają postanowieniom punktu 9.2 oraz 9.3:

(a) Dane kontaktowe osoby przesyłającej zgłoszenie do pomocy technicznej; oraz

(b) Wszelkie inne Dane osobowe przesłane przez Klienta podczas wypełniania zgłoszenia do pomocy technicznej. Klient może podjąć decyzję o nieprzesyłaniu Danych osobowych podczas wypełniania zgłoszenia do pomocy technicznej. Jeśli dane te są niezbędne dla celów procesu zarządzania incydentami, Klient może się zdecydować na anonimizację takich Danych osobowych przed przesłaniem firmie SAP wiadomości o incydencie.

10. DEFINITIONS

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

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

10.2 **"Data Center"** means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html or notified to Customer or otherwise agreed in an Order Form.

10.3 **"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).

10. DEFINICJE

Terminy pisane wielką literą niezdefiniowane w niniejszym dokumencie są użyte w znaczeniu, jakie zostało im przypisane w Umowie.

10.1 **„Administrator"** oznacza osobę fizyczną i prawną, organ publiczny, agencję lub inny podmiot, który samodzielnie lub wraz z innymi określa cele i środki przetwarzania Danych osobowych; dla celów niniejszego dokumentu DPA w przypadku, gdy Klient występuje w roli podmiotu przetwarzającego dla innego Administratora, zostanie on uznany przez firmę SAP za dodatkowego niezależnego Administratora, któremu przypisano odpowiednie prawa i obowiązki określone w niniejszym dokumencie DPA.

10.2 **„Centrum danych"** oznacza lokalizację, w której hostowana jest instancja produktywna Rozwiązania w chmurze dla Klienta w jego regionie, zgodnie z informacjami zawartymi na stronie: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html bądź przesłanymi Klientowi lub w inny sposób określonymi w Formularzu zamówienia.

10.3 **„Przepisy o ochronie danych"** to obowiązujące przepisy zapewniające ochronę podstawowych praw i wolności osób, a także ich prawa do prywatności w odniesieniu do przetwarzania Danych osobowych na podstawie Umowy (i obejmują, w zakresie, w jakim dotyczą relacji między stronami w związku z przetwarzaniem Danych osobowych przez SAP w imieniu Klienta, RODO jako minimalny

standard, niezależnie od tego, czy Dane osobowe podlegają RODO, czy też nie).

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

10.4 **„Osoba, której dotyczą dane** oznacza zidentyfikowaną lub możliwą do zidentyfikowania osobę fizyczną.

10.5 **"EEA"** means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

10.5 **„EOG"** oznacza Europejski Obszar Gospodarczy, czyli państwa członkowskie Unii Europejskiej oraz Islandię, Liechtenstein i Norwegię.

10.6 **"European Subprocessor"** means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

10.6 **„Europejski podwykonawca przetwarzania"** oznacza Podwykonawcę zajmującego się fizycznym przetwarzaniem Danych osobowych w EOG lub Szwajcarii.

10.7 **"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 (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SAP or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

10.7 **„Dane osobowe"** oznaczają wszelkie informacje odnoszące się do Osoby, której dotyczą dane, i chronione na podstawie Przepisów o ochronie danych. Dla celów DPA obejmują one wyłącznie dane osobowe, które zostały (i) wprowadzone przez Klienta lub jego upoważnionych użytkowników do Rozwiązania w chmurze lub pozyskane w trakcie korzystania przez nich z Rozwiązania w chmurze, lub (ii) dostarczone firmie SAP lub przez nią uzyskane dla celów świadczenia pomocy technicznej na podstawie Umowy. Dane osobowe stanowią podzbiór danych Klienta (zdefiniowanych w Umowie).

10.8 **"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.

10.8 **„Naruszenie danych osobowych"** oznacza potwierdzone (1) przypadkowe lub niezgodne z prawem zniszczenie, utratę, zmianę, nieupoważnione ujawnienie lub udostępnienie Danych osobowych nieuprawnej stronie trzeciej lub (2) podobny incydent dotyczący Danych osobowych; w obu przypadkach Administrator jest zobowiązany (na podstawie Przepisów o ochronie danych) do poinformowania właściwych organów ds. ochrony danych lub Osób, których dotyczą dane.

10.9 **"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.

10.9 **„Podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora - bezpośrednio, jako podmiot przetwarzający dane Administratora, lub pośrednio, jako podwykonawca podmiotu przetwarzającego, który przetwarza dane osobowe w imieniu Administratora.

10.10 **"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).

10.10 **„Standardowe klauzule umowne"**, niekiedy nazywane również „modelowymi klauzulami UE", oznaczają (Standardowe klauzule umowne (pomioty przetwarzające)) bądź ich kolejne wersje opublikowane przez Komisję Europejską (które będą stosowane automatycznie).

10.11 "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 Cloud Service and which process Personal Data in accordance with this DPA.

