

Requirement	Requirement ID	Control	Control ID	Specification	CSP is Data Controller	CSP is Data Processor	Additional sector	Additional specification on national level	Consensus Assessment Answers "Please specify how do you achieve compliance to each requirement"	English
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.	Applicable	Applicable	Comply with REG UE 2016/679 and Dlgs 196/03 smi		Abbiamo certificato i processi aziendali con lo standard BS10012. Solo per l'infrastruttura di erogazione è stata sviluppata la certificazione Iso 27001 con l'estensione dei controlli 27017 e 27018	We have certified business processes with the BS10012 standard. The ISO 27001 certification was developed only for the delivery infrastructure with the extension of the controls 27017 and 27018
			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).	Applicable	Applicable			Le procedure fanno parte del sistema di gestione e sono definite nel PIMS (Personal Information Management System). The ISO 27001 certification was developed only for the delivery infrastructure with the extension of the controls 27017 and 27018	The procedures are part of the management system and are defined in the PIMS (Personal Information Management System). The ISO 27001 certification was developed only for the delivery infrastructure with the extension of the controls 27017 and 27018
			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.	Applicable	Applicable			Le procedure sono descritte nel PIMS che è il manuale del sistema BS10012	The procedures are described in the PIMS which is the manual of the BS10012 system
			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.	Applicable	Applicable			Certificato BS10012 e rapporto di audit Certiquality. Solo per l'infrastruttura di erogazione è stata sviluppata la certificazione Iso 27001 con l'estensione dei controlli 27017 e 27018 relative a procedure organizzative e controlli IT (log dei sistemi, record di manutenzione ecc.)	Certificate BS10012 and Certiquality audit report. The ISO 27001 certification was developed only for the delivery infrastructure with the extension of controls 27017 and 27018 relating to organizational procedures and IT controls (system logs, maintenance records, etc.).
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);	Applicable	Applicable		Zucchetti Spa, via Solferino 1 - 26900 - Lodi - Italia - Mario Brocca - mario.brocca@zucchetti.it - +39 03715943191 - 3386366516		
			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);	Applicable	Applicable		N/A		
			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);	Applicable	Applicable		Processor and subprocessor		
			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;	Applicable	Applicable		Mario Brocca, Lodi, Viale Dante 17 - 26900- mario.brocca@zucchetti.it - 03715943191 - 3386366516		
			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.	Applicable	Applicable		Alberto Cazzulani - Lodi - Via Polenghi Lombardo 9 - 26900 - alberto.cazzulani@zucchetti.it - +39 0371-594.3024		
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		N/A		
			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		N/A		
			WWP-1.3	3. recipients or categories of recipients of the data;	Applicable	Not Applicable		N/A		

	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).		Applicable
	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)		
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).	Applicable	Applicable
	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.	Applicable	Applicable
	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).	Applicable	Applicable
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.	Applicable	Applicable

N/A	
N/A	
N/A	
N/A	
N/A	
Sono definite contrattualmente nella nomina a responsabile del trattamento dati	Extent and modalities are contractually defined in the designation as data processor
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	The information for the data Controller will be provided in the communication process that is handled for each update of the products or with a written communication sent to the Controller, if the change affects the Controller only
I dati sono trattati tutti in Italia	The data are all processed in Italy
Ogni modifica viene comunicata al cliente e convenuta contrattualmente con lo stesso	Each change is communicated contractually agreed with the customer
Il Titolare ha sempre il diritto di recedere qualora non sia d'accordo con la modifica	The data controller has always the right to terminate the contract if he does not agree with the amendment
Qualora siano previsti sub appaltatori gli stessi sono comunicati al cliente preventivamente	If sub-contractors are provided, they are communicated to the customer in advance

