Requirement	Requirement ID	Control	Control ID	Specification	Versione italiana	CSP is Data Controller	CSP is Data Processor	Additional sector specific requirements	Additional specification on national level	Consensus Assessment Answers "Please specify how do you achieve compliance to each requirement"
1. CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY.	**DCA**	**1. Declaration of compliance and accountability**	**DCA-1.1**	*1. Declare and ensure to comply with the applicable EU data protection law and with the terms of this Code of Conduct, also with respect to technical and organisational security measures, and to safeguard the protection of the rights of the data subject. Where there is a material change in applicable EU data protection law which may imply new or conflicting obligations regarding the terms of this Code of Conduct, the CSP commits to complying with the terms of the applicable EU data protection law.*	*Dichiarare e assicurare il rispetto della legge sulla protezione dei dati dell'UE applicabile e dei termini del presente Codice di condotta, anche in relazione alle misure di sicurezza tecniche e organizzative, e salvaguardare la tutela dei diritti dell'interessato. Laddove vi sia un cambiamento sostanziale nella normativa applicabile in materia di protezione dei dati dell'UE che potrebbe comportare obblighi nuovi o in conflitto in relazione ai termini del presente codice di condotta, il CSP si impegna a rispettare i termini della normativa sulla protezione dei dati dell'UE applicabile.*	Applicable	Applicable		Comply with REG UE 2016/679 and Dlgs 196/03 smi	L'Azienda ha implementato un modello gi gestione dei processi privacy, comprensivo di ruoli e responsabilità per ciascuna attività mandatoria, nel rispetto dei requisiti GDPR.
			DCA-1.2	*2. Declare and ensure to be able to demonstrate compliance with the applicable EU data protection law and with the terms of this Code of Conduct (accountability).*	*Dichiarare e garantire di essere in grado di dimostrare la conformità con la normativa sulla protezione dei dati dell'UE applicabile e con i termini del presente Codice di condotta (responsabilità).*	Applicable	Applicable		Comply with REG UE 2016/679 and Dlgs 196/03 smi	Tutte le procedure del modello di gestione sono state formalizzate e comunicate al personale aziendale
			DCA-1.3	*3. Describe what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its subcontractors (see also Controls no. WWP-3.1 to 3.5, below) or business associates, with the applicable EU data protection law and with the Terms of this Code of Conduct.*	*Descrivere quali politiche e procedure sono state implementate dal CSP per garantire e dimostrare la conformità da parte del CSP stesso e dei suoi subappaltatori (vedere anche Controls n ° da WWP-3.1 a 3.5, di seguito) o business associate, con la normativa applicabile sulla protezione dei dati dell'UE e con Termini del presente Codice di condotta.*	Applicable	Applicable			Tutte le procedure del modello di gestione, formalizzate e comunicate al personale aziendale, sono disponibili nella intranet aziendale. Sono altresì presenti e disponibili le procedure ISO27001 ed ISO 9001.
			DCA-1.4	*4. Identify the elements that can be produced as evidence to demonstrate such compliance. Evidence elements can take different forms, such as self-certification/attestation, third-party audits (e.g. certifications, attestations, and seals), logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the following levels:* *(i) organisational policies level to demonstrate that policies are correct and appropriate;* *(ii) IT controls level, to demonstrate that appropriate controls have been deployed; and* *(iii) operations level, to demonstrate that systems are behaving (or not) as planned.* *Examples of evidence elements pertaining to different levels are data protection certifications, seals and marks.*	*Identificare gli elementi che possono essere prodotti come prova per dimostrare tale conformità. Gli elementi di prova possono assumere forme diverse, come autocertificazione / attestazione, audit di terze parti (ad esempio certificazioni, attestati e sigilli), registri, tracce di controllo, registrazioni di manutenzione del sistema, o più rapporti di sistema generali e prove documentali di tutte le operazioni di elaborazione sotto la sua responsabilità. Questi elementi devono essere forniti ai seguenti livelli:* *(i) livello di politiche organizzative per dimostrare che le politiche sono corrette e appropriate;* *(ii) livello di controlli IT, per dimostrare che sono stati implementati controlli appropriati; e* *(iii) livello operativo, per dimostrare che i sistemi si stanno comportando (o meno) come pianificato.* *Esempi di elementi di prova relativi a diversi livelli sono le certificazioni, i sigilli ei marchi di protezione dei dati.*	Applicable	Applicable			Tutte le procedure del modello di gestione, formalizzate e comunicate al personale aziendale, sono disponibili nella intranet aziendale. Sono altresì presenti e disponibili le procedure ISO27001 ed ISO 9001. Sono disponibili i certificati ISO ed i verbali di audit GDPR di seconda parte e interni;
2. CSP RELEVANT CONTACTS AND ITS ROLE.	**CAR**	**1. CSP relevant contacts and its role**	**CAR-1.1**	*1. Specify CSP's identity and contact details (e.g., name, address, email address, telephone number and place of establishment);*	*Specificare l'identità e i dettagli di contatto di CSP (ad es. Nome, indirizzo, indirizzo e-mail, numero di telefono e luogo di stabilimento);*	Applicable	Applicable			Data Management S.r.L., P.zza S.Andrea dela Valle 6 - 00186 -Roma - Italia - Roberto Macciò - roberto.maccio@datamanagement.it - +39 06972721
			CAR-1.2	*2. Specify the identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of the CSP's local representative(s) (e.g. a local representative in the EU);*	*Specificare l'identità e i dettagli di contatto (ad es. Nome, indirizzo, indirizzo e-mail, numero di telefono e luogo di stabilimento) dei rappresentanti locali del CSP (ad esempio un rappresentante locale nell'UE);*	Applicable	Applicable			Na
			CAR-1.3	*3. Specify the CSP's data protection role for each of the relevant processing activities inherent to the services (i.e., controller, joint-controller, processor or subprocessor);*	*Specificare il ruolo di protezione dei dati di CSP per ciascuna delle attività di elaborazione pertinenti inerenti ai servizi (ad esempio, titolare, titolare congiunto, responsabile o subresponsabile);*	Applicable	Applicable			Responsabile o Sub Responsabile
			CAR-1.4	*4. Specify the contact details of the CSP's Data Protection Officer (DPO) or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests;*	*Specificare i dettagli di contatto del Responsabile della protezione dei dati del CSP (DPO) o, in assenza di DPO, i dettagli di contatto della persona responsabile della privacy a cui il cliente può indirizzare le richieste*	Applicable	Applicable			Data Management S.r.L., P.zza S.Andrea dela Valle 6 - 00186 -Roma - Italia - Gaia Cingolani - dpo@datamanagement.it - +39 06972721 - +39 3452624962
			CAR-1.5	*5. Specify the contact details of the CSP's Information Security Officer (ISO) or, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests.*	*Specificare i dettagli di contatto del responsabile della sicurezza delle informazioni del CSP (ISO) o, in assenza di ISO, i dettagli di contatto della persona responsabile delle questioni di sicurezza a cui il cliente può indirizzare le richieste*	Applicable	Applicable			Data Management S.r.L., P.zza S.Andrea dela Valle 6 - 00186 -Roma - Italia - Roberto Macciò - roberto.maccio@datamanagement.it - +39 010 8173762 - +39 348 2830018

3. WAYS IN WHICH THE DATA WILL BE PROCESSED.	**WWP**	**1. General Information**	**WWP-1.1**	*CSPs that are **controllers** must provide details to cloud customers regarding:* *1. categories of personal data concerned in the processing;*		Applicable	Not Applicable			
