



Autore	Ufficio privacy
Approvazione	Tiziano Colombi

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio privacy	22/10/2019	23/10/2019	Prima emissione
1.0	Ufficio Privacy	29/07/2020	29/07/2020	Modificato approvatore
2.0	Ufficio privacy	15/04/2021	16/04/2021	Modificati i tempi di retention
3.0	Ufficio Privacy	09/02/2022	09/02/2022	Modificata sezione delle procedure di assistenza per utilizzo nuovo strumento per collegamento da remoto
4.0	Ufficio Privacy	29/05/2023	31/05/2023	Modifica procedure di assistenza: aggiunta area Sharepoint per la condivisione di file con il cliente
5.0	Ufficio Privacy	18/06/2025	18/06/2025	Inserito Partner PAR-TEC S.p.A. quale fornitore di attività di assistenza sistemistica estesa H24 e aggiornato nome rappresentante legale
6.0	Ufficio Privacy	7/01/2026	7/01/2026	Variazione indirizzo sede Zucchetti Spa ed inserita Z Holding Spa come DPO

PARERE DPO OK



DIGITAL CFO

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Zucchetti Spa				
Partita Iva	05006900962				
Indirizzo	Piazza Mino Zucchetti,1				
Città	Lodi	Cap	26900	PV	LO
Legale Rappresentante	Alessandro Zucchetti preposto dalla società CONVERTENDO SRL, Legale rappresentante di Zucchetti SPA				
STRUTTURA ORGANIZZATIVA					
Divisione	Commercialisti	Responsabile Divisione		Mario Pedrazzini	
Area	Area piani, controllo e comunicazione	Responsabile Reparto		Tiziano Colombi	
INCARICATI DEL TRATTAMENTO					
help desk, consulenti applicativi					
DATI DI CONTATTO					
Responsabile del trattamento	Zucchetti Spa	ufficio.privacy@zucchetti.it		0371/594.1	
Rappresentante del responsabile	n.a.				
Responsabile protezione dati (DPO)	Z Holding Spa	ufficio.privacy@zucchetti.it		0371/594.3191	
DESCRIZIONE					
Digital CFO è una soluzione interamente cloud che permette a Professionisti, Associazioni di categoria, Sindaci e Revisori di disporre di uno strumento per guidare le aziende clienti nelle attività di controllo, orientamento e pianificazione finanziaria. Attraverso l’importazione di file (PDF della Centrale Rischi di Banca d’Italia, bilanci XBRL) e l’integrazione di alcune informazioni di natura qualitativa dell’azienda, il software, tramite una serie di algoritmi, restituisce in automatico l’analisi finanziaria delle aziende e, in caso di anomalie, le segnala in tempo reale ai clienti tramite un’apposita APP (non disponibile in tutte le configurazioni commerciali del servizio) per smartphone e tablet. Ogni analisi è esportabile in formato pdf e certificata attraverso l’apposizione di una firma elettronica, associata ad un riferimento temporale, per eventuali opposizioni in giudizio e in caso di procedure concorsuali. Il servizio CLOUD viene erogato dal DC di AMAZON WEB SERVICES e il software è prodotto dalla società GHOSTCFO SRL, con sede legale in Corso Porta Nuova, n. 133 a Verona (VR)					
FINALITA' DEL TRATTAMENTO					
Erogazione del servizio in modalità cloud, con relativa assistenza e manutenzione software.					
CATEGORIA INTERESSATI					
Le persone fisiche che riferiscono a soci, associati, amministratori, percipienti, collaboratori dei clienti finali.					