	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.	Not Applicable	Applicable
	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;	Not Applicable	Applicable
	WWP-3.4	4. Declare to cloud customers and further 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.	Not Applicable	Applicable
	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).	Applicable	Applicable
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).	Applicable	Applicable
	WWP-4.2	2. Indicate to cloud customers the software's implications from a data protection and data security point of view.	Applicable	Applicable
5 Data processing contract (or other	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		

come da contratto si può ricorrere a subresponsabili solo se previamente autorizzati dal cliente	As per contract, you can only use sub-contractors if you have been authorized by the customer
come da contratto con sub nomina a responsabile fatto sottoscrivere ai fornitori che effettuano attività di trattamento dati su Titolari del trattamento	As per contract with sub appoint a responsible person to subscribe to the suppliers who carry out data processing activities on holders of the treatment
La responsabilità del responsabile del trattamento rispetto a quanto eseguito dal sub responsabile è prevista dall'art. 28 Reg UE 2016/679 che è richiamato nella sub nomina a responsabile	The responsibility of the Controller in relation to what is done by the sub-responsible is regulated by art. 28 Reg EU 2016/679 which is recalled in the sub appointment to responsible
Il sub responsabile è sempre convenuto col cliente/Titolare prima del suo impiego. In caso di necessità e qualora il cliente voglia cambiare fornitore a seguito di ingaggio di sub responsabili non graditi può dare disdetta al contratto secondo le previsioni contrattuali e rispettando i previsti ed i tempi ivi previsti	The sub responsible is always agreed with the customer/controller before his employment. In case of necessity and if the customer wants to change supplier as a result of the hire of unwelcome subprocessor, the customer can cancel the contract according to the contractual regulations and respecting the pre-conditions and the time defined therein
i prodotti sono web based e non richiedono installazioni di agenti locali a meno che non ci siano esigenze di far funzionare il sistema fuori linea, come ad esempio per i sistemi di controllo accessi. In questi casi il cliente è previamente informato. Sono comunicate ai clienti con delle circolari le caratteristiche tecniche che devono avere gli strumenti da utilizzare per il funzionamento del sistema informativo (ad esempio browser)	The products are web based and do not require installations of local agents unless there are requirements to operate the system offline, such as for access control systems. In these cases the customer is informed beforehand. The technical characteristics required for the information system operations (e.g. browser) are communicated to customers via newsletters
sono trattati dati personali relativi alla gestione del personale. I dati sono personali identificativi, a rischio specifico, quali ad esempio valutazione di aspetti professionali, rispetto di processi aziendali, o dati sensibili quali iscrizione ai sindacati, dati relativi alla salute e a volte origine razziale o etnica. Sono rispettati tutti i requisiti del GDPR come da certificazione BS10012	Personal data relating to personnel management are processed. The data are personal identification, at specific risk, such as evaluation of professional aspects, respect of business processes, or sensitive data such as registration to trade unions, data related to health and sometimes racial or ethnic origin. All GDPR requirements are respected as certified by BS10012

binding legal act)			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.	Not Applicable	Applicable
	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;		Not Applicable	Applicable
	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;		Not Applicable	Applicable
	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;		Not Applicable	Applicable
	WWP-5.5	5. Respect the conditions for engaging another processor (see Controls no. WWP-3.1 to 3.5, above).		Not Applicable	Applicable
	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;		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
	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).		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.		Not Applicable	Applicable

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
			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
					Applicable	Not Applicable

con i clienti sono condivisi i registri dei trattamenti in cui sono presenti tutte le informazioni relative al trattamento, comprese quelle sugli interessati, sul tipo di dati, sui periodi di conservazione, sulle misure di sicurezza applicate e sugli addetti che tratteranno i dati	The records of the treatments are shared with the customers. Records contain all the information related to the treatment, including those on the subjects the type of data, the periods of preservation, the security measures applied and the attendants who will treat the data
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Nomina a responsabile del trattamento allegata ad ogni contratto. Al termine del rapporto contrattuale i dati sono conservati come da standard per 90 gg in produzione e 1 anno su supporti di backup	The data processor agreement is attached to every contract. At the end of the contractual relationship the data are stored by default for 90 days in production and 1 year on backup media
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract

N/A	
N/A	
N/A	

			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.	Not Applicable	Applicable
			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;	Not Applicable	Applicable
			REC-2.3	3. categories of processing carried out on behalf of each controller;	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;	Not Applicable	Applicable
			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).	Not Applicable	Applicable
					Not Applicable	Applicable
					Not Applicable	Applicable

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.	Applicable	Applicable
			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.	Applicable	Applicable