			WWP-1.2	*2. purposes of the processing for which data are intended and the necessary legal basis to carry out such processing in a lawful way;*		Applicable	Not Applicable			
			WWP-1.3	*3. recipients or categories of recipients of the data;*		Applicable	Not Applicable			
			WWP-1.4	*4. existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability;*		Applicable	Not Applicable			
			WWP-1.5	*5. where applicable, the fact that the CSP intends to transfer personal data to a third country or international organisation and the absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;*		Applicable	Not Applicable			
			WWP-1.6	*6. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*		Applicable	Not Applicable			
			WWP-1.7	*7. where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*		Applicable	Not Applicable			
			WWP-1.8	*8. the right to lodge a complaint with a supervisory authority (as defined in Article 4 (21) GDPR);*		Applicable	Not Applicable			
			WWP-1.9	*9. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;*		Applicable	Not Applicable			
			WWP-1.10	*10. the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;*		Applicable	Not Applicable			
			WWP-1.11	*11. where the CSP intends to further process the personal data for a purpose other than that for which the personal data is being collected, information on that other purpose, prior to the relevant further processing;*		Applicable	Not Applicable			
			WWP-1.12	*12. where personal data has not been obtained from the data subject, from which source the personal data originated, and if applicable, whether the data came from publicly accessible sources;*		Applicable	Not Applicable			
			WWP-1.13	*13. activities that are conducted to provide the agreed cloud service(s) (e.g., data storage), activities conducted at the customer's request (e.g., report production) and those conducted at the CSP's initiative (e.g., backup, disaster recovery, fraud monitoring).*		Applicable	Not Applicable			
			WWP-1.14	*CSPs that are **processors** must provide to cloud customers details on:* *14. the extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor (General Information - applicable to CSPs that are processors).*	*CSP che sono fornitori devono fornire ai clienti del cloud dettagli su:* *la portata e le modalità con cui il responsabile del trattamento dei dati del cliente può impartire le istruzioni vincolanti al CSP-elaboratore di dati (Informazioni generali - applicabili ai CSP che sono processori).*		Applicable			Sono definite contrattualmente nella nomina a responsabile del trattamento dati e in tutta la documentazione a corredo della fornitura
			WWP-1.15	*15. Specify how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors)*	*Specificare in che modo i clienti del cloud saranno informati sulle modifiche rilevanti relative ai servizi cloud pertinenti, quali l'implementazione o la rimozione di funzioni (Informazioni generali - applicabili a CSP sia controller che CSP che sono processori)*	Applicable	Applicable			Le informazioni ai titolari saranno dati nel processo di comunicazione che viene gestito per ogni aggiornamento dei prodotti oppure con un'apposita comunicazione scritta, inviata al titolare, qualora la modifica riguardi solo lui nello specifico
		2 Personal data location	**WWP-2.1**	*1. Specify the location(s) of all data centres or other data processing locations (by country) where personal data may be processed, and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means).*	*Specificare l'ubicazione / i di tutti i centri dati o altri luoghi di elaborazione dei dati (per paese) dove possono essere elaborati i dati personali, in particolare, dove e come i dati possono essere archiviati, copiati, sottoposti a backup e ripristinati (questo può includere sia mezzi digitali e non digitali).*	Applicable	Applicable			I dati sono trattati esclusivamente in Italia

			WWP-2.2	*2. Notify cloud customers of any intended changes to these locations once a contract has been entered into, in order to allow the cloud customer to acknowledge or object.*	*Informare i clienti del cloud di eventuali modifiche previste a queste posizioni una volta che è stato inserito un contratto, in modo da consentire al cliente cloud di riconoscere o opporsi.*	Applicable	Applicable			Ogni modifica viene comunicata al cliente e convenuta contrattualmente con lo stesso
			WWP-2.3	*3. Allow cloud customers to terminate the contract in the event that an objection cannot be satisfactorily resolved between the CSP and the cloud customer, and afford the cloud customer sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract).*	*Consentire ai clienti del cloud di risolvere il contratto nel caso in cui un'obiezione non possa essere risolta in modo soddisfacente tra il CSP e il cliente del cloud e offrire al cliente del cloud tempo sufficiente per procurarsi un CSP o una soluzione alternativa (stabilendo un periodo di transizione durante il quale un accordo a livello di servizi continueranno a essere forniti al cliente cloud, in base al*	Applicable	Applicable			Il Titolare ha sempre il diritto di recedere qualora non sia d'accordo con la modifica
		3 Subcontractors	WWP-3.1	*1. Identify subcontractors and subprocessors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled.*	*Identificare i subappaltatori e i subresponsabili che partecipano all'elaborazione dei dati, insieme alla catena di responsabilità e responsabilità utilizzate per garantire il rispetto dei requisiti di protezione dei dati.*	Applicable	Applicable			Qualora siano previste subforniture, queste sono comunicate al cliente preventivamente e, se autorizzate, vengono formalmente redatte nomine a subresponsabile da parte del Responsabile stesso che controlla e garantisce la catena di accountability verso il titolare.
			WWP-3.2	*2. Declare to cloud customers and further ensure that the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer.*	*Dichiarare ai clienti del cloud e assicurarsi inoltre che il CSP non coinvolga un altro processore senza previa autorizzazione scritta specifica o generale del cliente cloud.*	Not Applicable	Applicable			Qualora siano previste subforniture, queste sono comunicate al cliente preventivamente e, se autorizzate, vengono formalmente redatte nomine a subresponsabile da parte del Responsabile stesso che controlla e garantisce la catena di accountabiity verso il titolare.
			WWP-3.3	*3. Declare to cloud customers and further ensure that the CSP imposes on other processors the same data protection obligations stipulated between the CSP and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU applicable law;*	*Dichiarare ai clienti cloud e garantire inoltre che il CSP imponga ad altri responsabili gli stessi obblighi di protezione dei dati stipulati tra il CSP e il cliente del cloud, mediante un contratto (o altro atto giuridico vincolante), in particolare fornendo garanzie sufficienti per attuare gli opportuni e misure organizzative in modo tale che il trattamento soddisfi i requisiti della legge applicabile dell'UE;*	Not Applicable	Applicable			Il Responsabile controlla e garantisce tutta la catena di accountability (comprensiva di eventuali subforniture) verso il titolare.
			WWP-3.4	*4. Declare to cloud customers and futher ensure that the CSP remains fully liable to the cloud customer for the performance of other processors' obligations, in case the other processors fail to fulfil their data protection obligations.*	*Dichiarare ai clienti del cloud e inoltre assicurarsi che il CSP rimanga pienamente responsabile nei confronti del cliente del cloud per l'adempimento degli obblighi degli altri processori, nel caso in cui gli altri processori non rispettino i propri obblighi di protezione dei dati.*	Not Applicable	Applicable			Il Responsabile controlla e garantisce tutta la catena di accountability (comprensiva di eventuali subforniture) verso il titolare.
