Accordo sulla Protezione dei Dati (“DPA”) per Unify Cloud Services in conformità ad Art. 26 del GDPR

In vigore dal 28 Gennaio 2019 (la “Data di entrata in vigore”)

Tra il Cliente (“Cliente”) e Unify Software and Solutions GmbH & Co.KG (“Unify”)

di seguito singolarmente la “**Parte**” e congiuntamente le “**Parti**”.

Unify Cloud Services consentono al Cliente ed ai suoi Utenti Unify Cloud Services di inserire informazioni per il trattamento da parte del software fornito come servizio. Nella misura in cui queste informazioni contengono Dati personali, le Parti convengono espressamente l’applicazione del presente DPA sulla Responsabilità Condivisa, nei casi in cui entrambe condividono i ruoli e le responsabilità di un Titolare del trattamento dei dati come segue:

- Il Cliente (i) definisce le finalità del Trattamento di Dati personali, (ii) è responsabile dell’esattezza dei Dati Personali, (iii) ha la responsabilità di informare gli interessati in merito al trattamento di Dati Personali e alle modalità per l’esercizio dei loro diritti, e (iv) se necessario, è responsabile di effettuare le notifiche (comprese quelle per la Violazione della Protezione dei Dati) alle autorità per la protezione dei dati.
- Unify (i) definisce i mezzi del Trattamento ed (ii) è responsabile dell’attuazione delle misure di sicurezza,

Questi ruoli e responsabilità sono descritti in maggior dettaglio al successivo Articolo 4 (Ruoli e responsabilità).

Il presente DPA si applica a tutte le attività realizzate da Unify nel contesto di Unify Cloud Services e delle Condizioni per la produzione del servizio (TOSP) pubblicate da Unify per questi Unify Cloud Services, per mezzo delle quali i dipendenti di Unify o soggetti terzi ai quali Unify ha subappaltato tali attività potrebbero gestire i Dati personali del Cliente.

Il DPA non si applica ad altri prodotti, siti o servizi di Unify sia online che offline. Per quanto riguarda Unify Cloud Services, il presente DPA prevale su qualsiasi altro accordo per il trattamento dei dati in essere o accordo analogo tra Unify e il Cliente già esistente per tali altri prodotti, siti o servizi.

Il Cliente riconosce di aver ricevuto tutte le informazioni che ritiene necessarie per stabilire che Unify fornisce sufficienti garanzie per la protezione di Dati personali.

1. Definizioni

Oltre ai termini definiti in altre parti delle TOSP si applicano le seguenti definizioni:

1.1 Con “**Legge applicabile in materia di protezione dei dati**”: s’intendono le leggi e i regolamenti che riguardano il trattamento e la protezione di Dati personali applicabili nel paese in cui Unify ha la sua sede. In particolare, con Legge applicabile s’intendono (a) il Regolamento UE 2016/679 (Regolamento generale sulla protezione dei dati, ‘GDPR’) (b) le leggi o la normativa dello Stato membro in relazione al trattamento e alla protezione dei Dati personali in attuazione o integrazione del GDPR; e (c) qualsiasi altra legge o normativa applicabile in materia di trattamento e protezione dei Dati personali ai fini del presente Accordo.

1.2 "**Violazione della protezione dei dati**" indica una violazione della sicurezza che porta alla distruzione, perdita, alterazione o divulgazione non autorizzata o illegale dei dati personali elaborati ai fini del presente DPA.

1.3 "**Dati Personali**" indicano qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un numero di identificazione o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

1.4 Con “**Trattamento**” o “**Tratta**” s’intende qualsiasi operazione o serie di operazioni compiute sui Dati personali, con o senza l’ausilio di processi automatizzati, come la raccolta, la conservazione, l’adattamento o la modifica, il recupero, la consultazione l’utilizzo, la divulgazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, allineamento o combinazione, limitazione, cancellazione o distruzione.

1.5 Con “**Titolare del trattamento**” s’intende la persona fisica o giuridica che singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali.

2. Categorie di Dati personali ai sensi del presente DPA:

Le seguenti categorie di Dati personali sono, di norma, raccolti e trattati da Unify per realizzare i Servizi ai sensi delle TOSP:

- Dati di profilo: Dati personali di Utenti di Unify Cloud Services (Utenti) che creano, in particolare, nome utente, password, indirizzo e-mail e diritti di accesso;
- Dati di attività: Dati personali ricavati dall'utilizzo da parte dell'Utente di Unify Cloud Services, in particolare dati del registro chiamate, i record di modifica o eliminazione di contenuti o i dati che si riferiscono all'utilizzo del servizio (ad es. endpoint usati) da parte di un utente nella misura in cui tali dati non siano stati resi anonimi per generare Dati di utilizzo aggregati;
- Dati transitori e di sessione: Dati personali che non sono memorizzati sui Unify Cloud Services (come informazioni su presenza o posizione) oppure che sono legati ad una sessione di accesso su Unify Cloud Services (ad es. indirizzi IP).

Dal presente DPA sono escluse le seguenti categorie di Dati personali:

- Dati personali di soggetti terzi che gli Utenti di Unify Cloud Services possono immettere in Unify Cloud Services mediante post di testo, caricamento di documenti o registrazioni vocali. Questi dati non possono essere riconosciuti come Dati personali da Unify Cloud Services.
- Dati personali di soggetti terzi che gli Utenti di Unify Cloud Services possono inserire nei loro dispositivi telefonici come nelle rubriche private. Questi dati non sono memorizzati o trattati da Unify Cloud Services ma sono presenti solo sul telefono degli Utenti, al di fuori di Unify Cloud Services.
  Si consiglia al Cliente di regolare l'utilizzo in relazione a tali Dati personali di Unify Cloud Services mediante adeguate politiche per la protezione dei dati.