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;	Applicable	Applicable
			SEC-1.2	2. Describe to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) to ensure the following safeguards:	Applicable	Applicable
			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;	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.);	Applicable	Applicable

N/A	
N/A	
Nomina a responsabile del trattamento allegata ad ogni contratto	The data processor agreement is attached to every contract
Registro dei trattamenti consegnato ai clienti a richiesta e pubblicato nella loro area riservata contiene i dati richiesti dal GDPR	Record of treatments provided, on request, to customers and published in their reserved area contains the data required by GDPR
Registro dei trattamenti consegnato ai clienti a richiesta e pubblicato nella loro area riservata contiene i dati richiesti dal GDPR	Record of treatments provided, on request, to customers and published in their reserved area contains the data required by GDPR
Registro dei trattamenti consegnato ai clienti a richiesta e pubblicato nella loro area riservata contiene i dati richiesti dal GDPR	Record of treatments provided, on request, to customers and published in their reserved area contains the data required by GDPR
Registro dei trattamenti consegnato ai clienti a richiesta e pubblicato nella loro area riservata contiene i dati richiesti dal GDPR	Record of treatments provided, on request, to customers and published in their reserved area contains the data required by GDPR
Registro dei trattamenti consegnato ai clienti a richiesta e pubblicato nella loro area riservata contiene i dati richiesti dal GDPR	Record of treatments provided, on request, to customers and published in their reserved area contains the data required by GDPR
i dati sono trattati in Italia ed i piani di disaster recovery sono attuati sempre su territorio italiano	The data are processed in Italy and the disaster recovery plans are implemented on Italian territory
n/a, non sono trasferiti dati fuori dal territorio ue	N/A, no data are transferred outside the EU territory
riportate sul Registro dei trattamenti riferito al loro servizio	Reported on the record of treatments related to their service
Risk assessment - Valutazione di impatto	Risk assessment - Impact assessment
Risk assessment - Valutazione di impatto; Remediation plan	Risk assessment - Impact assessment - Remediation plan
Risk assessment - Valutazione di impatto; Remediation plan	Risk assessment - Impact assessment - Remediation plan

SEC-1.2.iii	<i>(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;</i>	Applicable	Applicable
SEC-1.2.iv	<i>(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);</i>	Applicable	Applicable
SEC-1.2.v	<i>(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);</i>	Applicable	Applicable
SEC-1.2.vi	<i>(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');</i>	Applicable	Applicable
SEC-1.2.vii	<i>(vii) portability - refer to Controls no. PMT-1.1 to 1.2, below;</i>	Applicable	Applicable
SEC-1.2.viii	<i>(viii) accountability: refer to Controls no. DCA-1.1 to 1.4, above.</i>	Applicable	Applicable
SEC-1.3	<p>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.</p> <p>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 SQ08 or SQ09 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.</p>	Applicable	Applicable
SEC-1.3.i	<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.</i>	Applicable	Applicable
SEC-1.3.ii	<i>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.</i>	Applicable	Applicable

Risk assessment - Valutazione di impatto; Remediation plan	Risk assessment - Impact assessment - Remediation plan
ogni procedura e istruzione di lavoro può essere consegnata al cliente dopo aver sottoscritto un apposito NDA	Each procedure and job instruction can be delivered to the customer after NDA signing
Procedura sulla privacy by default applicata agli ambienti di produzione	Privacy procedure by default applied to production environments
Procedura per esercizio del diritto di accesso per gli interessati	Procedure for the exercise of the right to data access for interested parties
la portabilità non si applica all'ambito di erogazione del servizio saas relativo al gestionale. In questo caso ci sono comunque procedure di estrazione in .csv	Portability does not apply to the scope of the SaaS service for the management. In this case there are extraction procedures (data extracted in .csv format)
Tutti i processi di assistenza e di trattamento dei dati dei clienti sono memorizzati sullo strumento di post vendita. Ogni documento può essere consegnato al cliente a richiesta e previa sottoscrizione di un NDA	All customer data help desk and treatment processes are stored on the post-sale tool. Each document can be provided to the customer on request and after NDA signature
Sono applicate misure di sicurezza sia Enisa che Iso27001 che richieste dallo standard BS10012	Security measures are applied, in particular Enisa and Iso27001 requirements, as well as requirements defined by the standard BS10012
Il Personal information management system riporta gli asset e le procedure adottate per il rispetto del GDPR. Il PIMS è fatto in adempimento dello standard BS10012	The Personal information Management system reports the assets and procedures adopted to respect the GDPR. The PIMS is made in compliance with the standard BS10012
Risk assessment fatto in relazione a quanto previsto dallo standard BS10012	Risk assessment performed in relation to the standard BS10012