			WWP-3.5	*5. Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or subprocessors with customers retaining at all times the possibility to object to such changes or terminate the contract. In the event of termination by the cloud customer, the cloud customer must be afforded sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract).*	*Identificare le procedure utilizzate per informare il cliente del cloud di eventuali modifiche previste relative all'aggiunta o alla sostituzione di subappaltatori o subprocessori con i clienti che mantengono in qualsiasi momento la possibilità di opporsi a tali modifiche o risolvere il contratto. In caso di risoluzione da parte del cliente del cloud, al cliente del cloud deve essere concesso tempo sufficiente per procurarsi un CSP o una soluzione alternativa (stabilendo un periodo di transizione durante il quale continuerà a essere fornito al cliente cloud un livello concordato di servizi, sotto contratto).*	Applicable	Applicable			Qualora siano previste subforniture, queste sono comunicate al cliente preventivamente e, se autorizzate, vengono formalmente redatte nomine a subresponsabile da parte del Responsabile stesso che controlla e garantisce la catena di accountabiity verso il titolare.
		4 Installation of software on cloud customer's system	WWP-4.1	*1. Indicate to cloud customers whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins).*	*Indicare ai clienti del cloud se la fornitura del servizio richiede l'installazione di software sul sistema del cliente cloud (ad es. Plug-in del browser).*	Applicable	Applicable			Le specifiche tecniche sono indicate nel contratto
			WWP-4.2	*2. Indicate to cloud customers the software's implications from a data protection and data security point of view.*	*Indicare ai clienti del cloud le implicazioni del software dal punto di vista della protezione dei dati e della sicurezza dei dati.*	Applicable	Applicable			Le specifiche tecniche e le relative implicazioni legali (GDPR) sono indicate nel contratto
		5 Data processing contract (or other binding legal act)	WWP-5.1	*1. Share with the cloud customers the model data processing contract (or other binding legal act) which will govern the processing carried out by the CSP on behalf of the cloud customer and set out the subject matter and duration of the processing, the type of personal data and categories of data subjects and the obligations and rights of the cloud customer.*	*Condividere con i clienti del cloud il modello di contratto di elaborazione dei dati (o altro atto legale vincolante) che disciplinerà il trattamento eseguito dal CSP per conto del cliente cloud e definirà l'oggetto e la durata del trattamento, il tipo di dati personali e categorie di soggetti dei dati e gli obblighi e i diritti del cliente cloud*	Not Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura.

			WWP-5.2	*The contract or other legal act stipulates, that the CSP will do the following:* *2. process personal data only upon documented instructions from the cloud customer, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the CSP is subject; in such a case, the CSP will inform the cloud customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*	*Il contratto o altro atto legale stabilisce che il CSP farà quanto segue:* *elaborare i dati personali solo su istruzioni documentate del cliente cloud, anche per quanto riguarda i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, a meno che ciò non sia richiesto dal diritto dell'Unione o dello Stato membro a cui è soggetto il CSP; in tal caso, il CSP informerà il cliente del cloud di tale requisito legale prima dell'elaborazione, a meno che tale legge non vieti tali informazioni per importanti motivi di pubblico interesse;*	Not Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura.
			WWP-5.3	*3. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they do not process personal data except upon instructions from the cloud customer, unless otherwise required by Union or Member State law;*	*garantire che le persone autorizzate a trattare i dati personali si siano impegnate a rispettare la riservatezza o siano soggette ad un obbligo statutario di riservatezza e che non trattino i dati personali se non dietro istruzioni del cliente del cloud, a meno che non sia diversamente previsto dalla legislazione dell'Unione o degli Stati membri;*	Not Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura.
			WWP-5.4	*4. implement all technical and organizational security measures which the CSP deems adequate, in light of the available technology, the state of the art, the costs in implementing those measures and the processing activities inherent to the services provided, to ensure that the CSP's services are covered by a level of security which is appropriate, considering the potential risks to the interests, rights and freedoms of data subjects;*	*attuare tutte le misure di sicurezza tecniche e organizzative che il CSP ritiene adeguati, alla luce della tecnologia disponibile, dello stato dell'arte, dei costi di attuazione di tali misure e delle attività di trattamento inerenti ai servizi forniti, per garantire che i servizi del CSP siano coperti da un livello di sicurezza appropriato, considerando i potenziali rischi per gli interessi, i diritti e le libertà degli interessati;*	Not Applicable	Applicable			
			WWP-5.5	*5. Respect the conditions for engaging another processor (see Controls no. WWP-3.1 to 3.5, above).*	*Rispettare le condizioni per l'attivazione di un altro Responsabile (vedere Comandi n. Da WWP-3.1 a 3.5, sopra).*	Not Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura.
			WWP-5.6	*6. taking into account the nature of the processing, assist the cloud customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the cloud customer's obligation to respond to requests for exercising the data subject's rights;*	*tenendo conto della natura del trattamento, assiste il cliente del cloud con adeguate misure tecniche e organizzative, nella misura del possibile, per l'adempimento dell'obbligo del cliente cloud di rispondere alle richieste di esercizio dei diritti dell'interessato;*	Not Applicable	Applicable			
			WWP-5.7	*7. assist the cloud customer in ensuring compliance with obligations related to security of processing, notification of a personal data breach to the supervisory authority; communication of a personal data breach to the data subject, and data protection impact assessment; taking into account the nature of processing and the information available to the processor;*		Not Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura.
			WWP-5.8	*8. at the choice of the cloud customer, delete or return all personal data to customer after end of the provision of services relating to processing; and delete existing copies unless Union or Member State law requires storage of the personal data (see Controls no. RRD-1.1 to 4.5, below).*	*su specifica scelta del cliente cloud, cancellare o restituire tutti i dati personali al cliente dopo la fine della fornitura di servizi relativi all'elaborazione; ed eliminare le copie esistenti a meno che la legislazione dell'Unione o degli Stati membri richieda la memorizzazione dei dati personali (vedere i Contr. da RRD-1.1 a 4.5, di seguito).*	Not Applicable	Applicable			
			WWP-5.9	*9. make available to the cloud customer all information necessary to demonstrate compliance with relevant data protection obligations; and allow for and contribute to audits, including inspections, conducted by the cloud customer or another auditor mandated by the customer.*	*mettere a disposizione del cliente del cloud tutte le informazioni necessarie a dimostrare la conformità con gli obblighi relativi alla protezione dei dati; e consentire e contribuire a verifiche, comprese le ispezioni, condotte dal cliente cloud o da un altro revisore incaricato dal cliente.*	Not Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura.