3. Categorie di Interessati ai sensi del presente DPA:

Nel contesto del presente DPA, il trattamento dei Dati personali riguarda le seguenti categorie di Interessati:

- Utenti della Tenancy nella Tenancy dei servizi cloud del Cliente,
- Utenti Cross-Tenancy con accesso alla Tenancy dei servizi cloud del Cliente (solo per Dati di attività tenuti nella Tenancy di servizi cloud del Cliente)
- Utenti guest della sessione con accesso alla Sessione di servizi cloud del Cliente

4. Ruoli e responsabilità di Cliente e Unify

4.1 Ruolo e responsabilità del Cliente:

4.1.1 **Finalità e legalità del Trattamento**: Il Cliente sarà responsabile della definizione della finalità del Trattamento di Dati personali, della legittimità del trasferimento di Dati personali a Unify nonché della legittimità del Trattamento dei dati. Il Cliente adempirà e farà sì che le sue società collegate e i suoi collaboratori adempiano a tutti i suoi obblighi ai sensi della Normativa in materia di protezione dei dati durante il trattamento di Dati personali in relazione ai servizi cloud. A questo proposito, il Cliente garantirà, in particolare, di aver ottenuto e di mantenere tutte le registrazioni e le autorizzazioni necessarie con le autorità per la protezione dei dati competenti e le basi giuridiche valide per trattare i Dati personali.

4.1.2 **Esercizio dei propri diritti da parte degli Interessati**: il Cliente sarà il contatto principale per gli Interessati per l'esercizio dei loro diritti come stabilito dalla Legislazione applicabile in materia di protezione dei dati.

4.1.3 **Esattezza, qualità, legalità e affidabilità dei Dati personali**: Il Cliente sarà il solo responsabile dell'esattezza, della qualità, della legalità e dell'affidabilità dei Dati personali e dei mezzi mediante i quali acquisisce Dati personali per il trattamento da parte di Unify Cloud Services.

4.1.4 **Valutazione dei rischi**: Il Cliente sarà responsabile della valutazione dei rischi derivanti dal Trattamento dei Dati personali.

4.1.5 **Registri del Trattamento**: Nella misura richiesta dalla legge applicabile, il Cliente sarà responsabile di predisporre e mantenere i Registri di Trattamento delle attività. Unify renderà disponibili le rispettive informazioni nella "Informativa sul trattamento dei dati personali per gli utenti"

4.1.6 **Informazioni agli Interessati**: Il Cliente sarà responsabile di fornire le informazioni agli Interessati in relazione al trattamento dei Dati personali in base alle disposizioni previste dalla Legislazione applicabile in materia di protezione dati.

4.1.7 **Informazioni sulla Ripartizione delle Responsabilità agli Interessati**: Il Cliente è responsabile di informare l'Interessato in ordine alla ripartizione di responsabilità tra le parti contraenti come indicato nel presente DPA.

4.1.8 **Notifica della Violazione della Protezione dei Dati**: Il Cliente è tenuto ad adempiere agli obblighi di notifica della violazione di dati derivanti dai requisiti applicabili di protezione dei dati. Quando è la Legge applicabile in materia di protezione dei dati ad imporlo, il Cliente è responsabile della notifica della violazione di protezione dei dati personali agli Interessati e alle Autorità per la Protezione dei Dati.

4.1.9 **Modifiche alla Legislazione applicabile**: Il Cliente è tenuto a comunicare a Unify, nei termini previsti, le modifiche alle disposizioni di legge che possono interessare gli obblighi contrattuali di Unify ai sensi del presente DPA e che possono richiedere la modifica del DPA e del corrispettivo pattuito. Unify ha anche la facoltà di presentare al Cliente delle proposte qualora ritenga necessaria l'introduzione di un determinato cambiamento per continuare ad agire in conformità alla Legge applicabile.

4.1.10 **Irregolarità o errori nel Trattamento di Dati personali**: Il Cliente è tenuto ad informare Unify in modo tempestivo ed esauriente in merito ad eventuali errori o irregolarità, di cui dovesse venire a conoscenza, che riguardano la Normativa per la protezione dei dati sul Trattamenti di Dati personali.

4.1.11 **Notifica ai Destinatari di Dati personali in merito alla rettifica, alla cancellazione di Dati personali o alla limitazione del Trattamento:** Unify divulga i Dati personali esclusivamente per il Trattamento necessario per l'erogazione di Unify Cloud Services (consultare l'articolo 8). Nella misura in cui il Cliente divulga Dati personali ad un destinatario ad es. aggregando Unify Cloud Services ad altri servizi cloud di trasmissione di Dati personali mediante interfacce Circuit al di fuori di Circuit, il Cliente è tenuto a informare i destinatari in questione in ordine alle richieste degli Interessati per la rettifica o la cancellazione di Dati personali divulgati oppure in merito a una limitazione del trattamento.

4.1.12 **Divulgazione di Dati personali**: Unify divulga i Dati personali solo ai destinatari per i quali è tenuto a farlo ai fini del trattamento. Per maggiori informazioni, consultare la "Informativa sul trattamento dei dati personali per gli utenti". Alcune funzioni di Unify Cloud Services consentono a clienti e utenti di divulgare Dati personali a terzi. Nella misura in cui il Cliente o i suoi utenti utilizzano tali funzioni, il Cliente ha la responsabilità di informare gli Interessati (articolo 4.1.6) e di inserire l'utilizzo in questione nei Registri di Trattamento (punto 4.1.5).