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.).	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable

I ruoli sono assegnati con lettere di incarico in relazione al ruolo e ai dati trattati dagli operatori. Inoltre sono attribuite le responsabilità nell'organigramma privacy aziendale	The roles are defined by the letters of assignment in relation to the role and the data processed by the operators. In addition, responsibilities are attributed in the privacy organization organisation chart
Nei contratti sono definiti i compiti e le responsabilità dei fornitori rispetto alle attività che vengono assegnate	The contracts define the tasks and responsibilities of the suppliers according to the activities that are assigned
In sede di assunzione l'ufficio HR verifica il passato professionale dichiarato da ogni singolo addetto. Viene compilato in sede di colloquio una scheda in cui il lavoratore dichiara la sua situazione lavorativa, familiare ed i suoi rapporti con pubbliche amministrazioni e clienti	During the recruitment stage, the HR department verifies the professional background stated by each individual person. A sheet in which the worker declares his working situation, family and his/her relations with public administrations and customers is compiled in the interview
Tutti i lavoratori sono formati/informati sulle procedure adottate per il trattamento dei dati e per la sicurezza delle informazioni. Gli interventi formativi riguardano ogni lavoratore in relazione ai compiti svolti.	All workers are trained/informed about the procedures adopted for data processing and information security. The formative sessions concern each worker in relation to the tasks carried out.
C'è un processo per la gestione degli inserimenti del personale in determinate mansioni e per il loro cambiamento di ruolo, fino ad arrivare alla gestione della cessazione del rapporto di lavoro. Ogni fase è gestita attraverso l'informazione mandata all'ufficio HR a tutti gli uffici coinvolti e interessati che provvedono a fare le modifiche di loro competenza	There is a process for the management of staff hiring for particular tasks and for their change of role, up to the management of the employment relationship ending. Each phase is managed through the information sent to the HR office to all the involved and interested offices that provide for the necessary interventions
Sono applicate le sicurezze al data center derivanti dai processi Iso 27001. L'accesso è controllato, vi è un impianto di spegnimento a argon con saturazione d'ossigeno, c'è un gruppo di continuità, non ci sono impianti sanitari, c'è un impianto di allarme con intervento 24h su 7 gg, impianto sonoro antincendio con collegamento ad una control room ed impianto di videosorveglianza attivo.	The securities are applied to the data center as defined by the Iso 27001 processes. Access is controlled, there is an argon shutdown system with oxygen saturation, there is a UPS, there are no sanitary facilities, there is an alarm system with intervention 24h on 7 days, fire sound system with connection to a control room and active video surveillance system.
c'è un gruppo di continuità che si attiva in caso di mancata energia e che viene mantenuto. La rete è ridondata e sono attivi servizi di connessione internet con 4 provider.	There is a UPS that is activated in the event of a power failure and it is maintained. The network is redundant and Internet connection services are active with 4 providers.
tutti gli accessi ai sistemi sono tracciati e avvengono con utenti individuali; c'è un proxy per il controllo della navigazione internet; firewall sempre attivo, IPS e IDS.	All accesses to systems are tracked and occur with individual users; there is a proxy for the control of Internet browsing; an always on firewall, IPS and IDS tools
sono attivi due sistemi antivirus ed un sistema antispam. Tutti gli amministratori di sistema sono loggati ed i log conservati in modo da garantirne l'integrità.	Two anti-virus systems and one antispam system are active. All system administrators are logged in and the logs kept and secured to ensure their integrity.