4. RECORDKEEPING.	**REC**	**1.Recordkeeping for CSP-controller**	**REC-1.1**	*1. CSP controller confirms to cloud customers and commits to maintain a* ***record*** *of processing activities under CSP responsibility and make it available to the supervisory authority on request.*		Applicable	Not Applicable			NA
			REC-1.2	*Record contains:* *2. name and contact details of controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*		Applicable	Not Applicable			
			REC-1.3	*3. the purposes of the processing;*		Applicable	Not Applicable			
			REC-1.4	*4. a description of the categories of data subjects and of the categories of personal data;*		Applicable	Not Applicable			
			REC-1.5	*5. categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;*		Applicable	Not Applicable			

			REC-1.6	*6. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;*		Applicable	Not Applicable			
			REC-1.7	*7. where possible, the envisaged time limits for erasure of different categories of data or, if that is not possible, the criteria used to determine that period;*		Applicable	Not Applicable			
			REC-1.8	*8. a description of technical and organisational security measures in place (see also Controls no. SEC-1.1 to 1.3.xxvii, below).*		Applicable	Not Applicable			
		2 Recordkeeping for CSP-processor	REC-2.1	*1. CSP processor confirms to cloud customers and commits to maintain a record of all categories of processing activities carried out on behalf of a controller and make it available to the supervisory authority upon request.*	*Il Responsabile prepara per i clienti del cloud e si impegna a mantenere un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare e a renderlo disponibile all'autorità di vigilanza su richiesta.*	Not Applicable	Applicable			Sono censite tutte le attività di trattamento per Cliente e sono stati creati specifici registri disponibili su richiesta.
			REC-2.2	*Record contains:* *2. name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;*	*I registri contengono:* *nome e dati di contatto del processore o dei responsabili del trattamento e di ciascun responsabile del trattamento per conto del quale agisce il responsabile del trattamento e, se del caso, del responsabile del trattamento o del responsabile del trattamento e del responsabile della protezione dei dati;*	Not Applicable	Applicable			Sono censite tutte le attività di trattamento per Cliente, comprensive di tutti i requisiti GDPR previsti, e sono stati creati specifici registri disponibili su richiesta.
			REC-2.3	*3. categories of processing carried out on behalf of each controller;*	*categorie di trattamento effettuate per conto di ciascun responsabile del trattamento*	Not Applicable	Applicable			
			REC-2.4	*4. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;*	*se del caso, trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione di tale paese terzo o organizzazione internazionale e la documentazione di adeguate salvaguardie;*	Not Applicable	Applicable			Sono censite tutte le attività di trattamento per Cliente, comprensive di tutti i requisiti GDPR previsti, e sono stati creati specifici registri disponibili su richiesta.
			REC-2.5	*5. a description of technical and organisational security measures in place (see also Controls no. SEC-1.1 to 1.3.xxvii, below).*	*una descrizione delle misure di sicurezza tecniche e organizzative in essere (vedere anche i Contr. n. da SEC-1.1 a 1.3.xxvii, di seguito).*	Not Applicable	Applicable			Sono censite tutte le attività di trattamento per Cliente, comprensive di tutti i requisiti GDPR previsti, e sono stati creati specifici registri disponibili su richiesta.
5. DATA TRANSFER.	**DTR**	**1. Data transfer**	**DTR-1-1**	*1. Clearly indicate whether data is to be transferred, backed up and/or recovered across borders, in the regular course of operations or in an emergency.*	*Indicare chiaramente se i dati devono essere trasferiti, copiati e / o recuperati attraverso i confini, nel corso regolare delle operazioni o in caso di emergenza.*	Applicable	Applicable			Al momento non sono previsti casi di questo tipo
			DTR-1-2	*If transfer restricted under applicable EU law:* *2. Clearly identify the legal ground for the transfer (including onward transfers through several layers of subcontractors), e.g., European Commission adequacy decision, model contracts/standard data protection clauses, approved codes of conduct or certification mechanisms, binding corporate rules (BCRs), and Privacy Shield.*	*Se il trasferimento è limitato ai sensi della normativa UE applicabile:* *Identificare chiaramente la base legale per il trasferimento (compresi i trasferimenti successivi attraverso diversi livelli di subappaltatori), ad esempio, decisione sull'adeguatezza della Commissione europea, contratti tipo / clausole standard sulla protezione dei dati, codici di condotta o meccanismi di certificazione approvati, norme aziendali vincolanti (BCR) e Scudo di privacy.*	Applicable	Applicable			Al momento non sono previsti casi di questo tipo
6. DATA SECURITY MEASURES.	**SEC**	**1. Data security measures**	**SEC-1.1**	*1. Specify to cloud customers the technical, physical and organisational measures that are in place to protect personal data against accidental or unlawful destruction; or accidental loss, alteration, unauthorized use, unauthorised modification, disclosure or access; and against all other unlawful forms of processing;*	*Specificare ai clienti del cloud le misure tecniche, fisiche e organizzative in vigore per proteggere i dati personali dalla distruzione accidentale o illecita; o perdita accidentale, alterazione, uso non autorizzato, modifica non autorizzata, divulgazione o accesso; e contro tutte le altre forme illecite di elaborazione;*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento.
			SEC-1.2	*2. Describe to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) to ensure the following safeguards:*	*Descrivere ai clienti del cloud le misure tecniche, fisiche e organizzative concrete (protettive, investigative e correttive) per garantire le seguenti salvaguardie*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento.
			SEC-1.2.i	*(i) availability - processes and measures in place to manage risk of disruption and to prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup, restore mechanisms and patch management;*	*disponibilità: processi e misure per gestire il rischio di interruzioni e prevenire, rilevare e reagire agli incidenti, come i collegamenti di rete Internet di backup, lo storage ridondante e il backup dei dati efficace, i meccanismi di ripristino e la gestione delle patch;*	Applicable	Applicable			

		SEC-1.2.ii	*(ii) integrity: - methods by which the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures, error-correction, hashing, hardware radiation/ionization protection, physical access/compromise/destruction, software bugs, design flaws and human error, etc.);*	*integrità: - metodi con i quali il CSP garantisce l'integrità (ad esempio, rilevamento di alterazioni ai dati personali mediante meccanismi crittografici come codici di autenticazione dei messaggi o firme, correzione degli errori, hashing, protezione da radiazioni / ionizzazione hardware, accesso / compromissione / distruzione fisica, bug del software , difetti di progettazione e errore umano, ecc.);*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento.
		SEC-1.2.iii	*(iii) confidentiality - methods by which the CSP ensures confidentiality from a technical point of view in order to assure that only authorised persons have access to data; including, inter alia as appropriate, pseudonymisation and encryption of personal data 'in transit' and 'at rest,' authorisation mechanism and strong authentication; and from a contractual point of view, such as confidentiality agreements, confidentiality clauses, company policies and procedures binding upon the CSP and any of its employees (full time, part time and contract employees), and subcontractors who may be able to access data;*	*riservatezza: metodi con i quali il CSP garantisce la riservatezza da un punto di vista tecnico al fine di garantire che solo le persone autorizzate abbiano accesso ai dati; tra cui, tra l'altro, la pseudonimizzazione e la crittografia dei dati personali "in transito" e "a riposo", meccanismo di autorizzazione e autenticazione forte; e da un punto di vista contrattuale, come accordi di riservatezza, clausole di riservatezza, politiche aziendali e procedure vincolanti per il CSP e qualsiasi dei suoi dipendenti (a tempo pieno, a tempo parziale e dipendenti a contratto) e subappaltatori che potrebbero essere in grado di accedere ai dati;*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento.