4.2 Ruolo e responsabilità di Unify

4.2.1 **Mezzi di Trattamento**: Unify sarà responsabile di definire i mezzi di Trattamento e, in riferimento ai punti 4.1.5 e 4.1.6, di fornire informazioni su tali mezzi al Cliente, in modo specifico per consentire al Cliente di completare i Registri di Trattamento e di informare gli Interessati come previsto dalla Legislazione applicabile in materia di protezione dei dati. Le "Informazioni sul Trattamento" sono disponibili nella "Informativa sul trattamento dei dati personali per gli utenti".http://go.unify.com/Dataprotection

4.2.2 **Ambito di applicazione del Trattamento da parte di Unify**: Unify può raccogliere e trattare Dati personali solo nel contesto del presente DPA e delle TOSP applicabili a Unify Cloud Services erogati al Cliente e per migliorare ed effettuare l'upgrade di questi servizi. Modifiche sostanziali che interessano l'ambito di applicazione del Trattamento dei dati vanno stabilite di comune accordo e devono essere documentate. In virtù del presente DPA, Unify riconosce espressamente che tratterà i Dati personali solo per erogare Unify Cloud Services, per migliorarli ed effettuarne l'upgrade.

4.2.3 **Attuazione delle Misure di sicurezza**: Unify sarà responsabile dell'attuazione delle misure di sicurezza per il Trattamento di Dati personali nel contesto di Unify Cloud Services. Unify adotterà le Misure tecniche e organizzative (TOM) adeguate, come indicato nell'Allegato 1 del presente DPA, elaborate per proteggere i Dati personali del Cliente da uso improprio e perdita, oppure da qualsiasi

altra violazione della protezione dei dati in conformità alla Normativa applicabile in materia di protezione dei dati. Il Cliente è consapevole del fatto che le misure tecniche e organizzative sono soggette al progresso tecnico e ad ulteriori sviluppi. A questo riguardo, Unify potrà usare misure alternative adatte, informandone i clienti rendendo disponibile, su richiesta, una descrizione delle misure in questione.

4.2.4 **Informazioni agli Interessati sulla ripartizione di responsabilità delle Parti**: Unify è responsabile di rendere accessibile il documento DPA standard senza modifiche a tutti gli Utenti di Unify Cloud Services. Qualora il DPA contenga delle modifiche rispetto al documento DPA standard richiesto dal Cliente, Unify non è in alcun modo responsabile di rendere tali modifiche accessibili agli Interessati.

4.2.5 **Notifica della Violazione della Protezione dei Dati**: In riferimento al punto 4.1.8, in caso di Violazione della Protezione dei Dati, Unify presterà assistenza al Cliente e metterà a disposizione tutte le informazioni necessarie alle quali ha accesso per consentire al Cliente di adempiere ai propri obblighi. Unify informerà il Cliente senza ritardo ingiustificato in relazione ad eventuali violazioni dei Dati personali del Cliente rilevate da Unify.

4.2.6 **Conservazione dei Dati personali/ Limitazioni per la cancellazione**: Di norma**,** i Dati personali trattati da Unify Cloud Services vengono conservati fino a) alla loro eliminazione da parte del Cliente o degli Utenti di Unify Cloud Services, oppure b) alla scadenza del periodo di conservazione indicato dal Cliente, oppure c) alla risoluzione dell'accordo per i servizi cloud del Cliente su Unify Cloud Services.

4.2.7 **Cancellazione dei Dati personali ed esportazione alla cessazione dell'Accordo per i Servizi Cloud**: Unify sarà responsabile di cancellare tutti i dati inseriti dal Cliente e dagli Utenti di Unify Cloud Services nelle applicazioni Software fornite da Unify Cloud Services ("Dati della Tenancy") compresi i Dati personali alla fine del mese solare successivo alla scadenza o alla cessazione dell'uso da parte del Cliente di Unify Cloud Services oppure, su richiesta del Cliente, in qualsiasi momento. Su richiesta da parte del Cliente, Unify fornirà un'esportazione dei Dati della Tenancy in un formato di dati che possa essere trattato dal Cliente per il trasferimento ad altri servizi cloud.

4.2.8 **Esercizio dei propri diritti da parte degli Interessati**: Nel caso in cui Unify riceva una richiesta da parte di un Interessato per l'esercizio dei diritti in conformità alle disposizioni previste nella Legislazione applicabile in materia di Protezione dei Dati, Unify è tenuta a inoltrare tale richiesta al Cliente che, senza ritardo ingiustificato, le fornirà indicazioni in merito a come procedere. Il Cliente riconosce che in caso di un conflitto tra l'Interessato e il Cliente, la legislazione applicabile potrebbe costringere Unify a soddisfare la richiesta dell'Interessato nonostante l'opposizione da parte del Cliente. Ad ogni modo, l'adozione di tale misura da parte di Unify avverrebbe solo dopo un'attenta valutazione della situazione legale con il Cliente.

4.2.9 **Effetti della Cancellazione di Dati personali**: Con il presente accordo il Cliente conferma e riconosce che qualora gli venga richiesto dal Cliente di cancellare i Dati personali o di limitarne il Trattamento, questo potrebbe rendere impossibile l'erogazione dei prodotti o dei servizi sottoscritti o forniti. Unify provvederà a darne comunicazione al Cliente prima di eseguire la richiesta.

4.2.10 **Copie di back-up di Dati personali**: Unify eseguirà delle copie di back-up dei Dati personali nella misura in cui le stesse sono necessarie per garantire il corretto trattamento dei Dati personali. Unify può copiare e conservare i Dati personali necessari per consentire al Cliente e a Unify di adempiere agli obblighi di conservazione dei documenti stabiliti per legge.