10.11 „Podwykonawca przetwarzania" odnosi się do podmiotów powiązanych SAP, SAP SE, podmiotów powiązanych SAP SE i podmiotów zewnętrznych zaangażowanych przez SAP, SAP SE lub podmioty powiązane SAP SE w związku z Rozwiązaniem w chmurze i przetwarzających Dane osobowe zgodnie z niniejszym dokumentem DPA.

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

Załącznik 1 do DPA oraz (w odpowiednich wypadkach) Standardowych klauzul umownych

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorized Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Eksporter danych

Eksporter danych to Klient, który nabył subskrypcję na Rozwiązanie w chmurze umożliwiające upoważnionym użytkownikom wprowadzanie, modyfikowanie, wykorzystywanie, usuwanie lub innego rodzaju przetwarzanie Danych osobowych. W przypadku gdy Klient umożliwia innym Administratorom korzystanie z Rozwiązania w chmurze, tacy Administratorzy również są eksporterami danych.

Data Importer

SAP and its Subprocessors provide the Cloud Service that includes the following support:

Importer danych

Firma SAP i jej Podwykonawcy przetwarzania zapewniają Rozwiązanie w chmurze, dla którego świadczone są następujące usługi pomocy technicznej:

SAP SE Affiliates support the Cloud Service data centers remotely from SAP facilities in St. Leon/Rot (Germany), India and other locations where SAP employs personnel in the Operations/Cloud Delivery function. Support includes:

Podmioty powiązane SAP SE obsługują Centra danych Rozwiązania w chmurze zdalnie z obiektów SAP znajdujących się w St. Leon/Rot (Niemcy), Indiach i innych lokalizacjach, w których firma SAP zatrudnia personel zajmujący się operacjami/świadczeniem usług w chmurze. Pomoc techniczna obejmuje:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing

- Monitorowanie Rozwiązania w chmurze
- Tworzenie kopii zapasowych i odtwarzanie danych przechowywanych w Rozwiązaniu w chmurze
- Udostępnianie i rozwój poprawek i uaktualnień dla Rozwiązania w chmurze
- Monitorowanie, rozwiązywanie problemów i administrowanie infrastrukturą i bazą danych Rozwiązania w chmurze
- Monitorowanie zabezpieczeń, pomoc w wykrywaniu nieautoryzowanego dostępu w modelu sieciowym, testy penetracyjne.

SAP SE Affiliates provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. SAP answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Podmioty powiązane SAP SE oferują pomoc techniczną, gdy Klient przesyła zgłoszenie do pomocy technicznej, ponieważ Rozwiązanie w chmurze jest niedostępne lub nie działa w sposób oczekiwany u niektórych lub wszystkich upoważnionych użytkowników. Firma SAP odbiera telefony i rozwiązuje podstawowe problemy oraz obsługuje zgłoszenia do pomocy technicznej w systemie śledzenia oddzielonym od instancji produktywnej Rozwiązania w chmurze.

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 stored in the Cloud Service.

Osoby, których dotyczą dane

O ile eksporter danych nie określił inaczej, przesłane Dane osobowe odnoszą się do następujących kategorii Osób, których dotyczą dane: pracownicy, wykonawcy, partnerzy biznesowi lub inne osoby, których Dane osobowe są przechowywane w Rozwiązaniu w chmurze.

Data Categories

The transferred Personal Data transferred concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. 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 that Authorized Users enter into the Cloud Service and may include bank account data, credit or debit card data.

Kategorie danych

Przesyłane Dane osobowe obejmują następujące kategorie danych:

Klient określa kategorie danych dla danego subskrybowanego Rozwiązania w chmurze. Klient może skonfigurować pola danych podczas wdrażania rozwiązana w chmurze lub w inny sposób zależny od rozwiązania. Przesyłane dane osobowe zwykle obejmują następujące kategorie danych: nazwisko, numery telefonu, adres e-mail, strefa czasowa, dane adresowe, dane dotyczące dostępu do systemu / korzystania z niego / dane uwierzytelniania, nazwa firmy, dane dotyczące umowy, dane dotyczące faktur, a także wszelkie dane odnoszące się do aplikacji, które upoważnieni użytkownicy wprowadzają do Rozwiązania w chmurze; mogą one obejmować dane dotyczące rachunku bankowego, kart kredytowych/debetowych.

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.

Specjalne kategorie danych (w odpowiednich przypadkach)

Przesłane Dane osobowe mogą obejmować specjalne kategorie danych wskazane w Umowie (w tym w Formularzu zamówienia).

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorized Users
- storage of Personal Data in dedicated Data Centers (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data

Operacje związane z przetwarzaniem/ cele

Przesłane Dane osobowe są przetwarzane w następujący sposób:

- wykorzystanie Danych osobowych dla celów obsługi, monitorowania i udostępniania Rozwiązania w chmurze (z uwzględnieniem wsparcia operacyjnego i pomocy technicznej)
- świadczenie usług doradczych;
- komunikacja z upoważnionymi użytkownikami
- przechowywanie Danych osobowych w dedykowanych Centrach danych (architektura obejmująca wielu mandantów)
- wczytywanie poprawek lub uaktualnień do Rozwiązania w chmurze
- tworzenie kopii zapasowych Danych osobowych

- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

- komputerowe przetwarzanie Danych osobowych obejmujące ich udostępnianie, przesyłanie i uzyskiwanie dostępu
- uzyskiwanie dostępu do sieci w celu umożliwienia transferu Danych osobowych
- realizacja zaleceń Klienta zgodnie z Umową.