		SEC-1.2.iv	*(iv) transparency - technical, physical and organisational measures the CSP has in place to support transparency and to allow review by customers (see, e.g., Control no. MON-1.1, below);*	*trasparenza: misure tecniche, fisiche e organizzative implementate dal CSP per supportare la trasparenza e consentire la revisione da parte dei clienti (vedere, ad esempio, Controllo n. MON-1.1, di seguito);*	Applicable	Applicable			
		SEC-1.2.v	*(v) isolation (purpose limitation) - How the CSP provides appropriate isolation to personal data (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on the "least privilege" principle; hardening of hypervisors; and proper management of shared resources wherever virtual machines are used to share physical resources among cloud customers);*	*isolamento (limitazione delle finalità) - Come il CSP fornisce un appropriato isolamento ai dati personali (ad esempio, un'adeguata governance dei diritti e ruoli per l'accesso ai dati personali (revisionati su base regolare), la gestione degli accessi basata sul principio del "minimo privilegio"; hypervisor e corretta gestione delle risorse condivise ovunque vengano utilizzate macchine virtuali per condividere le risorse fisiche tra i clienti del cloud*	Applicable	Applicable			
		SEC-1.2.vi	*(vi) intervenability - methods by which the CSP enables data subjects' rights of access, rectification, erasure ('right to be forgotten'), blocking, objection, restriction of processing (see Control no. ROP-1.1, below), portability (see Controls no. PMT-1.1 to 1.2, below) in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further processed by subcontractors (this is also relevant for Section 9, 'Data portability, migration, and transfer back');*	*accesso ai dati - metodi con i quali il CSP consente ai soggetti interessati diritti di accesso, rettifica, cancellazione ("diritto all'oblio"), blocco, opposizione, restrizione dell'elaborazione (cfr. Controllo ROP-1.1, di seguito), portabilità (vedi Controlli da PMT-1.1 a 1.2, di seguito) al fine di dimostrare l'assenza di ostacoli tecnici e organizzativi a questi requisiti, compresi i casi in cui i dati vengono ulteriormente elaborati dai subappaltatori (questo è anche rilevante per la Sezione 9, "Portabilità dei dati, migrazione e trasferimento indietro ');*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento.
		SEC-1.2.vii	*(vii) portability - refer to Controls no. PMT-1.1 to 1.2, below;*	*Portabilità*	Applicable	Applicable			Misure di sicurezza applicabili ex GDPR
		SEC-1.2.viii	*(viii) accountability: refer to Controls no. DCA-1.1 to 1.4, above.*	*Accountability*	Applicable	Applicable			Misure di sicurezza applicabili ex GDPR
		SEC-1.3	*3. As a minimum acceptable baseline, this CoC requires CSPs to comply with the controls set out in ENISA's Technical Guidelines for the implementation of minimum security measures for Digital Service Providers; for each control, the tables on sophistication levels regarding security measures provided in the ENISA's Technical Guidelines will apply, and the CSP must indicate the appropriate sophistication level complied with per each control (1 to 3), taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.* *It shall be noted that not all the minimum security measures listed in the ENISA's Technical Guidelines are directly applicable to all the CSPs. For instance, the requirements SO08 or SO09 cannot be directly implemented by a PaaS or SaaS provider. In any case, if some of the below mentioned security measures cannot be directly implemented by a CSP, the CSP in question shall nonetheless guarantee their implementation through their providers.*	*Come base minima accettabile, questo CoC richiede che i CSP rispettino i controlli stabiliti nelle Linee guida tecniche dell'ENISA per l'attuazione delle misure minime di sicurezza per i fornitori di servizi digitali; per ciascun controllo, si applicheranno le tabelle sui livelli di adeguatezza relativi alle misure di sicurezza fornite nelle Linee guida tecniche dell'ENISA e il CSP deve indicare il livello di sofisticazione appropriato per ciascun controllo (da 1 a 3), tenendo conto dello stato dell'arte, costi di attuazione e natura, portata, contesto e finalità del trattamento, nonché i rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.*	Applicable	Applicable			Misure di sicurezza applicabili ex GDPR (il DPIA è stato redatto su metodologia ENISA)
		SEC-1.3.i	*i. (SO 01) – Information security policy: The CSP establishes and maintains an information security policy. The document details information on main assets and processes, strategic security objectives.*	*Information Security Policy*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)

		SEC-1.3.ii	*ii. (SO 02) – Risk Management: The CSP establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risks management procedures can include (but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools and Risk Assessment (RA) tools etc.*	*Gestione del rischio: il CSP stabilisce e mantiene un quadro appropriato di governance e gestione del rischio, per identificare e affrontare i rischi per la sicurezza dei servizi offerti. Le procedure di gestione dei rischi possono includere (ma non sono limitate a), mantenendo un elenco di rischi e attività, utilizzando strumenti di Governance Risk Management and Compliance (GRC) e strumenti di valutazione del rischio (RA) ecc.*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.iii	*iii. (SO 03) – Security Roles: The CSP assigns appropriate security roles and security responsibilities to designated personnel. (i.e. CSO, CISO, CTO etc.).*	*Ruoli e Responsbailità*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.iv	*iv. (SO 04) – Third party management: The CSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services.*	*Getsione delle terze parti*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.v	*v. (SO 05) – Background checks: The CSP performs appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory framework. Background checks may include checking past jobs, checking professional references, etc.*	*Verifica di profili e competenze*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.vi	*vi. (SO 06) – Security knowledge and training: The CSP verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training. This is achieved through for example, security awareness raising, security education, security training etc.*	*Conoscenza e formazione sulla sicurezza: il CSP verifica e garantisce che il personale disponga di conoscenze sufficienti in materia di sicurezza e che sia dotato di regolare addestramento sulla sicurezza. Ciò si ottiene attraverso, ad esempio, sensibilizzazione alla sicurezza, educazione alla sicurezza, formazione alla sicurezza ecc*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.vii	*vii. (SO 07) – Personnel changes: The CSP establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities.*	*Assunzioni, dimissioni, licenziamenti e cambi mansione: il CSP stabilisce e mantiene un processo appropriato per la gestione dei cambiamenti nel personale o cambiamenti nei ruoli e nelle responsabilità.*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.viii	*viii. (SO 08) – Physical and environmental security: The CSP establishes and maintains policies and measures for physical and environmental security of datacenters such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.*	*Sicurezza fisica*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti dal sistema ISO 27001 e dalla normativa D.Lgs. 81/08 e sono riportati nel DVR.
		SEC-1.3.ix	*ix. (SO 09) – Security of supporting utilities: The CSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.*	*Sicurezza delle dotazioni*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti dal sistema ISO 27001 e dalla normativa D.Lgs. 81/08 e sono riportati nel DVR.
		SEC-1.3.x	*x. (SO 10) – Access control to network and information systems: The CSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.*	*Controllo degli accessi ai sistemi di rete e di informazione: il CSP ha istituito e mantiene politiche e misure appropriate per l'accesso alle risorse aziendali. Ad esempio, modello di affidabilità zero, gestione ID, autenticazione degli utenti, sistemi di controllo degli accessi, firewall e sicurezza di rete, ecc.*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi,).
		SEC-1.3.xi	*xi. (SO 11) – Integrity of network components and information systems: The CSP establishes, protects, and maintains the integrity of its own network, platforms and services by taking steps to prevent successful security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information.*	*Integrità dei componenti di rete e dei sistemi informativi: il CSP stabilisce, protegge e mantiene l'integrità della propria rete, delle proprie piattaforme e servizi adottando misure per prevenire incidenti di sicurezza di successo. L'obiettivo è la protezione da virus, iniezioni di codice e altri malware che possono alterare la funzionalità dei sistemi o l'integrità o l'accessibilità delle informazioni*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi, piano di business continuity e disaster recovery).