4.2.11 **Gestione supporti e materiale di prova**: Unify memorizzerà e gestirà con cura i supporti forniti da Unify, e tutte le copie e riproduzioni degli stessi, in modo da non renderli accessibili a terzi. Unify sarà tenuta a predisporre la distruzione del materiale di prova e di altro materiale contente Dati personali la cui eliminazione deve avvenire in conformità alla legge solo a seguito di una richiesta specifica da parte del Cliente e a spese di quest'ultimo.

4.2.12 **Responsabile della protezione dati**: Unify è tenuta a mettere a disposizione su Internet i dati di contatto del suo Responsabile della protezione dati (DPO). Alla Data di entrata in vigore del presente DPA, i dati di contatto del DPO sono dp.it-solutions@atos.net.

5. Responsabilità e accordi reciproci

5.1 Le Parti convengono che eventuali richieste relative ai Dati personali formulate dal Cliente saranno presentate in forma scritta ed esplicita. Nel caso in cui per tali richieste sia necessaria una modifica dei servizi, tale modifica sarà rinegoziata in buona fede dalle parti, unitamente al relativo prezzo.

5.2 Ogni Parte garantirà che il proprio personale sia vincolato per legge a rispettare gli obblighi di protezione dei dati ed a mantenere la riservatezza dei dati e che sia a conoscenza di altre disposizioni applicabili per la protezione di Dati personali, in particolare in riferimento alla segretezza delle telecomunicazioni. L'obbligo alla segretezza dei dati continua per il personale una volta concluso il lavoro o il contratto d'impiego.

5.3 Qualora ritenga che soddisfare le richieste del Cliente potrebbe comportare una violazione della Normativa applicabile in materia di protezione dei dati, Unify è tenuta a darne tempestiva comunicazione al Cliente. Unify avrà diritto a sospendere l'attuazione di tale richiesta fino alla conferma o alla modifica della stessa da parte del Cliente.

5.4 In virtù del presente DPA le Parti riconoscono che le misure di sicurezza di cui all'Allegato 1 (Misure tecniche e organizzative) forniscono garanzie sufficienti ai Dati personali Trattati. Il Cliente è consapevole del fatto che le misure tecniche e organizzative sono soggette al progresso tecnico e ad ulteriori sviluppi. A questo riguardo, Unify potrà adottare le opportune misure alternative.

5.5 Nel caso in cui i Dati personali del Cliente siano soggetti a perquisizione e sequestro, ad un ordine di pignoramento, a confisca durante procedure fallimentari o concorsuali, oppure ad eventi o a misure analoghe da parte di terzi, se consentito dalla legge, Unify è tenuta ad informare il Cliente senza ritardo ingiustificato. A sua volta, senza ritardo ingiustificato, Unify comunicherà a tutte le parti interessate da tale azione che i Dati personali interessati dalle misure in questione sono di proprietà esclusiva del Cliente ed è lo stesso a disporne in via esclusiva, e che è il Cliente ad essere responsabile in conformità alla Legge applicabile in materia di protezione dei dati.

6. Richieste da parte di autorità di controllo

6.1 Nei casi previsti dalla legge, entrambe le Parti conserveranno i documenti relativi ai Dati personali trattati ai fini del presente DPA, collaboreranno e forniranno tutte le informazioni necessarie per l'adempimento dei succitati obblighi e dell'obbligo di notifica ai sensi della Legge applicabile in materia di protezione dei dati.

6.2 Nei casi in cui Unify deve prestare assistenza al Cliente per adempiere agli obblighi legali di quest'ultimo in conformità alle disposizioni di cui al presente articolo 6, il Cliente provvederà a rimborsare a Unify eventuali ulteriori costi ragionevoli legati all'assistenza prestata.

7. Diritti di controllo

7.1 Non più di una volta all'anno e con una richiesta scritta inviata almeno sessanta (60) giorni prima, ogni Parte avrà diritto a realizzare un controllo per verificare il rispetto delle disposizioni contenute nel presente DPA, verificando le misure tecniche e organizzative attuate dalla parte che viene sottoposta al controllo. Le prove per dimostrare l'attuazione di tali misure che non sono collegate esclusivamente a questo specifico DPA o all'Accordo possono essere anche fornite presentando un certificato attuale, relazioni o estratti da relazioni redatte da soggetti terzi indipendenti, ad es. da revisori ufficiali dei conti, da revisori contabili, da uno o più responsabili della protezione dati interni o esterni della Parte sottoposta al controllo, dall'ufficio per la sicurezza IT, dagli auditor per la privacy interni ed esterni, dagli auditor per la qualità, oppure presentando un certificato idoneo rilasciato successivamente alla verifica realizzata da un soggetto terzo sulla protezione dei dati o sulla sicurezza IT della parte sottoposta al controllo.

7.2 Ogni parte si riserva il diritto di rifiutarsi di fornire all'altra Parte segreti industriali o aziendali, know-how operativo ed informazioni il cui controllo costituirebbe un rischio per la sicurezza della Parte sottoposta al controllo o dei suoi clienti, oppure che la Parte sottoposta al controllo non è tenuta a fornire o rivelare, trattandosi di dati tutelati dalla legge o di dati di altri clienti.

8. Sub-responsabili

8.1 In virtù del presente DPA, il Cliente riconosce e accetta che Unify possa assumere subappaltatori per la fornitura di Unify Cloud Services. Tali subappaltatori possono essere società del Gruppo Atos

(“Subappaltatori interni”) oppure subappaltatori terzi (“Subappaltatori esterni”). Un elenco completo dei subappaltatori approvati alla Data di entrata in vigore del presente DPA è disponibile nella "Informativa sul trattamento dei dati personali per gli utenti", con l’inclusione delle misure di salvaguardia applicabili a garanzia di un’adeguata protezione dei Dati personali.