CATEGORIE DI DATI PERSONALI
Dati anagrafici di società clienti del Titolare; dati economici e fiscali.
CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
Aziende del gruppo Zucchetti Fornitori di servizi collegati alle applicazioni principali: GHOSTCFO SRL, con sede legale in Corso Porta Nuova, n. 133 a Verona (VR), per manutenzione e assistenza di secondo livello. Nel dettaglio GHOSTCFO effettuerà per conto del Responsabile le seguenti attività che comportano il trattamento dati: - sviluppi e rilasci di nuove versioni applicative; - attivazione della licenza sulla piattaforma, attraverso un contatto diretto da parte del Cliente/Titolare del trattamento, tramite email (l'indirizzo è contenuto all'interno della mail di attivazione);- assistenza di secondo livello su richiesta del Responsabile del trattamento, senza che sia previsto un contatto diretto con il Cliente/Titolare del trattamento. AMAZON WEB SERVICES in qualità di fornitore del servizio Cloud. Incaricati di gruppi interni alla Zucchetti Spa chiamati ad eseguire attività di , assistenza e manutenzione. PAR-TEC S.p.A. quale partner fornitore di attività di assistenza sistemistica estesa H24
TRASFERIMENTO DATI ALL'ESTERO
No Il Trattamento sarà effettuato con sistema localizzato in Europa.
TERMINI PER LA CANCELLAZIONE DEI DATI
I dati conservati nel Data Center di Amazon, in vigenza di contratto, saranno conservati (archiviati su un disco rigido) per un periodo non superiore a 36 mesi e, nei casi in cui lo richiedano improrogabili esigenze di servizio, il periodo potrà essere ridotto a 18 mesi. I dati trasmessi attraverso lo strumento di ticketing, per finalità di assistenza, vengono conservati nello strumento stesso per 5 anni dalla chiusura del ticket. Alla cessazione del contratto, i dati saranno visualizzabili dal Cliente/Titolare del trattamento per 30 giorni e conservati, complessivamente per 90 giorni dalla cessazione, decorsi i quali saranno cancellati. Il Cliente/Titolare del trattamento ha la possibilità, attraverso le funzioni applicative di richiedere al fornitore la cancellazione di dati personali salvati nel db.



DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

- *Gestione credenziali di accesso*
- Username: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede. Viene inviata una email al cliente/utilizzatore con un URL, con cui viene richiesto di inserire la password.
Nel sistema c'è una credenziale amministrativa che resta in possesso dello sviluppatore della soluzione e viene utilizzata dallo stesso solo per attività straordinarie, su richiesta del Titolare del trattamento;
- Password: non ci sono regole di complessità predefinite; le regole di complessità della password sono configurabili nel sistema da parte del Cliente/Titolare. Esiste un controllo sulla debolezza della credenziale inserita.
- Disattivazione/disabilitazione/cambio credenziali: non c'è una scadenza delle credenziali. Le tempistiche di cambio password devono essere definite dal Cliente con una specifica procedura organizzativa.
 - *Identificazione di chi ha trattato i dati:*
- Strumenti di log: sono presenti strumenti di log che registrano i log in e log failed, in una tabella applicativa accessibile solo dall'amministratore di sistema. A livello di DB vengono "loggati" inserimenti di dati, modifiche e attività che sono associate alle singole utenze. Tali funzionalità sono visibili solo attraverso l'utenza amministrativa. Con una query dal DB, su richiesta del cliente, è possibile fornire evidenza. I log applicativi non sono soggetti a cancellazione.
- Presenza di utenze di servizio per personale di assistenza: coloro che eseguono assistenza e manutenzione sulla procedura hanno utenze nominali che vengono attivate e disattivate dall'amministratore di sistema su richiesta del Titolare in funzione della necessità.
 - *Tecniche di crittografia:*
- Crittografia delle password: viene registrato un hash delle password con l'algoritmo bcrypt aggiungendo un "salt" di applicazione.
 - *Privacy by default*
- Attivazione profilo utente: per il cliente/Titolare è prevista una sola utenza. Lo stesso può, tuttavia, abilitare l'accesso ai clienti finali attraverso l'invio del link per la generazione delle credenziali e con la possibilità di determinare a quali dati il cliente finale può accedere.
- E' presente la divisione tra utenze master e utenze con diversi livelli di "visibilità" (profili autorizzativi configurabili dal cliente/Titolare).
 - *Diritti degli interessati:*
- Diritti degli interessati: è prevista, a livello applicativo, una funzionalità che garantisce la cancellazione "logica" del dato, che non risulta più visibile ma rimane salvato a livello di DB. Per procedere alla definitiva cancellazione il Cliente/utente deve rivolgere una richiesta al Responsabile, per la cancellazione definitiva dell'anagrafica e di tutte le tabelle collegate.
- Per la portabilità è prevista la consegna dei file (report in .pdf) generati.



- E' in corso di implementazione la funzionalità che consente che il sistema sia configurabile con un sistema SSO
- C'è una funzione CAPTCHA Block User account enumeration

Queste misure di sicurezza devono essere correttamente impostate da parte del Titolare.



2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

ASSISTENZA ON SITE

Gli addetti Zucchetti accedono presso la struttura del Titolare per fare formazione od effettuare attività tecnica di manutenzione.

In questo caso gli addetti Zucchetti lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezze implementate dallo stesso. I Titolari potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale. Qualora durante l'attività di assistenza l'addetto Zucchetti abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolare e registri tale attività sulla Nota di intervento:

Al termine dell'attività presso gli uffici Zucchetti sarà informato il Titolare sulla soluzione adottata e sulla successiva cancellazione dell'archivio.