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

This Appendix 2 comprises two sets of technical and organizational measures ("**TOMs**"):

- **TOMs Set 1 (last updated April 2018, without change):** applies to all Cloud Services, except for the TOMs Set 2 Services defined below.
- **TOMs Set 2**: applies to the TOMs Set 2 Services only. As of May 4, 2020, "**TOMs Set 2 Services**" means the following Cloud Services: SAP Analytics Cloud, SAP SuccessFactors and SAP Cloud Platform. SAP may remove a Cloud Service from the list of TOMs Set 2 Services from time to time, in which case such Cloud Service will be subject to TOMs Set 1.

TOMs SET 1

Last Updated: April 2018

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.

Załącznik 2 do DPA oraz (w odpowiednich wypadkach) Standardowych klauzul umownych – Środki techniczne i organizacyjne

Niniejszy Załącznik 2 obejmuje dwa zestawy środków technicznych i organizacyjnych („**TOM**"):

- **TOM Zestaw 1 (ostatnia aktualizacja kwiecień 2018, bez zmiany):** dotyczy wszystkich rozwiązań w chmurze, za wyjątkiem TOM Zestaw 2 określonych poniżej.
- **TOM Zestaw 2:** dotyczy jedynie Usług TOM Zestaw 2. Od dnia 4 maja 2020, „**Usługi TOM Zestaw 2**" oznacza następujące Usługi rozwiązań w chmurze: SAP Analytics Cloud, SAP SuccessFactors oraz SAP Cloud Platform. Firma SAP może usunąć usługę rozwiązań w chmurze z listy Usług TOM Zestaw 2 od czasu do czasu, w takim przypadku taka usługa będzie podlegać TOM Zestaw 1.

TOM ZESTAW 1

Ostatnia aktualizacja: kwiecień 2018

1. ŚRODKI TECHNICZNE I ORGANIZACYJNE

W poniższych punktach zdefiniowano aktualne środki techniczne i organizacyjne firmy SAP. Firma SAP może w każdej chwili i bez powiadomienia zmienić te środki, o ile zapewni porównywalny lub wyższy poziom bezpieczeństwa. Poszczególne środki mogą zostać zastąpione nowymi, które pełnią tę sama funkcję, bez obniżania poziomu zabezpieczeń chroniących Dane osobowe.

1.1 Fizyczna kontrola dostępu Osobom nieuprawnionym uniemożliwia się uzyskanie fizycznego dostępu do obiektów, budynków lub pomieszczeń, w których znajdują się systemy przetwarzania danych, które przetwarzają oraz/lub wykorzystują Dane osobowe.

Środki:

- Firma SAP chroni swoje aktywa i obiekty, stosując odpowiednie metody oparte na polityce bezpieczeństwa SAP
- Na ogół budynki są zabezpieczane przy użyciu systemów kontroli dostępu (np. system dostępu z użyciem kart chipowych).
- Minimalnym wymogiem jest, aby pry wejściach w najbardziej zewnętrznej strefie budynku został wprowadzony certyfikowany system klucza obejmujący nowoczesne i aktywne zarządzanie kluczami.

- 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.

- W zależności od klasyfikacji zabezpieczeń budynki, poszczególne obszary i pobliskie tereny mogą być zabezpieczone przy użyciu dodatkowych środków. Obejmują one określone profile dostępu, monitoring wideo, systemy antywłamaniowe, a nawet biometryczne systemy kontroli dostępu.

- 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.

- Prawa dostępu są udzielane indywidualnie upoważnionym osobom zgodnie ze środkami kontroli dostępu do systemu i danych (zob. punkt 1.2 oraz 1.3 poniżej). Dotyczy to również dostępu dla osób odwiedzających. Goście i osoby odwiedzające budynki firmy SAP muszą wpisać swoje nazwisko do rejestru w recepcji i musi im towarzyszyć członek upoważnionego personelu firmy SAP.

- SAP employees and external personnel must wear their ID cards at all SAP locations.

- Pracownicy firmy SAP i personel zewnętrzny muszą nosić identyfikatory we wszystkich lokalizacjach firmy SAP.

Additional measures for Data Centers:

Dodatkowe środki stosowane w Centrach danych:

- 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.

- We wszystkich Centrach danych przestrzega się ścisłych procedur bezpieczeństwa realizowanych przez pracowników ochrony, za pomocą kamer monitorujących, czujników ruchu, mechanizmów kontroli dostępu oraz innych środków zabezpieczających urządzenia i obiekty Centrum danych. Dostęp do systemów i infrastruktury w obiektach Centrów danych mają wyłącznie upoważnieni przedstawiciele. Urządzenia zapewniające bezpieczeństwo fizyczne (np. czujniki ruchu, kamery itd.) są regularnie konserwowane w celu zapewnienia ich właściwego działania.