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.).	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
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.	Applicable	Applicable
SEC-1.3.xvi	xvi. (SO 16) – Security incident reporting: The CSP establishes and maintains appropriate procedures for reporting and communicating about security incidents.	Applicable	Applicable
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	Applicable	Applicable
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	Applicable	Applicable
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.).	Applicable	Applicable
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	Applicable	Applicable
SEC-1.3.xxi	xxi. (SO 21) – Security assessments: The CSP establishes and maintains appropriate procedures for performing security assessments of critical assets	Applicable	Applicable
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	Applicable	Applicable

tutte le procedure sono definite in conformità allo standard Iso 27001 e BS 10012. Le procedure riguardano ogni misura di sicurezza da adottare a tutela dei dati.	All procedures are defined in accordance with the standards Iso 27001 and BS 10012. The procedures concern every security measure to be taken to protect the data.
In relazione al processo di gestione iso 27001 sono state realizzate e applicate procedure per la gestione del change management	Procedures for change management have been implemented according to ISO27001 standard
Sono presenti misure tecniche e organizzative in conformità allo standard Iso 27001 che gestiscono i change quali installazioni patches, cambio password, utilizzo e dismissione supporti, introduzione nuovi strumenti, etc	There are technical and organizational measures in compliance with ISO 27001 for change management such as patches, password change, use and disposal of media, introduction new tools, etc
Gli incidenti di sicurezza sono gestite sia con processi Iso 27001 che BS10012. Se sono data breach viene immediatamente data comunicazione al cliente compilando un modulo di analisi dell'incidente e registrando l'evento sul registro dei presunti data breach. L'incidente viene classificato in modo provvisorio. Sarà il cliente a classificarlo in modo definitivo e a comunicarlo all'autorità	Security incidents are handled with both Iso 27001 and BS10012 processes. If a data breach is detected, it is immediately communicated to the customer by filling an incident analysis form and registering the event on the record of alleged data breach. The incident is provisionally classified. The customer will classify it definitively and will communicate it to the authority
ci sono procedure dell'incident di sicurezza del sistema Iso27001 applicabili a tutti i servizi di dc	There are Iso27001 system security incident procedures applicable for all DC services
c'è un piano di disaster recovery. La business continuity deve essere attivata a richiesta dei clienti previa valutazione progettuale	There's a disaster recovery plan. Business continuity must be activated at the request of customers after design evaluation
c'è il piano di disaster recovery che viene verificato una volta l'anno	There is the disaster recovery plan that is verified once a year
Strumenti di monitoraggio dei servizi offerti tramite tool automatici che registrano le varie azioni/transazioni svolte sul sistema	Tools for monitoring services are provided through automated tools that record the various actions/transactions carried out on the system
ogni servizio viene testato da un gruppo dedicato al controllo qualità dei prodotti realizzati. Il processo è definito da procedure Iso9001	Each service is tested by a group dedicated to the quality control of the products realized. The process is defined by Iso9001 procedures
annualmente, o in occasione dell'introduzione di nuovi servizi, viene effettuata la valutazione del rischio secondo gli standard Iso27001 e tenendo in considerazione i controlli Iso27017/27018	Annually, or at the time of the introduction of new services, the risk assessment is carried out according to the Iso27001 standards and taking into account the Iso27017/27018 controls
c'è un ufficio dedicato allo studio delle norme di settore che formano gli analisti sulle funzionalità applicative. L'aggiornamento normativo e alle buone prassi fa parte del contratto di manutenzione stipulato dai clienti.	There is an office dedicated to the study of the industry norms that form analysts on the application functionalities. The regulatory update and good practice is part of the customer service contract.

SEC-1.3.xxiii	xxiii. (ISO 23) – Security of data at rest: The CSP establishes and maintains appropriate mechanisms for the protection of the data at rest	Applicable	Applicable
SEC-1.3.xxiv	xxiv. (ISO 24) – Interface security: The CSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data	Applicable	Applicable
SEC-1.3.xxv	xxv. (ISO 25) – Software security: The CSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security	Applicable	Applicable
SEC-1.3.xxvi	xxvi. (ISO 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	Applicable	Applicable
SEC-1.3.xxvii	xxvii. (ISO 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	Applicable	Applicable

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	Applicable	Applicable
----------------	-----	---------------	---------	--	------------	------------

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.	Applicable	Applicable
			PDB-1.2	Explain to cloud customers the procedures in place to collect and disclose the following information: 2. the nature of the personal data breach including, where possible, the categories and approximate number of personal data records concerned;	Applicable	Applicable
			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);	Applicable	Applicable