Qualora vi fosse la necessità di conservare gli archivi per il tempo necessario al collaudo della soluzione adottata, dovrà essere informato il Titolare sul tempo massimo di conservazione di tali archivi.

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email i tecnici Zucchetti inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.

L'addetto Zucchetti non è autorizzato a farsi mandare le credenziali di accesso del Titolare via email né tantomeno potrà salvarle sullo strumento di ticketing.

Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico Zucchetti è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico Zucchetti dovrà richiedere credenziali individuali oppure collegamento tramite strumenti a ciò dedicati.

I tecnici Zucchetti firmeranno ogni email con nome e cognome e l'informazione sarà salvata nel ticketing.

ASSISTENZA ATTRAVERSO LA RICEZIONE DI DATA BASE DEI CLIENTI

Qualora per risolvere il problema segnalato dal Titolare fosse necessario farsi mandare la base dati o altri files o query contenenti dati personali è necessario comunicare al Titolare o l'area ftp su cui dovrà caricare i file oppure per i Titolari con l'ambiente installato sul ns. data center, richiedere l'autorizzazione per far effettuare la copia ai nostri sistemisti.

Area FTP

L'area ftp sarà impostata affinché il Titolare veda solo l'upload. Il download sarà visualizzato solo dal gruppo di assistenza a cui la richiesta di assistenza è stata effettuata.

Almeno 1 volta al giorno una routine cancellerà i file caricati in area ftp.



Area SharePoint

Essendo diventato Office 365 strumento aziendale anche di collaborazione ogni utente Zucchetti ha a disposizione Sharepoint che può utilizzare anche tale strumento per la condivisione dei documenti e file in genere coi clienti.

L'azienda al fine di tutelare la privacy del dipendente non entrerà nel merito dello sharepoint individuale, pertanto, una volta che il cliente ha scaricato i files, l'operatore avrà anche la responsabilità della relativa cancellazione.

Scaricamento archivi tramite wetransfer o link di collegamento su ambienti del Titolare

In questo caso la gestione è in carico al Titolare che fornirà le credenziali per accedere all'ambiente dove risiedono gli archivi.

L'assistenza dovrà scaricarli in dischi di rete non soggetti a backup e cancellarli al termine dell'attività come nelle altre ipotesi.

Autorizzazione di backup da parte dei nostri sistemisti

L'archivio ricevuto viene scaricato su una directory del gruppo di assistenza non soggetta a backup.

L'assistenza di primo livello trasmette il db all'assistenza di 2 livello. L'assistenza di 2 livello procederà alle analisi di cui il problema necessita e poi cancellerà gli archivi ricevuti.

In ogni caso l'assistenza che ha in carico il problema, sia essa di primo o secondo livello, al termine dell'attività, cancellerà gli archivi ricevuti.

L'assistenza che ha in carico la gestione, terminata l'attività dovrà cancellare gli archivi ricevuti dal disco condiviso e da eventuali supporti di memorizzazione locali.

Qualora vi fosse la necessità di mantenere gli archivi sarà mandata una email al Titolare che ne darà l'autorizzazione.

Gli archivi dei Titolari non potranno mai essere trasmessi a gruppi di lavoro differenti rispetto a quelli finalizzati alla risoluzione del problema segnalato dal Titolare.

L'unica possibilità che i tecnici hanno per conservare gli archivi senza la previa autorizzazione del Titolare è l'anonimizzazione degli stessi.

ASSISTENZA ATTRAVERSO LA NECESSITÀ DI AVERE IL BACKUP DEI CLIENTI DI UN SERVIZIO DATA CENTER

Qualora i dati personali del Titolare siano su sistema Zucchetti/Data center, in nessun caso l'assistenza di 1 livello potrà richiedere il backup ai sistemisti di Data center se non previa autorizzazione del Titolare stesso.

I sistemisti non potranno estrarre nessun backup dei Titolari per esigenze e finalità differenti rispetto al fornire assistenza agli stessi; ad esempio non potranno essere effettuati backup indirizzati alla produzione per l'esecuzione di test.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO ATTRAVERSO STRUMENTI A CIO' DEDICATI

Questa modalità di collegamento sugli strumenti dei clienti garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal cliente
- Le credenziali di accesso sono sempre individuali
- Il cliente ci fa accedere ad un ambiente con profilo di autorizzazione da lui scelto per farci eseguire le attività di assistenza
- Il cliente può sconnetterci quando desidera.

Attraverso tali strumenti è possibile far accedere anche l'assistenza di 2 livello alla stessa sessione da noi aperta. In questo caso il cliente ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità.