- 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.

- Firma SAP oraz wszyscy zewnętrzni dostawcy Centrów danych rejestrują nazwiska i godziny uzyskania dostępu do prywatnych obszarów SAP w Centrach danych.

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

1.2 Kontrola dostępu do systemu Systemy przetwarzania danych wykorzystywane do zapewniania Rozwiązania w chmurze muszą być zabezpieczone przed ich użyciem bez zezwolenia.

Measures:

Środki:

- 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

- W celu udzielania dostępu do systemów wrażliwych (w tym systemów, w których przechowuje się i przetwarza Dane osobowe) stosuje się wiele poziomów autoryzacji. Upoważnieniami zarządza się za pośrednictwem zdefiniowanych procesów zgodnie z polityką bezpieczeństwa SAP

- 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.

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

Measures:

- 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.

- Cały personel uzyskuje dostęp do systemów firmy SAP przy użyciu unikatowego identyfikatora (ID użytkownika).

- Firma SAP wdrożyła procedury, zgodnie z którymi wymagane zmiany uprawnień są zawsze wprowadzane zgodnie z polityką bezpieczeństwa SAP (np. uprawnienia nie są udzielane bez autoryzacji). Gdy członek personelu odchodzi z firmy, jego prawa dostępu zostają cofnięte.

- Firma SAP stosuje politykę dotyczącą haseł, która zabrania udostępniania hasła, reguluje sposób postępowania w przypadku jego ujawnienia oraz nakłada obowiązek regularnej zmiany hasła. Konieczne jest także modyfikowanie haseł domyślnych. Dla celów uwierzytelniania przypisywane są indywidualne identyfikatory użytkownika. Wszystkie hasła muszą spełniać zdefiniowane wymagania minimalne i być przechowywane w zaszyfrowanej formie. W przypadku haseł domeny system wymusza ich zmianę co sześć miesięcy zgodnie wymaganiami dotyczącymi złożoności haseł. Każdy komputer ma zabezpieczony hasłem wygaszacz ekranu.

- Sieć firmowa jest zabezpieczona zaporami przed ruchem płynącym z sieci publicznej.

- Firma SAP stosuje aktualne oprogramowanie antywirusowe w punktach dostępu do sieci firmowej (w przypadku kont poczty e-mail) oraz na wszystkich serwerach plików i stacjach roboczych.

- Zarządzanie poprawkami zabezpieczeń umożliwia regularne i okresowe wdrażanie odpowiednich aktualizacji zabezpieczeń. Pełny zdalny dostęp do sieci korporacyjnej SAP oraz krytycznej infrastruktury jest chroniony za pomocą silnego uwierzytelnienia.

1.3 Kontrola dostępu do danych Osoby uprawnione do korzystania z systemów przetwarzania danych uzyskują dostęp wyłącznie do Danych osobowych, do których mają prawo dostępu. Dane nie mogą być odczytywane, kopiowane, modyfikowane ani usuwane bez zezwolenia w trakcie przetwarzania, używania i przechowywania.

Środki:

- W ramach polityki bezpieczeństwa SAP Dane osobowe wymagają co najmniej takiego samego poziomu ochrony, jak ten stosowany w przypadku informacji poufnych zgodnie ze standardem klasyfikacji danych obowiązującym w firmie 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.

- Dostęp do Danych osobowych jest udzielany wyłącznie w zakresie wymaganym do realizacji określonych zadań. Członkowie personelu mają dostęp do informacji, które są im niezbędne do wykonywania ich obowiązków. Firma SAP wykorzystuje koncepcje uprawnień, które dokumentują procesy udzielania uprawnień oraz role przypisane do każdego konta (ID użytkownika). Wszystkie dane Klienta są chronione w sposób zgodny z polityką bezpieczeństwa 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.

- Wszystkie serwery produkcyjne są obsługiwane w Centrach danych lub zabezpieczonych serwerowniach. Środki bezpieczeństwa chroniące aplikacje przetwarzające Dane osobowe są regularnie kontrolowane. W tym celu firma SAP przeprowadza wewnętrzne i zewnętrzne kontrole bezpieczeństwa oraz testy penetracyjne swoich systemów IT.

- SAP does not allow the installation of software that has not been approved by SAP.

- Firma SAP nie zezwala na instalowanie niezatwierdzonego przez nią oprogramowania.

- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

- Standard bezpieczeństwa SAP reguluje sposób usuwania lub niszczenia danych i nośników danych, gdy nie są już wymagane.

1.4 Data Transmission Control. Except as necessary for the provision of the Cloud Services in accordance with the 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 Kontrola transmisji danych Z wyjątkiem przypadków, w których jest to konieczne do zapewnienia rozwiązań w chmurze zgodnie z Umową, podczas przesyłania Dane osobowe nie mogą być odczytywane, kopiowane, modyfikowane lub usuwane bez upoważnienia. W przypadku fizycznego transportu nośników danych w firmie SAP stosuje się odpowiednie środki zapewniające ustalony w umowie poziom usług (np. szyfrowanie i pojemnik wyłożony ołowiem).