I dati seguono delle politiche di cancellazione definite e condivise col cliente. Il dato inattivo, in relazione al servizio offerto può essere minimale e comunque prevede l'intervento del cliente per la scelta se mantenerlo o meno. Ove necessario viene attivata la cifratura dei dati a riposo tramite algoritmo MS SQL TDE, mentre i documenti presenti nel Document Management System sono criptati di default	The data are deleted according to the cancellation policies defined and shared with the client. The inactive data, in relation to the service offered can be minimal and in any case involves the intervention of the customer for the choice whether to keep it or not. Where required, data encryption is activated by the MS SQL TDE algorithm, while the documents in the Document Management System are encrypted by default
---	---

Il gruppo ricerca e sviluppo che mantiene e aggiorna il tool di sviluppo con cui sono scritti i software si preoccupa della sicurezza delle interfacce con cui verranno gestiti i dati dai Clienti	The research and Development group that maintains and updates the development tool with which the software is written is concerned about the security of the interfaces with which the data will be managed by the customers
--	--

i programmatori utilizzano un tool già strutturato per garantire la sicurezza dell'ambiente che sviluppano.	Developers use a tool already structured to ensure the security of the environment.
---	---

la migrazione ad altri sistemi deve essere verificata a livello progettuale. I sistemi software prevedono estrazioni .csv che consentono l'esportazione di tutte le informazioni presenti nel prodotto.	The transfer of information and data to other systems must be verified at the design level. The software systems include extractions .csv that allow the export of all the information in the product..
---	---

il fornitore collabora con il titolare per effettuare le indagini di sicurezza necessarie in relazione agli eventi di sicurezza occorsi.	The supplier collaborates with the holder to carry out the necessary safety investigations in relation to the security events needed.
--	---

Sono accettati contrattualmente audit dei clienti o di terze parti per la verifica delle misure di sicurezza poste in essere. Ogni audit presuppone la sottoscrizione di un nda da parte di chi lo conduce.	Contractually audits of customers or third parties are accepted for the verification of the security measures in place. Each audit assumes the signing of an NDA by those who lead it.
---	--

E' definita la procedura di comunicazione dei data breach secondo le prescrizioni del GDPR e le regole della BS10012	The procedure for communicating data breach is defined according to the requirements of the GDPR and the rules of the BS10012
--	---

Nel modello di comunicazione sono previste queste informazioni	This information is provided in the communication model
--	---

Nel modello di comunicazione sono previste queste informazioni. Inoltre queste informazioni sono presenti sul registro del trattamento pubblicato nell'area riservata del cliente	This information is provided in the communication model. Moreover this information is present on the register of the treatment published in the reserved area of the customer
---	---

			PDB-1.4	4. the likely consequences of the personal data breach;	Applicable	Applicable
			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.	Applicable	Applicable
			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).	Applicable	Applicable
			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:	Applicable	Applicable
			PMT-1.1.i	(i) to the cloud customer ('transfer back', e.g., to an in-house IT environment);	Applicable	Applicable
			PMT-1.1.ii	(ii) directly to the data subjects;	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).	Applicable	Applicable
			PMT-1.2	2. how and at what cost the CSP will assist customers in the possible migration of data to another provider or back to an in-house IT environment. Whatever the procedure implemented, the CSP must cooperate in good faith with cloud customers, by providing a reasonable solution.	Applicable	Applicable

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.	Applicable	Applicable
--------------------------------	-----	------------------------------	---------	--	------------	------------

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.	Applicable	Applicable
			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.	Applicable	Applicable
		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,		