È essenziale utilizzare i nostri strumenti in quanto licenziati e personalizzati con tutta la documentazione che



deve essere prodotta dalla legge sul trattamento dei dati personali.

Solo in casi eccezionali e dopo attenta valutazione del responsabile e dell'ufficio privacy è possibile utilizzare altri strumenti di connessione che si comportano in modo uguale.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO SU IP PUBBLICI OPPURE TRAMITE VPN

Qualora l'attività di assistenza debba essere svolta su sistemi cloud su IP pubblici oppure tramite VPN o accessi privati è necessario che gli addetti Zucchetti entrino nei sistemi dei Titolari:

- Previa autorizzazione del cliente
- Previa ricezione delle credenziali individuali e le stesse siano state attivate per il tempo necessario all'esecuzione delle attività richieste
- al termine dell'attività siano disattivate le credenziali da parte del Titolare

Regole che riguardano gli ambienti dei Titolari, in qualsiasi forma di delivery (Saas/PaaS/On Premise) riferite a:

- creazione utenze per consulenti applicativi;
- creazione utenze per personale di assistenza.

Consulenti applicativi

Per effettuare tutte le attività di start up sull'ambiente del Titolare è necessario che venga appositamente creata un'utenza all'interno del sistema come di seguito indicato:

- ZU_ + prime 3 lettere del cognome + prime 3 lettere del nome
- nella descrizione (nome completo) apporre: Utente Zucchetti

In questo modo il Cliente potrà riconoscere la provenienza dell'utenza stessa.

Es: per il soggetto Rossi Mario dovrà essere creata l'utenza: ZU_ROSMAR

Per la creazione dovrà essere coinvolto il Titolare, il quale dovrà essere guidato all'accesso e alla creazione dell'utenza precisando e condividendo con lui, i diritti che verranno assegnati a quest'ultima.

Personale di Help Desk

La creazione dell'utenza deve essere richiesta solo al Titolare che, attraverso l'amministratore di applicazione, potrà creare il nuovo utente.

Non deve mai essere utilizzato l'utente amministratore da parte degli operatori di assistenza.

Anche in questo caso, per la creazione delle utenze, valgono le regole di creazione esplicitate per i consulenti applicativi

Le utenze dovranno essere generate con la codifica: ZU_prime tre cognome_prime tre nome

Nella descrizione dovrà essere inserito Zucchetti Utente

CONVERSIONI E PROGETTI DI START UP

Qualora si verifichino le seguenti casistiche:

- Conversione o start up con contratto
- Conversioni o startup senza contratto

Nel primo caso le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite.

In questo caso è necessario redigere un documento di progetto in cui si convengono con il Titolare le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati di cui necessita l'esecuzione delle attività
- Dettaglio delle operazioni da eseguire sui dati



- Identificazione del periodo entro cui sarà terminata tale attività
- La previsione di un collaudo in cui il Titolare proverà la conversione

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Zucchetti di svolgere tutte le attività necessarie all'erogazione del servizio.

In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Zucchetti, in qualità di responsabile, agli addetti Zucchetti.

Qualora non vi sia il contratto invece è necessario inviare al Titolare la nomina a responsabile al trattamento. Nella nomina dovrà essere previsto un termine di svolgimento e portata a termine dell'attività. Zucchetti provvederà ad incaricare gli addetti in qualità di responsabile.

Anche in questo caso è necessario prevedere una fase progettuale in cui condividere gli step sopra riportati. Al termine sarà anche in questo caso essenziale prevedere il collaudo.

Con il documento di collaudo, che dovrà essere sottoscritto dal Titolare, lo stesso ci dichiarerà che le attività da noi effettuate sono corrette e quindi ci autorizzerà a cancellare i suoi archivi.

Nel documento di collaudo dovranno essere inserite le seguenti indicazioni:

- Il lavoro svolto è conforme rispetto all'ambito contrattuale convenuto
- Il Titolare ha provato la conversione e dichiara che il prodotto funziona e tutte le funzioni sono state correttamente configurate e implementate
- Che non ci sono errori nei dati convertiti e che quindi potrà utilizzare il prodotto per le finalità per cui lo ha acquistato

Inoltre il Titolare deve dichiarare che dalla data della firma del contratto non avrà nulla a pretendere rispetto all'attività di conversione svolta e prevista dal contratto e che autorizza Zucchetti a cancellare ogni dato, archivio, data base che è servito per portare a termine la fase di conversione.