8.2 Nel caso in cui Unify intenda assumere un nuovo subappaltatore esterno che non figura nell’elenco dei subappaltatori approvati alla Data di entrata in vigore del presente DPA, saranno applicati i punti 9.2 e 9.3. A scanso di equivoci, si conviene espressamente che i Subappaltatori interni sono esclusi dalla presente disposizione e si ritiene che il Cliente non si opponga al ricorso a Subappaltatori interni.

8.3 Trasferimenti di Dati personali a Paesi o Paesi terzi:

8.3.1 In virtù del presente DPA, il Cliente riconosce ed accetta espressamente che i Dati personali possano essere trasferiti e/o trattati da Subappaltatori esterni secondo quanto indicato al precedente punto 8.1 compreso il caso in cui tali Subappaltatori esterni siano al di fuori dello Spazio Economico Europeo (SEE).

8.3.2 I Subappaltatori interni fanno parte del Gruppo Atos e sono quindi vincolati dalle Binding Corporate Rules (BCR) come approvate dalle autorità europee per la protezione dei dati e disponibili all’indirizzo: https://atos.net/content/dam/global/documents/atos-binding-corporate-rules.pdf (le “BCR”). Il Cliente riconosce che qualora Unify trasferisca i Dati personali a qualsiasi entità del Gruppo Atos che si trova al di fuori del SEE, le BCR rappresentano una misura di salvaguardia sufficiente per stabilire che tali entità forniscono una protezione adeguata ai Dati personali come previsto ai sensi della Legge applicabile in materia di protezione dei dati. Di conseguenza, con il presente DPA, il Cliente acconsente espressamente che i Dati personali possano essere trasferiti alle entità del Gruppo Atos vincolate dalle condizioni delle BCR come indicato all’Allegato 2 delle stesse. Utilizzando ogni mezzo opportuno, Unify renderà disponibili al Cliente eventuali aggiornamenti all’Allegato 2 delle BCR. Il Cliente si impegna a fornire informazioni sufficienti agli Interessati in relazione alle BCR.

8.3.3 Nei casi in cui Unify trasferisce i Dati personali ad un Subappaltatore esterno, fuori dal SEE, che non rientra nell’ambito di applicazione delle BCR, con il presente DPA, il Cliente concede espressamente a Unify un mandato per stipulare qualsiasi accordo per garantire che la parte ricevente metta in atto un livello sufficiente di protezione per i Dati personali riconosciuto come adeguato dalle autorità locali o europee competenti.

9. Modifiche al presente DPA

9.1 Il Cliente riconosce che le condizioni di cui al presente DPA e all’Allegato 1 possono essere modificate da Unify. Una modifica richiede il consenso da parte del Cliente qualora a) interessi la ripartizione delle responsabilità tra le parti contraenti, oppure b) limiti i diritti del Cliente, o c) richieda il consenso in conformità alle disposizioni di cui alla Legislazione applicabile sulla Protezione dei Dati. Negli altri casi è necessario solo che il Cliente sia informato della modifica.

9.2 Nel caso di un cambiamento per il quale è necessario ottenere il consenso del Cliente, Unify comunicherà al Cliente la modifica mediante e-mail all’amministratore del tenant in base al quale la Tenancy del servizio cloud del Cliente è registrata a Unify, oppure mediante un partner di vendita accreditato di Unify con il quale il Cliente ha stipulato l’accordo per i servizi cloud per un singolo Unify Cloud Service e renderà le informazioni pertinenti disponibili al Cliente affinché possa consultarle almeno trenta (30) giorni solari prima della data in cui la modifica entra in vigore. Unify offrirà al Cliente la possibilità di esprimere il proprio consenso o di opporsi. Qualora Unify non riceva alcuna obiezione da parte del Cliente dopo il periodo di risposta indicato nella comunicazione di modifica, che dovrà essere di almeno dieci (10) giorni solari dalla data della comunicazione, il consenso del Cliente si intenderà concesso. In situazioni di emergenza, è possibile una riduzione dei periodi per la comunicazione e la risposta.

9.3 Il Cliente non si opporrà ad una modifica senza fornire a Unify una spiegazione scritta dettagliata delle motivazioni per tale opposizione. Unify metterà in atto ogni sforzo ragionevole, da un punto di vista commerciale, per fornire spiegazioni in merito alle preoccupazioni manifestate dal Cliente. Le Parti collaboreranno in buona fede per raggiungere un accordo. Qualora ciò non sia possibile, si procederà alla cessazione di Unify Cloud Services contrattualizzati.

10. Responsabilità

10.1 Unify e il Cliente adempieranno ai rispettivi obblighi come indicato nel presente DPA e dalla Legge applicabile in materia di protezione dati.

10.2 Il Cliente sarà totalmente responsabile in caso di mancato adempimento degli obblighi di cui al precedente punto 4.1 e di quelli indicati al precedente articolo 5.

10.3 Unify sarà totalmente responsabile in caso di mancato adempimento degli obblighi di cui al precedente punto 4.2 e di quelli indicati al precedente articolo 5, ferma restando l'eventuale responsabilità del Cliente.

10.4 La Parte inadempiente sarà esonerata da eventuali responsabilità qualora riesca dimostrare di essere totalmente estranea alla circostanza che ha determinato il danno.