		SEC-1.3.xii	*xii. (SO 12) – Operating procedures: The CSP establishes and maintains procedures for the operation of key network and information systems by personnel. (i.e. operating procedures, user manual, administration procedures for critical systems etc.).*	*Procedure operative: il CSP stabilisce e mantiene procedure per il funzionamento dei principali sistemi di rete e di informazione da parte del personale. (cioè procedure operative, manuale utente, procedure amministrative per sistemi critici, ecc.).*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)
		SEC-1.3.xiii	*xiii. (SO 13) – Change management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.*	*Change Management*	Applicable	Applicable			Oltre alla documentazione GDPR molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi)

			SEC-1.3.xiv	*xiv. (SO 14) – Asset management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.*	*Gestione degli asset*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, la gestione degli asset assegnati è descritta nel Sistema ISO 27001.
			SEC-1.3.xv	*xv. (SO 15) – Security incident detection & Response: The CSP establishes and maintains procedures for detecting and responding to security incidents appropriately. These should consider detection, response, mitigation, recovery and remediation from a security incident. Lessons learned should also be adopted by the service provider.*	*Gestione degli incidenti*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi, piano di business continuity e disaster recovery). E' presente una procedura di gestione incidenti di sicurezza ed una specifica per la gestione dei Data Breach
			SEC-1.3.xvi	*xvi. (SO 16) – Security incident reporting: The CSP establishes and maintains appropriate procedures for reporting and communicating about security incidents.*	*Procedure di Escalation nella getsione incidenti*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001 (documentazione, manuale, policy, analisi dei rischi, piano di business continuity e disaster recovery). E' presente una procedura di gestione incidenti di sicurezza ed una specifica per la gestione dei Data Breach
			SEC-1.3.xvii	*xvii. (SO 17) – Business continuity: The CSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered*	*Business Continuity*	Applicable	Applicable			E' presente un piano di BC
			SEC-1.3.xviii	*xviii. (SO 18) – Disaster recovery capabilities: The CSP establishes and maintains an appropriate disaster recovery capability for restoring the offered services in case of natural and/or major disasters*	*Disaster recovery*	Applicable	Applicable			E' presente un piano di DR
			SEC-1.3.xix	*xix. (SO 19) – Monitoring and logging: The CSP establishes and maintains procedures and systems for monitoring and logging of the offered services (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.).*	*Logging & monitoring*	Applicable	Applicable			E' prevista un'attività di tracciamento in linea con i requisiti di legge; per la parte di loggig ADS è presente il sistema centralizzato Balabit.
			SEC-1.3.xx	*xx. (SO 20) – System test: The CSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services*	*Test*	Applicable	Applicable			Soo eseguite attività di test, su base regolare, su sistemi reti e applicazioni
			SEC-1.3.xxi	*xxi. (SO 21) – Security assessments: The CSP establishes and maintains appropriate procedures for performing security assessments of critical assets*	*Verifiche di sicurezza*	Applicable	Applicable			Sono effettuate attività di VA/PT sui diversi ambienti, commissionate ad aziende specializzate
			SEC-1.3.xxii	*xxii. (SO 22) – Compliance: The CSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis*	*Conformità*	Applicable	Applicable			Il presidio della conformità è garantito con la collaborazione di diverse strutture interne
			SEC-1.3.xxiii	*xxiii. (SO 23) – Security of data at rest: The CSP establishes and maintains appropriate mechanisms for the protection of the data at rest*	*Sicurezza dei dati a riposo: il CSP stabilisce e mantiene meccanismi appropriati per la protezione dei dati a riposo*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001.
			SEC-1.3.xxiv	*xxiv. (SO 24) – Interface security: The CSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data*	*Sicurezza delle interfacce*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001.
			SEC-1.3.xxv	*xxv. (SO 25) – Software security: The CSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security*	*Sicurezza del sw*	Applicable	Applicable			Vengono effettuate analisi del codice regolarmente ed ogni sw prima di essere rilasciato viene sottoposto a verifiche di sicurezza. Si sviluppa seguendo le linee guida OWASP ed è stata condotta una specifica analisi in ottica privacy by design e by default, formalizzata in una roadmap di adeguamento fornita ai clienti
			SEC-1.3.xxvi	*xxvi. (SO 26) – Interoperability and portability: The CSP uses standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services*	*Interoperabilità e portabilità*	Applicable	Applicable			Oltre alla documentazione GDPR e al Regolamento Interno, molti task della normativa sono previsti e gestiti nel Sistema ISO 27001.
			SEC-1.3.xxvii	*xxvii. (SO 27) – Customer Monitoring and log access: The CSP grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed*	*Monitoraggio del cliente e accesso al registro di tracciamneto: il CSP garantisce ai clienti l'accesso ai log in modo che i clienti possano indagare su problemi o incidenti di sicurezza quando necessario*	Applicable	Applicable			E' prevista la tenuta e l'aggiornamento di un registro incidenti disponibile su richiesta e per attività di indagine.

7. MONITORING.	**MON**	**1. Monitoring**	**MON-1.1**	*1. Indicate to cloud customers the options that the CSP has in place to allow the customer has to monitor and/or audit in order to ensure appropriate privacy and security measures described in the PLA are met on an on-going basis (e.g., logging, reporting, first- and/or third-party auditing of relevant processing operations performed by the CSP or subcontractors). Any audits carried out which imply that an auditor will have access to personal data stored on the systems used by the CSP to provide the services will require that auditor to accept a confidentiality agreement*	*Indicare ai clienti del cloud le opzioni che il CSP è in grado di consentire al cliente di monitorare e / o audit al fine di garantire che le adeguate misure di privacy e sicurezza descritte nel PLA siano soddisfatte su base continuativa (ad esempio, registrazione, segnalazione , audit di prima e / o di terze parti delle operazioni di elaborazione pertinenti eseguite dal CSP o dai subappaltatori). Qualsiasi audit effettuato che implichi che un revisore avrà accesso ai dati personali memorizzati sui sistemi utilizzati dal CSP per fornire i servizi richiederà che il revisore accetti un accordo di riservatezza*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento.