Nel modello di comunicazione sono previste queste informazioni	This information is provided in the communication model
Nel modello di comunicazione sono previste queste informazioni	This information is provided in the communication model
Nel modello di comunicazione sono previste queste informazioni	This information is provided in the communication model
N/A	
N/A	

possibile ma da definire a livello progettuale	Possible but to be defined at the design level
come data processor non gestiamo i rapporti con gli interessati ma facilitiamo l'interazione tra interessato e cliente formando il cliente ad estrarre i dati.	As a data processor we do not manage the relations with the subjects but we facilitate the interaction between subjects and customer, training the customer to extract the data by itself
I dati contenuti nelle tabelle del db sono estraibili in formato .csv; i file sono copiabili e trasportabili su altri sistemi a livello progettuale convenendo le modalità con i clienti	The data contained in the DB tables are extractable in .csv format; The files can be copied and transported on other systems at the design level, by agreeing the procedure with the customers
le migrazioni devono essere verificate a livello progettuale ed i costi applicabili saranno quelli concordati con il cliente in sede di sottoscrizione contrattuale relativi agli interventi dei consulenti (importo espresso in ore di intervento)	The migrations of data must be verified at the design level and the applicable costs will be agreed with the customer in the contract. Costs will relate to the interventions of the consultants (amount expressed in hours of intervention)

In caso di richiesta di limitazione viene analizzata da parte dell'ufficio privacy la richiesta del cliente e valutata in relazione agli adempimenti contrattuali assunti. Al cliente viene data risposta entro 30 gg dalla sua richiesta specificando come avverrà la limitazione e se sarà applicabile.	In case of request for limitation, the customer's request is analysed by the privacy office and assessed in relation to the contractual fulfillments assumed. The customer is answered within 30 days of his request specifying how the limitation will take place and whether applicable.
---	--

queste informazioni sono previste dal contratto e nel registro del trattamento	This information is provided in the contract and in the record of treatments
viene garantito ce gli eventuali sub responsabili prestano al cliente/Titolare del trattamento le stesse garanzie fornite dal responsabile in sede di stipula del contratto ed eventualmente rideterminate in corso di rapporto.	It is guaranteed that any sub-processor lends to the customer/controller of the treatment the same guarantees provided by the person responsible in the conclusion of the contract and possibly re-established in the course of the report.

The cooperation is defined by...

				<i>the personal data will or may be retained, or if that is not possible, the criteria used to determine such a period.</i>	Applicable	Applicable
			RRD-2.2	2. Take into consideration the following criteria, when defining retention periods: <i>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).</i>	Applicable	Applicable
		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.	Applicable	Applicable
		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);	Applicable	Applicable
			RRD-4.2	2. the methods available or used to delete data;	Applicable	Applicable
			RRD-4.3	3. whether data may be retained after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract;	Applicable	Applicable
			RRD-4.4	4. the specific reason for retaining the data;	Applicable	Applicable
			RRD-4.5	5. the period during which the CSP will retain the data.	Applicable	Applicable
					Applicable	Applicable
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.	Applicable	Applicable
			CPC-1.2	2. Make available to the cloud customer and the competent supervisory authority the information necessary to demonstrate	Applicable	Applicable

la conservazione, come prevista da contratto, sarà garantita per la durata del contratto, per i successivi 90 giorni e su supporto di backup per i successivi 12 mesi a meno che con il cliente siano convenuti tempi più lunghi	the conservation, as defined by contract, will be guaranteed for the duration of the contract, for the following 90 days and on backup support for the following 12 months unless longer terms are agreed with the customer
essendo noi data processor ereditiamo i tempi di conservazione quali definiti contrattualmente	As data processor, Zucchetti observes the retention times defined contractually
Il servizio è standard, quindi il cliente deve valutare nelle attività precontrattuali se il servizio è conforme allo standard di settore che deve rispettare. Il servizio può essere personalizzato solo a livello progettuale prima della stipula del contratto.	The service is standard, therefore the customer must evaluate in the pre-contractual activities if the service respects the industry standard required. The service can only be customized at the design level before the contract is concluded
i dati possono essere estratti in .csv o formato equivalente	The data can be extracted in .csv or equivalent format
sono presenti apposite funzioni applicative che consentono al Titolare in autonomia di cancellare i dati riferibili ad un interessato. I dati possono essere cancellati o anonimizzati in modo irreversibile a seconda che il titolare voglia conservare i dati a livello statistico o non abbia tale interesse. Qualora il cliente abbia più sistemi interoperabili dovrà procedere alla cancellazione in modo dedicato su tutti i sistemi. Tali misure di sicurezza sono presenti e aggiornate sul registro del trattamento	There are special application functions that allow the owner to independently erase the data referable to an interested person. The data may be cancelled or anonymized irreversibly depending on whether the rightholder wants to retain the data at a statistical level or does not have such interest. If the customer has more interoperable systems, he will have to delete them in a dedicated way on all systems. These security measures are present and updated on the treatment register
per i servizi cloud i dati cancellati risiedono comunque sui supporti di backup per i 12 mesi successivi	For cloud services, deleted data still resides on the backup media for the next 12 months
I dati sono conservati in adempimento del contratto	The data is kept in compliance with the contract
tali periodi sono previsti a livello contrattuale, come sopra descritto	These periods are defined at contractual level, as described above
Il data processor evaderà le richieste del cliente/Titolare del trattamento da un punto di vista tecnico, facilitando il riscontro ed estraendo, cancellando, modificando i dati come richiesti dal cliente. Se si verifica un data breach viene comunicato al cliente entro 24 ore con la relativa analisi dell'accaduto	The data processor will fulfill the requests of the customer/controller of the treatment from a technical point of view, facilitating the feedback and extracting, deleting, modifying the data as requested by the customer. If a data breach is detected, it is communicated to the customer within 24 hours with the relevant analysis of the incident
	As agreed in the contract, the