10.5 Nei casi in cui il Cliente e Unify sono responsabili di eventuali danni causati in violazione di un adempimento previsto dal presente DPA, ogni Parte sarà ritenuta responsabile dell'intero danno per garantire l'effettivo risarcimento dell'Interessato. La Parte che si è fatta carico per intero del risarcimento per il danno subito avrà diritto di richiedere all'altra Parte coinvolta la quota di risarcimento che corrisponde alla sua parte di responsabilità per il danno in questione.

11. Disposizioni generali

11.1 Qualora una singola disposizione del DPA sia illegale, priva di valore, nulla, annullabile o inapplicabile, il resto del DPA continuerà ad avere piena validità ed efficacia. Le Parti concorderanno una disposizione efficace che rifletta, per quanto legalmente possibile, le intenzioni delle Parti nel modo più preciso possibile.

Allegato 1 - **Misure tecniche e organizzative generali di Unify (TOM)**

Unify applica le misure tecniche e organizzative previste dalla legge in base al "Data Privacy and Information Security Framework" (il "DIS Framework") che definisce gli standard richiesti dalla policy (livello 2) e le procedure operative (livello 3) in conformità allo standard internazionale ISO27001 sulla base della policy aziendale "Data Privacy and Information Security Policy". I documenti sono disponibili per il Cliente su richiesta.

Non è possibile per la seguente descrizione dello *status quo* delle misure elementari in materia di protezione dei dati coprire la totalità delle misure di sicurezza adottate da Unify. In particolare per quanto riguarda la protezione e la sicurezza dei dati, non è possibile fornire delle descrizioni dettagliate delle misure riservate, dal momento che la tutela delle misure di sicurezza per evitare la divulgazione non autorizzata è almeno tanto importante quanto la misura di sicurezza stessa.

Il Cliente viene incoraggiato a parlare di ogni singola questione che riguarda le misure tecniche e organizzative con l'account manager del Cliente presso Unify, con il DPO di Unify e, se del caso, con il Chief Information Security Officer (CISO) di Unify.

1. Controllo degli ingressi

Misure tecniche od organizzative in relazione al controllo degli ingressi, in particolare alla legittimazione delle persone autorizzate:

Il controllo degli ingressi ha lo scopo di impedire alle persone non autorizzate di accedere fisicamente alle attrezzature per il trattamento dei dati in cui avviene l'utilizzo o il trattamento dei Dati personali.

In funzione dei rispettivi requisiti per la sicurezza, i locali e le strutture aziendali sono suddivisi in varie zone di sicurezza con autorizzazioni di accesso diverse. Queste zone sono controllate da personale addetto alla sicurezza. I dipendenti possono accedere solo con un ID codificato e una foto. Per tutte le altre persone l'accesso è consentito solo dopo la registrazione (ad es. all'ingresso principale).

L’accesso alle aree di sicurezza speciali come il centro servizi per la manutenzione a distanza è ulteriormente protetto da un’area di accesso separata. Gli standard di sicurezza costruttivi e sostanziali sono conformi ai requisiti di sicurezza per i data center.

2. Controllo dell’accesso al sistema

Misure tecniche (protezione della password) e organizzative (dati master dell’utente) in relazione a ID utente ed autenticazione:

Il controllo dell’accesso al sistema ha lo scopo di evitare l’uso non autorizzato di sistemi per il trattamento dei dati in cui avviene il trattamento e l’utilizzo di Dati personali.

I dati master dell’utente di ogni dipendente e il codice di identificazione individuale sono registrati nell’elenco globale dei contatti. È possibile accedere ai sistemi per il trattamento dei dati dopo aver eseguito l’identificazione e l’autenticazione con il codice di identificazione e la password per quel determinato sistema.

Sono presenti protezioni tecniche aggiuntive mediante l’utilizzo di firewall e server proxy.

Il controllo dell’accesso viene garantito mediante l’utilizzo di tecnologie di crittografia (ad es. accesso remoto alla rete aziendale tramite tunnel VPN). L’adeguatezza di una tecnologia di crittografia viene confrontata con lo scopo della protezione.

3. Controllo dell’accesso ai dati

Struttura su richiesta del concetto di autorizzazione e dei diritti di accesso ai dati nonché il loro monitoraggio e registrazione:

Le misure per il controllo dell’accesso ai dati devono essere mirate a consentire l’accesso solo ai dati per i quali esiste un’apposita autorizzazione e a rendere impossibile la lettura, la copia, la modifica o la cancellazione dei Dati personali in modo non autorizzato durante il trattamento, l’utilizzo e successivamente al salvataggio dei dati in questione.

L’accesso ai dati necessario per l’esecuzione di un determinato compito viene assicurato all’interno dei sistemi e delle applicazioni attraverso un concetto di autorizzazione e ruolo corrispondente. In conformità al principio della “necessità di conoscere”, ogni ruolo dispone solo di quei diritti che sono necessari per l’esecuzione del compito che il singolo individuo deve eseguire.

Il controllo dell’accesso ai dati viene garantito mediante l’utilizzo di tecnologie di crittografia (ad es. accesso remoto alla rete aziendale tramite tunnel VPN). L’adeguatezza di una tecnologia di crittografia viene confrontata con lo scopo della protezione.

4. Controllo della trasmissione

Misure che interessano il trasporto, il trasferimento, la trasmissione o la memorizzazione di Dati personali sui supporti (di memorizzazione) dati (in modo manuale o elettronico) e in relazione alla successiva verifica:

Il controllo della trasmissione mira a garantire che i Dati personali non possano essere letti, copiati, modificati o cancellati senza autorizzazione durante il loro trasferimento o mentre sono memorizzati su supporti dati e che sia possibile monitorarli e stabilire per quali destinatari è previsto un trasferimento di Dati personali.