Measures:

Środki:

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.

- Dane osobowe przesyłane w wewnętrznych sieciach SAP są chronione w sposób określony w polityce bezpieczeństwa SAP.

- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant 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).

- W przypadku przesyłania danych między firmą SAP i jej Klientami środki ochrony stosowane w odniesieniu do przesyłanych Danych osobowych są zgodne z wcześniejszymi ustaleniami zapisanymi w odpowiedniej umowie. Dotyczy to zarówno fizycznego, jak i sieciowego transferu danych. W każdym przypadku Klient przejmuje odpowiedzialność za transfer danych, które opuszczają systemy kontrolowane przez firmę SAP (np. dane są przesyłane poza zaporę Centrum danych 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.

Measures:

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- SAP has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.

1.6 Kontrola wprowadzania danych Dostępna będzie możliwość retrospektywnego zbadania i ustalenia, czy i przez kogo Dane osobowe zostały wprowadzone, zmienione lub usunięte z systemów SAP wykorzystywanych do przetwarzania danych.

Środki:

- Firma SAP umożliwia dostęp do Danych osobowych jedynie upoważnionemu personelowi na podstawie wymogów wynikających z wykonywanych obowiązków.
- Firma SAP wdrożyła system rejestracji wprowadzania, modyfikacji i usuwania lub blokowania Danych osobowych przez firmę SAP lub jej podwykonawców przetwarzania w ramach Rozwiązania w chmurze w zakresie, w jakim jest to technicznie możliwe.

1.7 Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the Agreement and related instructions of the customer.

Measures:

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
- 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.
- 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.

1.8 Kontrola zadań Dane osobowe przetwarzane na zlecenie (np. Dane osobowe przetwarzane w imieniu Klienta) są przetwarzane wyłącznie zgodnie z Umową i powiązanymi poleceniami Klienta.

Środki:

- Firma SAP wykorzystuje mechanizmy kontrolne i procesy umożliwiające monitorowanie przestrzegania umów między firmą SAP i jej klientami, podwykonawcami przetwarzania lub innymi usługodawcami.
- W ramach polityki bezpieczeństwa SAP Dane osobowe wymagają co najmniej takiego samego poziomu ochrony, jak ten stosowany w przypadku informacji poufnych zgodnie ze standardem klasyfikacji danych obowiązującym w firmie SAP.
- Wszyscy pracownicy firmy SAP i kontraktowi podwykonawcy przetwarzania danych lub inni usługodawcy są zobowiązani na mocy umowy do respektowania poufności wszystkich danych wrażliwych, w tym tajemnic handlowych klientów i partnerów firmy SAP.

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

Measures:

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.

1.7 Kontrola dostępności Dane osobowe będą chronione przed przypadkowym lub nieupoważnionym zniszczeniem bądź utratą.

Środki:

- Firma SAP stosuje procesy regularnego tworzenia kopii zapasowych umożliwiające w razie potrzeby szybkie przywrócenie systemów niezbędnych do prowadzenia działalności biznesowej.

- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.

- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.

- 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 the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.

- Customer (including its Controllers) has access only to its own data.

- 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;

- Firma SAP używa również zasilaczy awaryjnych (na przykład zasilaczy UPS, akumulatorów, generatorów itd.), aby zagwarantować ciągłość zasilania w Centrach danych.

- Firma SAP opracowała plany awaryjne dla procesów niezbędnych do prowadzenia działalności i może zaoferować strategie odtwarzania po awarii dla usług o krytycznym znaczeniu dla działalności, opisane w dokumentacji lub uwzględnione w Formularzu zamówienia dla odpowiedniego Rozwiązania w chmurze.

- Procesy i systemy awaryjne są regularnie testowane.

1.8 Kontrola rozdzielania danych Dane osobowe zebrane w różnych celach mogą być oddzielnie przetwarzane.

Środki:

- Firma SAP wykorzystuje możliwości techniczne wdrożonego oprogramowania (na przykład: architektura oparta na wielu mandantach lub osobne struktury systemów) w celu skutecznego oddzielenia Danych osobowych pochodzących od różnych klientów.

- Klient (dotyczy to również Administratorów) ma dostęp wyłącznie do własnych danych.

- Jeśli przekazanie Danych osobowych jest niezbędne do obsługi incydentu zgłoszonego przez Klienta, dane są przypisywane do konkretnej wiadomości i wykorzystywane wyłącznie do jej przetwarzania; nie są używane do innych celów. Takie dane są przechowywane w dedykowanych systemach pomocy technicznej.

1.9 Kontrola integralności danych W trakcie przetwarzania Danych osobowych zapewniona zostanie ich nienaruszalność, kompletność i aktualność.

Środki:

Firma SAP wdrożyła całościową strategię ochrony zabezpieczającą przed nieupoważnionymi zmianami.