Solo qualora ci fosse la necessità di mantenere gli archivi del Titolare per finalità di cautela e verifica del lavoro da noi svolto, dobbiamo inviare una comunicazione con la quale il Titolare ci autorizza a conservare gli archivi per l'ulteriore periodo, terminato il quale gli archivi dovranno essere eliminati.

Tutto l'iter autorizzativo dovrà essere inserito nel post vendita al fine di averne memoria.

Tutti i documenti contenenti dati dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.



3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI – CLOUD – EROGATI DA AMAZON WEB SERVICES

Le misure di sicurezza adottate dal fornitore del servizio cloud sono consultabili al seguente link: <https://www.amazon.it/gp/help/customer/display.html?nodeId=201908990>

Il fornitore è stato nominato responsabile del trattamento mediante apposito atto di nomina consultabile al seguente link: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

CODICE	CLASSE DELLA MISURA	LIVELLO DI APPLICAZIONE
M1	Autenticazione	I servizi sono accessibili solo attraverso il superamento di una procedura di autenticazione che prevede l'utilizzo di credenziali associate agli incaricati. I sistemi prevedono l'accesso tramite chiave crittografata emessa direttamente da AWS e unica per ogni apparato.
M2	Autorizzazione	L'accesso ai dati è controllato attraverso i profili di autorizzazione definiti attraverso Identity Access Manager di Amazon AWS.
M3	Backup e Ripristino dei dati	Sono in atto politiche di backup per i dati ed attività indirizzate a ridurre il disservizio in caso di guasto (disaster recovery)

Classificazione e scheda dettagliata delle Misure di sicurezza adottate

CLASSE MISURA	MISURA	DESCRIZIONE SINTETICA
M1.	1.1 Adozione di procedure di gestione delle credenziali di Autenticazione: USERNAME	Tutti i lavoratori sono identificati nel sistema informativo attraverso una user name assegnata in modo univoco agli stessi. La User name non sarà associata ad altri lavoratori neppure in tempi diversi. Le username si suddividono in username per accesso ad ambienti di lavoro e username per accesso alle applicazioni funzionali. Ogni sistema ha la propria gestione e memorizzazione della username.
	1.2 Adozione di procedure di gestione delle credenziali di Autenticazione: PASSWORD	L'accesso ad ogni ambiente o strumento elettronico avviene attraverso credenziali di autenticazione. Ogni utente viene formato sulle regole minime di composizione della password (almeno 8 caratteri e costituita da caratteri alfanumerici non facilmente riconducibili al soggetto di appartenenza). L'utente viene edotto sulla necessità di modifica delle password ogni sei mesi nel caso in cui tratti dati personali e ogni tre mesi qualora tratti dati sensibili.



		Gli strumenti utilizzati per i trattamenti spesso non gestiscono in autonomia il cambio password, né effettuano controlli sulla ripetitività delle stesse password nel tempo per cui tali adempimenti sono a carico dello stesso utente. Le password di tutti i sistemi elettronici quando vengono digitate sono in formato inintelligibile, cioè riportano asterischi e non caratteri alfanumerici.
	1.3 Uso esclusivo delle credenziali di autenticazione.	Ogni credenziale di autenticazione (username e password) viene assegnata ad un unico operatore che la utilizzerà in modo esclusivo.
	1.4 Verifica delle credenziali	Tutte le credenziali sono verificate con cadenza annuale, in occasione della redazione della DPIA, al fine di controllarne l'effettiva corrispondenza con le mansioni effettivamente svolte.
M2	2.1 Profilo di autorizzazione per singolo incaricato	Detto processo garantisce, a fronte del superamento della fase di autenticazione, la corretta e completa associazione tra utenza ed oggetti del sistema informatico connessi al profilo assegnato; comprende l'insieme delle informazioni, associate ad una persona, dirette ad individuare a quali dati essa possa accedere ed altresì di quali trattamenti essa possa usufruire; esso stabilisce a quali aree del sistema informatico l'incaricato possa accedere e quali azioni, una volta entrato, possa compiere.
	2.2 Aggiornamento periodico dei profili di autorizzazione	Ad ogni incaricato, prima di iniziare il trattamento, viene configurato un profilo di autorizzazione. Il profilo di autorizzazione viene configurato dal coordinatore del gruppo di lavoro di cui la risorsa farà parte, valutando profili analoghi di colleghi che prestano la stessa attività professionale ed evidenziando le eccezioni.
M3	3.1 Procedure di backup	Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza giornaliera
	3.2 Procedure di ripristino	Sono adottate idonee misure atte a garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni. Sono altresì previste attività indirizzate a ridurre il disservizio in caso di guasto.