Le misure necessarie per garantire la sicurezza dei dati durante il trasporto, il trasferimento e la trasmissione di Dati personali nonché di qualsiasi altro dato del cliente o della società sono illustrate in dettaglio nella policy sulla protezione delle informazioni commerciali riservate. Questa policy descrive in dettaglio l’intero trattamento dei dati, dalla creazione alla cancellazione, compreso il loro trattamento in conformità alla classificazione assegnata.

Il controllo del trasferimento viene garantito mediante l’utilizzo di una tecnologia di crittografia (ad es. accesso remoto alla rete aziendale tramite tunnel VPN). L’adeguatezza di una tecnologia di crittografia viene confrontata con lo scopo della protezione.

Il trasferimento di Dati personali ad un soggetto terzo (ad es. clienti, subappaltatori, fornitore di servizi) viene effettuato solo in presenza di un apposito contratto e solo per uno scopo specifico. Qualora i Dati personali siano

trasferiti a società la cui sede è fuori dall'UE/SEE, Unify stabilisce la presenza di un livello adeguato di protezione dei dati presso la sede o l'organizzazione di destinazione in conformità ai requisiti per la protezione dei dati dell'Unione europea, ad es. utilizzando contratti che si fondano sulle clausole contrattuali del modello UE.

5. Controllo inserimento dati

Misure in relazione alla verifica successiva, per stabilire se e da chi i dati sono stati inseriti, modificati o cancellati:

Il controllo dell'inserimento dei dati ha lo scopo di verificare, con l'ausilio delle misure adeguate, che sia possibile esaminare e controllare in modo retroattivo le circostanze dell'inserimento dei dati.

Gli input del sistema sono registrati in forma di file di registro, questo consente, in una fase successiva, di verificare se e da chi i Dati personali sono stati inseriti, modificati o cancellati.

6. Controllo del trattamento dei dati

Il controllo del trattamento dei dati ha lo scopo di assicurare che il trattamento dei Dati personali da parte di Unify avvenga in conformità alle Condizioni per la produzione del servizio (TOSP) pubblicate da Unify per il servizio cloud previsto per contratto e alle disposizioni stabilite nell'Accordo per il trattamento dei dati per Unify Cloud Services.

L'accesso ai Dati personali trattati in Unify Cloud Services è consentito solo all'organizzazione di gestione e all'assistenza tecnica. Unify ha introdotto delle policy per evitare che questa organizzazione utilizzi i Dati personali per qualsiasi altra finalità o per divulgare le Informazioni personali a qualsiasi altra organizzazione o soggetto terzo tranne che su istruzione del Cliente.

Un trasferimento di Dati personali ad un soggetto terzo, come un subappaltatore, viene effettuato solo nel rispetto degli accordi contrattuali e della Legge applicabile in materia di protezione dei dati.

7. Controllo della disponibilità

Misure in relazione al backup dei dati (fisico/logico):

Il controllo della disponibilità ha lo scopo di assicurare la protezione dei Dati personali da distruzioni e perdite accidentali.

Qualora i Dati personali non siano più necessari per le finalità per le quali sono stati trattati, vengono cancellati immediatamente. Va rilevato che con ogni cancellazione, i Dati personali, in prima battuta, sono solo bloccati per poi essere cancellati definitivamente in un momento successivo. Questa misura viene adottata per evitare cancellazioni accidentali o eventuali danni intenzionali.

Per motivi tecnici, è possibile che copie di Dati personali siano presenti nei file di backup e possono essere fatte mediante il mirroring dei servizi. Fermo restando l'obbligo di conservazione dei dati di Unify previsto dalla legge (si veda l'Accordo di Trattamento), anche tali copie vengono cancellate, se necessario, con un ritardo determinato in modo tecnico. La disponibilità dei sistemi stessi è garantita in conformità al livello di sicurezza necessario mediante le relative misure di sicurezza (ad es. mirroring di dischi rigidi, sistemi RAID e USV).

8. Controllo della separazione

Misure relative al trattamento separato (salvataggio, modifica cancellazione e trasferimento) dei dati con finalità diverse:

Il controllo della separazione ha lo scopo di assicurare che possano essere trattati separatamente i dati che sono stati raccolti per finalità diverse.

I Dati personali sono utilizzati solo per finalità interne (ad es. come parte del relativo rapporto con il cliente). Un trasferimento ad un soggetto terzo, come un subappaltatore, viene eseguito esclusivamente nel rispetto degli accordi contrattuali e della normativa in materia di protezione dei dati.

Ai dipendenti vengono date istruzioni per raccogliere, trattare e usare i Dati personali solo nel contesto e per le finalità previste dai compiti che devono svolgere (ad es. l'erogazione del servizio). A livello tecnico, a tale scopo,

vengono utilizzate funzionalità multi-client, la separazione delle funzioni e la separazione dei sistemi di produzione e prova.

9. Procedure aggiuntive per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (Art. 32 Sezione 1 (d) GDPR; Art. 25 Sezione 2 GDPR)

Gestione della protezione dei dati

In Atos la protezione dei dati è strutturata in base ad un'organizzazione globale con responsabili della protezione dei dati ed esperti in questioni legali per singole Global Business Unit (GBU) e paesi.

La GBU Germania dispone di un ufficio per la protezione dei dati composto da tre responsabili della protezione dei dati (DPO) e da almeno un esperto in questioni legali. L'ufficio per la protezione dei dati fa parte dell'organizzazione per la sicurezza delle informazioni e la protezione dei dati che, con cadenza regolare, si consulta e condivide opinioni sugli argomenti trattati.