				субъекты обрабатывающие информацию necessary to demonstrate compliance (see also Controls no. DCA-1.1 to 1.4, above).	Applicable	Applicable
13. LEGALLY REQUIRED DISCLOSURE.	LRD	1. Legally required disclosure	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.	Applicable	Applicable
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.	Applicable	Applicable
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).	Applicable	Applicable

<p>Come previsto dal contratto il processor è disponibile nel ricevere audit dei clienti, di terze parti o dalle autorità competenti. Qualora gli audit dei clienti o di terze parti comportino dei costi, l'intervento deve essere valutato a livello progettuale. Il processor in autonomia sostiene audit di terze parti in adempimento dei processi Iso27001; BS10012; ed effettua ogni anno VA e PT</p>	<p>processor is available to receive audits of customers, third parties or competent authorities. Should the audits of the customers or third parties entail any cost, the intervention must be assessed at the design level. The processor independently also undergoes third parties audits in fulfilment of the Iso27001 processes; BS10012; and performs every year VA and PT</p>
<p>Le richieste di accesso ai dati da parte delle autorità competenti avvengono solo a seguito di apposito mandato da parte del giudice. In relazione alla richiesta fatta viene valutato dall'ufficio legale e dall'ufficio privacy la modalità operativa e le eventuali comunicazioni da fare ai clienti. Le comunicazioni ai clienti avvengono all'indirizzo email comunicato dagli stessi in sede di stipula contrattuale oppure modificato ed inserito nel portale di postvendita in corso di rapporto.</p>	<p>Requests for access to the data by the competent authorities only take place following a specific mandate from the court. In relation to the request made is assessed by the Legal Office and the Privacy Office the mode of operation and any communication to be done to customers. The communications to the customers take place at the email address communicated by the same in the contract stipulation or modified and inserted in the portal of post-sale in course of report.</p>
<p>ogni sanzione, in relazione agli inadempimenti delle prestazioni come convenute contrattualmente, è imputabile al data processor solo se attribuibile a sua colpa. Il Data processor è assicurato per gli eventuali inadempimenti professionali con una RCT professionale fino a 2.500.000 € di copertura. Commercialmente potranno essere convenute misure compensative rispetto ai danni prodotti verso i clienti. Tali misure dovranno essere valutate dal Responsabile di Business Unit in modo dedicato e specifico.</p>	<p>Any sanction, in relation to the breach of performance contractually agreed, is attributable to the data processor only if attributable to its fault. The Data processor is insured for any professional failures with a professional RCT up to €2.5 million coverage. Countervailing measures may be commercially agreed with respect to the damage produced to customers. These measures will have to be assessed by the responsible of the Business Unit in a dedicated and specific way.</p>
<p>RCT professionale come sopra descritta. I sub responsabili non sono previsti ma se dovessero essere previsti saranno prestate ai clienti le stesse garanzie date dal data processor.</p>	<p>Professional RCT as described above. The sub-responsibles are not expected, but if they are expected, the same guarantees given by the data processor will be provided to customers.</p>