8. PERSONAL DATA BREACH.	**PDB**	**1. Personal Data Breach**	**PDB-1.1**	*Specify to cloud customers:* *1. how the customer will be informed of personal data breaches affecting the customer's data processed by the CSP and/or its subcontractors, without undue delay and, where feasible, no later than 72 hours from the moment on which the CSP is made aware of the personal data breach in question. A CSP will be considered as "aware" of a personal data breach on the moment that it detects (e.g., directly, or due to a notification received from a subcontractor/sub-processor) an incident which qualifies as a personal data breach and establishes that that incident has affected data processed by the CSP and/or its subcontractors on behalf of a given customer. Should it not be feasible to inform a given customer of a personal data breach within the 72-hour deadline, the CSP will inform that customer of the personal data breach as soon as possible and accompany this communication to the customer with reasons for the delay.*	*Specificare ai clienti cloud:* *in che modo il cliente sarà informato delle violazioni dei dati personali che riguardano i dati del cliente elaborati dal CSP e / o dai suoi subappaltatori, senza indebito ritardo e, ove possibile, non oltre 72 ore dal momento in cui il CSP viene informato del personale violazione dei dati in questione. Un CSP sarà considerato "consapevole" di una violazione dei dati personali nel momento in cui rileva (ad esempio, direttamente o a causa di una notifica ricevuta da un subappaltatore / sub-processore) un incidente che si qualifica come una violazione dei dati personali e stabilisce che tale incidente ha interessato i dati elaborati dal CSP e / o dai suoi subappaltatori per conto di un determinato cliente. Qualora non fosse possibile informare un determinato cliente di una violazione dei dati personali entro il termine di 72 ore, il CSP informerà il cliente della violazione dei dati personali il prima possibile e accompagnerà questa comunicazione con il cliente per i motivi del ritardo.*	Applicable	Applicable			E' previsto un kit documentale per le forniture di servizi Cloud comprensivo di NDA, PLA e requisiti di sicurezza, oltre alle condizioni generali di fornitura. Il Cliente riceve un'informativa sul trattamento dei dati e sulle misure di sicurezza a garanzia delle operazioni di trattamento. All'interno della documentazione è prevista una sezione specifica dedicata alla gestione dei data breach
			PDB-1.2	*Explain to cloud customers the procedures in place to collect and disclose the following information:*	*Requisiti segnalazione data breach*	Applicable	Applicable			Contenuti del Modulo di segnalazione
				2. the nature of the personal data breach including, where possible, the categories and approximate number of personal data records concerned;	*Requisiti segnalazione data breach*					Contenuti del Modulo di segnalazione
			PDB-1.3	*3. the name and contact details of the data protection officer or other contact point where more information can be obtained (see Section 2 'CSP relevant contacts and its role', above);*	*Requisiti segnalazione data breach*	Applicable	Applicable			Contenuti del Modulo di segnalazione
			PDB-1.4	*4. the likely consequences of the personal data breach;*	*Requisiti segnalazione data breach*	Applicable	Applicable			Contenuti del Modulo di segnalazione
			PDB-1.5	*5. the measures taken (or propose to be taken) to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*	*Requisiti segnalazione data breach*	Applicable	Applicable			Contenuti del Modulo di segnalazione
			PDB-1.6	*6. Where it is not feasible to provide all the above information in an initial notification, the CSP must provide as much information to the customer as possible on the reported incident, and provide and further details needed to meet the above requirement as soon as possible (i.e., provision of information in phases).*	*Requisiti segnalazione data breach*	Applicable	Applicable			Contenuti del Modulo di segnalazione
			PDB-1.7	*Specify to cloud customers:*						
				7. how the competent supervisory authority/ies will be informed of personal data security breaches, in less than 72 hours of becoming aware of a personal data breach);		Applicable	Not Applicable			
			PDB-1.8	*8. how data subjects will be informed, without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.*		Applicable	Not Applicable			
9. DATA PORTABILITY, MIGRATION AND TRANSFER BACK.	**PMT**	**1. Data portability, migration and transfer back**	**PMT-1.1**	*Specify to cloud customers:* *1. how the CSP assures data portability, in terms of the capability to transmit personal data in a structured, commonly used, machine-readable and interoperable format:*	*Specificare al cliente cloud:* *come il CSP assicura la portabilità dei dati, in termini di capacità di trasmissione dei dati personali in un formato strutturato, comunemente utilizzato, leggibile da una macchina e interoperabile*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie della portabilità dei dati all'interno del contratto di fornitura

			PMT-1.1.i	*(i) to the cloud customer ('transfer back', e.g., to an in-house IT environment);*	*requisiti di portabilità*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie della portabilità dei dati all'interno del contratto di fornitura
			PMT-1.1.ii	*(ii) directly to the data subjects;*	*requisiti di portabilità*	Applicable	Applicable			
			PMT-1.1.iii	*(iii) to another service provider ('migration'), e.g., by means of download tools or Application Programming Interfaces, or APIs).*	*requisiti di portabilità*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie della portabilità dei dati all'interno del contratto di fornitura
10. RESTRICTION OF PROCESSING.	**ROP**	**1. Restriction of processing**	**ROP-1.1**	*1. Explain to cloud customers how the possibility of restricting the processing of personal data is granted; considering that where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.*	*Spiegare ai clienti del cloud come viene concessa la possibilità di limitare il trattamento dei dati personali; considerando che se il trattamento è stato limitato, tali dati personali, ad eccezione della conservazione, devono essere trattati solo con il consenso dell'interessato o per l'istituzione, l'esercizio o la difesa di rivendicazioni legali, o per la protezione dei diritti di un'altra persona fisica o persona giuridica o per motivi di rilevante interesse pubblico dell'Unione o di uno Stato membro*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie di eventuali trasferimenti dei dati all'interno del contratto di fornitura
11. DATA RETENTION, RESTITUTION AND DELETION.	**RRD**	**1. Data Retention, Restitution and Deletion policies.**	**RRD-1.1**	*1. Describe to cloud customers the CSP's data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated.*	*Descrivere ai clienti del cloud le politiche di conservazione dei dati, le scadenze e le condizioni di conservazione dei dati di CSP per la restituzione dei dati personali o l'eliminazione dei dati una volta terminato il servizio.*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie dei tempi di conservazione e delle modalità di cancellazione dei dati all'interno del contratto di fornitura
			RRD-1.2	*2. Describe to cloud customers CSP's subcontractors data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated.*	*Descrivere ai clienti del cloud le politiche di conservazione dei dati dei subappaltatori di CSP, le tempistiche e le condizioni per la restituzione dei dati personali o l'eliminazione dei dati una volta che il servizio è stato interrotto*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie dei tempi di conservazione e delle modalità di cancellazione dei dati all'interno del contratto di subfornitura
		2. Data Retention	**RRD-2.1**	*1. Indicate and commit to complying with the time period for which the personal data will or may be retained, or if that is not possible, the criteria used to determine such a period.*	*Indicare e impegnarsi a rispettare il periodo per il quale i dati personali saranno conservati o potrebbero essere mantenuti, o se ciò non è possibile, i criteri utilizzati per determinare tale periodo.*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie dei tempi di conservazione e delle modalità di cancellazione dei dati secondo le indicazioni GDPR