Firma SAP wykorzystuje wiele różnych elementów w celu zapewnienia opisanych wyżej mechanizmów kontrolnych i środków bezpieczeństwa. W szczególności:

- Zapory;

- Centrum monitorowania zabezpieczeń;

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

- Oprogramowanie antywirusowe;
- Tworzenie kopii zapasowych i odzyskiwanie danych;
- Zewnętrzne i wewnętrzne testy penetracyjne;
- Regularne audyty zewnętrzne sprawdzające skuteczność środków bezpieczeństwa.

TOMs SET 2

(*applies to TOMs Set 2 Services defined above*)

Last Updated: May 4, 2020

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.

- 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,

TOM ZESTAW 2

(dotyczy Usług TOM Zestaw 2 określonych powyżej)

Ostatnia aktualizacja: 4 maja 2020

1. ŚRODKI TECHNICZNE I ORGANIZACYJNE

W poniższych punktach zdefiniowano aktualne środki techniczne i organizacyjne firmy SAP. Firma SAP może w każdej chwili i bez powiadomienia zmienić te środki, o ile zapewni porównywalny lub wyższy poziom bezpieczeństwa. Poszczególne środki mogą zostać zastąpione nowymi, które pełnią tę sama funkcję, bez obniżania poziomu zabezpieczeń chroniących Dane osobowe.

1.1 Fizyczna kontrola dostępu

- Firma SAP chroni swoje aktywa i obiekty, stosując odpowiednie metody oparte na polityce bezpieczeństwa SAP
- Na ogół budynki są zabezpieczane przy użyciu systemów kontroli dostępu (np. system dostępu z użyciem kart chipowych).
- Minimalnym wymogiem jest, aby pry wejściach w najbardziej zewnętrznej strefie budynku został wprowadzony certyfikowany system klucza obejmujący nowoczesne i aktywne zarządzanie kluczami.
- W zależności od klasyfikacji zabezpieczeń budynki, poszczególne obszary i pobliskie tereny mogą być zabezpieczone przy użyciu dodatkowych środków. Obejmują one określone profile dostępu, monitoring wideo, systemy antywłamaniowe, a nawet biometryczne systemy kontroli dostępu.
- Prawa dostępu są udzielane indywidualnie upoważnionym osobom zgodnie ze środkami kontroli dostępu do systemu i danych (zob. punkt 1.2 oraz 1.3 poniżej). Dotyczy to również dostępu dla osób odwiedzających. Goście i osoby odwiedzające budynki firmy SAP muszą wpisać swoje nazwisko do rejestru w recepcji i musi im towarzyszyć członek upoważnionego personelu firmy SAP.
- Pracownicy firmy SAP i personel zewnętrzny muszą nosić identyfikatory we wszystkich lokalizacjach firmy SAP.

Dodatkowe środki stosowane w Centrach danych:

- We wszystkich Centrach danych przestrzega się ścisłych procedur bezpieczeństwa realizowanych

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.

przez pracowników ochrony, za pomocą kamer monitorujących, czujników ruchu, mechanizmów kontroli dostępu oraz innych środków zabezpieczających urządzenia i obiekty Centrum danych. Dostęp do systemów i infrastruktury w obiektach Centrów danych mają wyłącznie upoważnieni przedstawiciele. Urządzenia zapewniające bezpieczeństwo fizyczne (np. czujniki ruchu, kamery itd.) są regularnie konserwowane w celu zapewnienia ich właściwego działania.

- 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.

- Firma SAP oraz wszyscy zewnętrzni dostawcy Centrów danych rejestrują nazwiska i godziny uzyskania dostępu do prywatnych obszarów SAP w Centrach danych.

1.2 System Access Control.

1.2 Kontrola dostępu do systemu

- 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.

- W celu udzielania dostępu do systemów wrażliwych (w tym systemów, w których przechowuje się i przetwarza Dane osobowe) stosuje się wiele poziomów autoryzacji. Upoważnieniami zarządza się za pośrednictwem zdefiniowanych procesów zgodnie z polityką bezpieczeństwa SAP.

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

- Cały personel uzyskuje dostęp do systemów firmy SAP przy użyciu unikatowego identyfikatora (ID użytkownika).

- SAP has policies designed to provide that no rights are granted without authorization and in case personnel leaves the company their access rights are revoked.

- Firma SAP stosuje politykę w celu zapewnienia, że uprawnienia nie są udzielane bez autoryzacji i gdy członek personelu odchodzi z firmy, jego prawa dostępu zostają cofnięte.

- 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.

- Firma SAP stosuje politykę dotyczącą haseł, która zabrania udostępniania hasła, reguluje sposób postępowania w przypadku jego ujawnienia oraz nakłada obowiązek regularnej zmiany hasła. Konieczne jest także modyfikowanie haseł domyślnych. Dla celów uwierzytelniania przypisywane są indywidualne identyfikatory użytkownika. Wszystkie hasła muszą spełniać zdefiniowane wymagania minimalne i być przechowywane w zaszyfrowanej formie. W przypadku haseł domeny system wymusza ich zmianę co sześć miesięcy zgodnie wymaganiami dotyczącymi złożoności haseł. Każdy komputer ma zabezpieczony hasłem wygaszacz ekranu.