In Atos, la protezione dei dati si fonda sulla policy del Gruppo per la protezione dei dati. Nella policy sono illustrati i principi della protezione dei dati ed i processi che riguardano i diritti delle persone interessate, i controlli, la formazione e la sensibilizzazione. La policy fa riferimento alla policy globale per la sicurezza delle informazioni con i suoi ulteriori regolamenti.

L'ufficio per la protezione dei dati mette a disposizione dei documenti predefiniti nell'Atos Integrated Management System (AIMS), come moduli, elenchi di controllo, manuali e istruzioni di lavoro che vengono utilizzati nei processi aziendali e delle risorse umane (HR). Tutti i dipendenti si impegnano alla segretezza dei dati e al mantenimento dei segreti commerciali e aziendali e dipendono dal GDPR - Articoli 29 e 32 (4) – per trattare i dati personali solo in base alle istruzioni impartite dal titolare del trattamento. Inoltre, sono tenuti a rispettare la Legge [tedesca] sulle telecomunicazioni (Articolo 88) e, se del caso, a tutelare i segreti sociali e/o bancari.

Nel corso di sessioni di formazione obbligatorie che si svolgono ogni anno, i dipendenti Atos sono tenuti ad aggiornare la loro consapevolezza sulla privacy.

Le misure tecniche e organizzative per la protezione dei dati in conformità all'Articolo 32 del GDPR vengono sottoposte a revisioni regolari nell'ambito della certificazione ISO e degli audit ISAE3402. Inoltre, nel corso delle verifiche interne dei processi vengono esaminate anche questioni che riguardano la protezione dei dati.

Gestione di rischi e sicurezza

Atos organizza i propri servizi sulla base di un sistema per la gestione della sicurezza. Questo sistema comprende, tra l'altro, linee guida documentate e linee guida per il funzionamento di IT / Data Center. Queste linee guida si fondano su regolamenti sia elaborati internamente che previsti dalla legge. I processi per la sicurezza sono sottoposti a controlli periodici. Le linee guida sono vincolanti anche per i Subappaltatori. Ogni anno, per i dipendenti Atos sono previste delle sessioni di formazione obbligatorie sulla consapevolezza della sicurezza.

Atos ha adottato un processo per la gestione dei rischi che interessa tutti i livelli della società ed ha nominato dei responsabili della gestione dei rischi a vari livelli dell'organizzazione per garantire l'attuazione della gestione dei rischi.

I processi per la gestione dei rischi sono suddivisi in gestione dei rischi operativi, che interessa proposte, contratti (dal trasferimento del servizio ad Atos o dall'inizio del progetto fino al suo completamento o alla conclusione del servizio) ed area operativa, vale a dire i relativi processi, servizi e sedi.

I rischi, la loro valutazione e il follow-up delle misure definite sono documentati in registri dei rischi che vengono esaminati e aggiornati periodicamente dai responsabili, con il coinvolgimento del responsabile della gestione dei rischi e degli esperti competenti. I controlli sono definiti e documentati per tutti i rischi inerenti all'attività. Per ciascuno di essi, vengono predisposte delle verifiche per controllarne regolarmente l'efficacia.

Certificazione

Le società Atos tedesche sono certificate in base a

- DIN EN ISO 9001: 2015 (Gestione qualità)

- ISO / IEC 27001: 2013 (Gestione della sicurezza delle informazioni)
- ISO / IEC 20000-1: 2011 (Gestone dei servizi IT)

da parte di Ernst & Young CertifyPoint B.V.

Al momento, nelle società Unify, questo processo è in fase di attivazione.

Gestione della risposta ad un evento imprevisto

Atos si occupa degli eventi che interessano la sicurezza utilizzando procedure operative standard e processi basati su strumenti fondati sulla "ITIL Best Practice", al fine di ripristinare quanto prima un funzionamento senza problemi. Gli incidenti che riguardano la sicurezza sono monitorati ed analizzati tempestivamente dall'organizzazione di Atos per la gestione della sicurezza. In funzione della natura dell'evento, al processo parteciperanno gli specialisti e i team di assistenza necessari e competenti, compreso il "Computer Security Incident Response Team" (CSIRT) di Atos. Al momento, nelle società Unify, questa Gestione della risposta ad un evento imprevisto è in fase di attivazione.

Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (Art. 25 Sezione 2 del GDPR)

In Atos la protezione dei dati viene presa in considerazione nel più breve tempo possibile utilizzando dei set di impostazioni compatibili con la protezione dei dati ("Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita") per evitare il trattamento illecito o l'uso improprio dei dati. Con l'adozione di set di impostazioni tecniche adeguati si intende garantire la raccolta e il trattamento solo dei Dati personali che sono effettivamente necessari per una finalità specifica (Principio della minimizzazione dei dati).

I valori predefiniti per la protezione dei dati fin dalla progettazione e per la protezione per impostazione predefinita sono definiti nella Linea Guida e nella Policy di Atos per la codifica sicura.

Per ottenere un trattamento dei dati personali a basso rischio, si adottano, tra l'altro, le seguenti misure protettive:

- Ridurre al minimo la quantità di dati personali
- Eseguire la pseudo anonimizzazione o la crittografia dei dati quanto prima possibile
- Creare trasparenza in relazione alle procedure e al trattamento di dati
- Cancellare o rendere anonimi i dati quanto prima possibile
- Ridurre al minimo l'accesso ai dati
- Stabilire in anticipo le opzioni di configurazione esistenti sui valori più adatti alla privacy
- Documentare la valutazione dei rischi alle persone interessate