			RRD-2.2	*2. Take into consideration the following criteria, when defining retention periods:* *Necessity – Personal data is retained for as long as necessary in order to achieve the purpose for which it was collected, so long as it remains necessary to achieve that purpose (e.g., to perform the services);* *Legal Obligation – Personal data is retained for as long as necessary in order to comply with an applicable legal obligation of retention (e.g., as defined in applicable labour or tax law), for the period of time defined by that obligation;* *Opportunity – Personal data is retained for as long as permitted by the applicable law (e.g., processing based on consent, processing for the purpose of establishing, exercising or defending against legal claims – based on applicable statutes of limitations regarding legal claims related to the performance of the services).*	*Prendi in considerazione i seguenti criteri, quando definisci i periodi di conservazione:* *Necessità: i dati personali vengono conservati per tutto il tempo necessario al fine di raggiungere lo scopo per il quale sono stati raccolti, purché sia necessario per raggiungere tale scopo (ad es. Per eseguire i servizi);* *Obbligo legale - I dati personali vengono conservati per tutto il tempo necessario al fine di ottemperare a un obbligo legale di conservazione applicabile (ad esempio, come definito nella legge sul lavoro o fiscale applicabile), per il periodo di tempo definito da tale obbligo;* *Opportunità: i dati personali vengono conservati per tutto il tempo consentito dalla legge applicabile (ad esempio, elaborazione basata sul consenso, elaborazione allo scopo di stabilire, esercitare o difendersi da rivendicazioni legali) in base alle leggi applicabili in materia di limitazioni relative alle prestazioni dei servizi)*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie dei tempi di conservazione e delle modalità di cancellazione dei dati secondo le indicazioni GDPR
		3. Data retention for compliance with sector-specific legal requirements	**RRD-3.1**	*1. Indicate whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations.*	*Indicare se e in che modo il cliente del cloud può richiedere al CSP di rispettare le leggi e i regolamenti specifici del settore.*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti GDPR in merito alla protezione dei dati
		4. Data restitution and/or deletion	**RRD-4.1**	*1. Indicate the procedure for returning to the cloud customers the personal data in a format allowing data portability (see also Controls no. PMT-1.1 to 1.2, above);*	*Indicare la procedura per restituire ai clienti del cloud i dati personali in un formato che consenta la portabilità dei dati (vedere anche i numeri di controllo da PMT-1.1 a 1.2, sopra);*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie di portabilità dei dati secondo le indicazioni GDPR
			RRD-4.2	*2. the methods available or used to delete data;*	*Modalità di cancellazione*	Applicable	Applicable			Il Fornitore Cloud garantisce la copertura dei requisiti tempi e garanzie di retention e cancellazione dei dati secondo le indicazioni GDPR
			RRD-4.3	*3. whether data may be retained after the cloud customer has*	*se i dati possono essere conservati dopo che il cliente del*	Applicable	Applicable			

			RRD-4.4	*4. the specific reason for retaining the data;*	*Le motivazioni specifiche del mantenimento dei dati oltre tempo*	Applicable	Applicable			Se è necessario tenere i dati oltre il tempo richiesto dalle finalità, il Fornitore provvede a darne comunicazione (su tempi, motivazioni e modalità di retention/cancellazione) in informativa oltre che nel contratto
			RRD-4.5	*5. the period during which the CSP will retain the data.*	*La durata ulteriore*	Applicable	Applicable			Se è necessario tenere i dati oltre il tempo richiesto dalle finalità, il Fornitore provvede a darne comunicazione (su tempi, motivazioni e modalità di retention/cancellazione) in informativa
12. COOPERATION WITH THE CLOUD CUSTOMERS.	**CPC**	**1. Cooperation with the cloud customers**	**CPC-1.1**	*1. Specify how the CSP will cooperate with the cloud customers in order to ensure compliance with applicable data protection provisions, e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights: rights of access, rectification, erasure ('right to be forgotten'), restriction of processing, portability), to manage incidents including forensic analysis in case of security/data breach. See also Controls no. SEC-1.1 to 1.3.xxvii and PDB-1.1 to 1.8, above.*	*Specificare in che modo il CSP collaborerà con i clienti del cloud al fine di garantire la conformità con le disposizioni applicabili sulla protezione dei dati, ad esempio per consentire al cliente di garantire efficacemente l'esercizio dei diritti delle persone interessate: diritti di accesso, rettifica, cancellazione ("diritto di essere dimenticato '), restrizione dell'elaborazione, portabilità), per gestire gli incidenti inclusa l'analisi forense in caso di violazione della sicurezza / dei dati. Vedi anche i comandi n. Da SEC-1.1 a 1.3.xxvii e da PDB-1.1 a 1.8, sopra*	Applicable	Applicable			Il Fornitore Cloud, all'interno del contratto e nell'informativa, garantisce l'assistenza adeguata all'esercizio dei diritti da parte degli interessati secondo le indicazioni GDPR
			CPC-1.2	*2. Make available to the cloud customer and the competent supervisory authorities the information necessary to demonstrate compliance (see also Controls no. DCA-1.1 to 1.4, above).*	*Rendere disponibili al cliente del cloud e alle autorità di vigilanza competenti le informazioni necessarie a dimostrare la conformità (vedere anche Controls n ° DCA-1.1 a 1.4, sopra).*	Applicable	Applicable			Il Fornitore Cloud garantisce disponibilità a collaborare con Istitituzioni e Autorità
13. LEGALLY REQUIRED DISCLOSURE.	**LRD**	**1. Legally required disclousure**	**LRD-1.1**	*1. Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, including to verify the legal grounds upon which such requests are based prior to responding to them, with special attention to the notification procedure to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.*	*Descrivere il processo in atto per gestire e rispondere alle richieste di divulgazione di dati personali da parte delle autorità preposte all'applicazione della legge, anche per verificare i motivi giuridici su cui tali richieste si basano prima di rispondere ad esse, con particolare attenzione alla procedura di notifica ai clienti interessati, se non diversamente vietato, ad esempio un divieto di diritto penale per preservare la riservatezza di un'indagine di polizia.*	Applicable	Applicable			Il Fornitore Cloud, all'interno del contratto e nell'informativa, garantisce l'eventuale comunicazione dei dati personali alle autorità preposte solo per i casi necessari per legge o per la tutela dei diritti.
14. REMEDIES FOR CLOUD CUSTOMERS.	**RMD**	**1. Remedies for customer**	**RMD-1.1**	*1. Indicate what remedies the CSP makes available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Controls no. WWP-1.1 to 5.9, above and, more specifically, Controls no. WWP-3.1 to 3.5, above) – breach the obligations under the PLA. Remedies could include service credits for the cloud customer and/or contractual penalties for the CSP.*	*Indicare quali rimedi il CSP mette a disposizione del cliente cloud nel caso in cui il CSP - e / oi subappaltatori del CSP (vedere Controlli n ° da WWP-1.1 a 5.9, sopra e, più specificamente, Controls n ° da WWP-3.1 a 3.5, sopra) - violare gli obblighi previsti dal PLA. I rimedi potrebbero includere crediti di servizio per il cliente cloud e / o penali contrattuali per il CSP.*	Applicable	Applicable			Il Fornitore Cloud, all'interno del contratto , garantisce in prima prima persona l'eventuale gestione di violazioni degli accordi privacy da parte del sub fornitore.
15. CSP INSURANCE POLICY.	**INS**	**1. CSP insurance policy**	**INS-1.1**	*1. Describe the scope of the CSP's relevant insurance policy/ies (e.g., data protection compliance-insurance, including coverage for sub-processors that fail to fulfil their data protection obligations and cyber-insurance, including insurance regarding security/data breaches).*	*Descrivere la portata della / le relative polizze assicurative / i della CSP (ad es. Assicurazione sulla conformità alla protezione dei dati, compresa la copertura per i subprocessori che non rispettano i loro obblighi in materia di protezione dei dati e assicurazione cibernetica, compresa l'assicurazione in materia di sicurezza / violazioni dei dati).*	Applicable	Applicable			Esistono polizze specifiche a copertura dei rischi professionali