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

- Sieć firmowa jest zabezpieczona zaporami przed ruchem płynącym z sieci publicznej.

- 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.

- Firma SAP stosuje aktualne oprogramowanie antywirusowe w punktach dostępu do sieci firmowej (w przypadku kont poczty e-mail) oraz na wszystkich serwerach plików i stacjach roboczych.

- Security patch management processes to deploy relevant security updates on a regular and periodic basis.

- Full remote access to SAP's corporate network and critical infrastructure is protected by authentication.

1.3 Data Access Control.

- 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.

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil 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.

- 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/or penetration tests on its IT systems.

- Processes and policies to detect the installation of unapproved software on production systems.

- An SAP security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control

- Personal Data in transfer over SAP internal networks is protected according to SAP Security Policy.

- When data is transferred between SAP and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant 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

- Procedury zarządzania poprawkami zabezpieczeń umożliwiające regularne i okresowe wdrażanie odpowiednich aktualizacji zabezpieczeń.

- Pełny zdalny dostęp do sieci korporacyjnej SAP oraz krytycznej infrastruktury jest chroniony za pomocą uwierzytelnienia.

1.3 Kontrola dostępu do danych

- W ramach polityki bezpieczeństwa SAP Dane osobowe wymagają co najmniej takiego samego poziomu ochrony, jak ten stosowany w przypadku informacji poufnych zgodnie ze standardem klasyfikacji danych obowiązującym w firmie SAP.

- Dostęp do Danych osobowych jest udzielany wyłącznie w zakresie wymaganym do realizacji określonych zadań. Członkowie personelu mają dostęp do informacji, które są im niezbędne do wykonywania ich obowiązków. Firma SAP wykorzystuje koncepcje uprawnień, które dokumentują procesy udzielania uprawnień oraz role przypisane do każdego konta (ID użytkownika). Wszystkie dane Klienta są chronione w sposób zgodny z polityką bezpieczeństwa SAP.

- Wszystkie serwery produkcyjne są obsługiwane w Centrach danych lub zabezpieczonych serwerowniach. Środki bezpieczeństwa chroniące aplikacje przetwarzające Dane osobowe są regularnie kontrolowane. W tym celu firma SAP przeprowadza wewnętrzne i zewnętrzne kontrole bezpieczeństwa oraz/lub testy penetracyjne swoich systemów IT.

- Procedury i polityka do wykrywania instalacji niezatwierdzonego oprogramowania na systemach produkcyjnych.

- Standard bezpieczeństwa SAP reguluje sposób usuwania lub niszczenia danych i nośników danych, gdy nie są już wymagane.

1.4 Kontrola transmisji danych

- Dane osobowe przesyłane w wewnętrznych sieciach SAP są chronione w sposób określony w polityce bezpieczeństwa SAP.

- W przypadku przesyłania danych między firmą SAP i jej Klientami środki ochrony stosowane w odniesieniu do przesyłanych Danych osobowych są zgodne z wcześniejszymi ustaleniami zapisanymi w odpowiedniej umowie. Dotyczy to zarówno fizycznego, jak i sieciowego transferu danych. W każdym przypadku Klient przejmuje odpowiedzialność za transfer danych, które opuszczają systemy kontrolowane przez firmę

transmitted outside the firewall of the SAP Data Center).

SAP (np. dane są przesyłane poza zaporę Centrum danych SAP).

1.5 Data Input Control

1.5 Kontrola wprowadzania danych

- SAP only allows authorized personnel to access Personal Data as required in the course of their duty.
- Firma SAP umożliwia dostęp do Danych osobowych jedynie upoważnionemu personelowi na podstawie wymogów wynikających z wykonywanych obowiązków.
- SAP has in most cases implemented a logging system for input, modification and deletion, or blocking of Personal Data by SAP or its subprocessors within the Cloud Service to the extent technically possible.
- Firma SAP wdrożyła w większości przypadków system rejestracji wprowadzania, modyfikacji i usuwania lub blokowania Danych osobowych przez firmę SAP lub jej podwykonawców przetwarzania w ramach Rozwiązania w chmurze w zakresie, w jakim jest to technicznie możliwe.

1.6 Job Control.

1.6 Kontrola zadań

- SAP uses controls and processes to monitor compliance with contracts between SAP and its customers, subprocessors or other service providers.
- Firma SAP wykorzystuje mechanizmy kontrolne i procesy umożliwiające monitorowanie przestrzegania umów między firmą SAP i jej klientami, podwykonawcami przetwarzania lub innymi usługodawcami.
- 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.
- W ramach polityki bezpieczeństwa SAP Dane osobowe wymagają co najmniej takiego samego poziomu ochrony, jak ten stosowany w przypadku informacji poufnych zgodnie ze standardem klasyfikacji danych obowiązującym w firmie 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.
- Wszyscy pracownicy firmy SAP i kontraktowi podwykonawcy przetwarzania danych lub inni usługodawcy są zobowiązani na mocy umowy do respektowania poufności wszystkich danych wrażliwych, w tym tajemnic handlowych klientów i partnerów firmy SAP.

1.7 Availability Control

1.7 Kontrola dostępności

- SAP employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- Firma SAP stosuje procesy regularnego tworzenia kopii zapasowych umożliwiające w razie potrzeby szybkie przywrócenie systemów niezbędnych do prowadzenia działalności biznesowej.
- SAP uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.
- Firma SAP używa również zasilaczy awaryjnych (na przykład zasilaczy UPS, akumulatorów, generatorów itd.), aby zagwarantować ciągłość zasilania w Centrach danych.
- SAP has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Order Form for the relevant Cloud Service.
- Firma SAP opracowała plany awaryjne dla procesów niezbędnych do prowadzenia działalności i może zaoferować strategie odtwarzania po awarii dla usług o krytycznym znaczeniu dla działalności, opisane w dokumentacji lub uwzględnione w Formularzu zamówienia dla odpowiedniego Rozwiązania w chmurze.

- Emergency processes and systems are regularly tested.

- Procesy i systemy awaryjne są regularnie testowane.

1.8 Data Separation Control

1.8 Kontrola rozdzielania danych

- SAP uses the technical capabilities of the deployed software (for example: multi-tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.

- Firma SAP wykorzystuje możliwości techniczne wdrożonego oprogramowania (na przykład: architektura oparta na wielu mandantach lub osobne struktury systemów) w celu skutecznego oddzielenia Danych osobowych pochodzących od różnych klientów.

- Customer (including its Controllers) has access only to its own data.

- Klient (dotyczy to również Administratorów) ma dostęp wyłącznie do własnych danych.

- 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.

- Jeśli przekazanie Danych osobowych jest niezbędne do obsługi incydentu zgłoszonego przez Klienta, dane są przypisywane do konkretnej wiadomości i wykorzystywane wyłącznie do jej przetwarzania; nie są używane do innych celów. Takie dane są przechowywane w dedykowanych systemach pomocy technicznej.

1.9 Data Integrity Control

1.9 Kontrola integralności danych

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

Firma SAP wdrożyła całościową strategię ochrony zabezpieczającą przed nieupoważnionymi zmianami.

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

Firma SAP wykorzystuje wiele różnych elementów w celu zapewnienia opisanych wyżej mechanizmów kontrolnych i środków bezpieczeństwa. W szczególności:

- Firewalls;

- Zapory;

- Security Monitoring Center;

- Centrum monitorowania zabezpieczeń;

- Antivirus software;

- Oprogramowanie antywirusowe;

- Backup and recovery;

- Tworzenie kopii zapasowych i odzyskiwanie danych;

- External and internal penetration testing and/or regular external audits to prove security measures.

- Zewnętrzne i wewnętrzne testy penetracyjne i/lub regularne audyty zewnętrzne sprawdzające skuteczność środków bezpieczeństwa.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

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	Bezpieczeństwo przetwarzania And Appendix 2 Technical and Organizational Measures
28(2), 28(3) (D) And 28 (4)	6	SUBPROCESSORS
28 (3) Sentence 1	1.1 And Appendix 1, 1.2	Purpose and Application., Appendix 1, Struktura
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	Bezpieczeństwo przetwarzania 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	Bezpieczeństwo przetwarzania And Appendix 2 Technical and Organizational Measures, Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (G)	4	Data export and Deletion
28(3) (H)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) C)	7.2	Standard Contractual Clauses.

Załącznik 3 do DPA oraz (w odpowiednich wypadkach) Standardowych klauzul umownych

W poniższej tabeli przedstawiono istotne artykuły RODO oraz odpowiadające im warunki DPA. Tabela ma wyłącznie charakter poglądowy.

Artykuł RODO	Punkt DPA	Kliknij łącze, aby przejść do wybranego punktu
28(1)	2 oraz Appendix 2	Bezpieczeństwo przetwarzania oraz Appendix 2 Technical and Organizational Measures
28(2), 28(3) (D) oraz 28 (4)	6	SUBPROCESSORS
28 (3) Zdanie 1	1.1 oraz Appendix 1, 1.2	Purpose and Application., Appendix 1, Struktura
28(3) (A) oraz 29	3.1 oraz 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (B)	3.3	Personnel.
28(3) (C) oraz 32	2 oraz Appendix 2	Bezpieczeństwo przetwarzania oraz Appendix 2 Technical and Organizational Measures
28(3) (E)	3.4	Cooperation.
28(3) (F) oraz 32-36	2 oraz Appendix 2 , 3.5, 3.6	Bezpieczeństwo przetwarzania oraz Appendix 2 Technical and Organizational Measures, Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (G)	4	Data export and Deletion
28(3) (H)	5	CERTIFICATIONS AND AUDITS
28 (4)	6	SUBPROCESSORS
30	8	Documentation; Records of processing
46(2) C)	7.2	Standard Contractual Clauses.