DOCUMENTO DI SINTESI E DI ASSUNZIONE DELLE RESPONSABILITA'

Obiettivi del documento:

Il documento redatto e sottoscritto digitalmente dall'Amministratore della Unidos S.r.l. costituisce un documento di sintesi dei prodotti software della Unidos S.r.l. e definisce, con chiarezza, le responsabilità oggettive e soggettive della Unidos S.r.l. in merito a:

Conservazione a norma dei documenti digitali del cliente;
conservazione digitale e archiviazione elettronica dei dati informatici del cliente;
modalità del trattamento informatico dei dati informatici del cliente;
trasparenza e sicurezza informatica dei procedimenti;
posizione geografica dei server sui quali sono archiviati i dati informatici del cliente;
personale incaricato al trattamento;
procedure di disaster recovery.

Forma del documento

Il documento è redatto nella forma della dichiarazione sostitutiva dell'atto di notorietà ai sensi dell'art. 47 D.P.R. 28 dicembre 2000, n.445. Gli Amministratori della società Unidos S.r.l. Guido Palladino e Nicola Palladino firmano il documento consapevoli delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art.76 D.P.R. 445 del 28/12/2000. La dichiarazione ai sensi dell'art. 38, D.P.R. 445 del 28/12/2000, è sottoscritta dagli Amministratori della Unidos S.r.l. a mezzo digitale unitamente a copia fotostatica, non autenticata di un documento di identità.
Il presente documento è esclusivamente redatto e consultabile in formato digitale. Al suo interno sono presenti link consultabili che puntano a normative, comunicati e documenti ufficiali degli enti preposti al controllo e all'emanazione di leggi, note e aggiornamenti. A titolo esemplificativo e non esaustivo AgiD, Ministero della Pubblica Istruzione, Aruba S.p.A.

Destinatari del documento

Il documento è destinato ai clienti della Unidos S.r.l. nelle persone dei legali rappresentanti responsabili dei dati.
Per i clienti Comuni italiani il sig. Sindaco, per i clienti Istituti scolastici il Dirigente Scolastico, per le associazioni di Comuni, il rappresentate legale nominato in fase di associazione, per le Aziende il legale rappresentante con poteri di firma, per le altre Pubbliche Amministrazioni i Dirigenti responsabili.

Software di proprietà intellettuale della Unidos S.r.l.

Il documento riguarda tutti i software progettati e sviluppati dalla Unidos S.r.l., di seguito un elenco.

Segreteria Cloud (SC)
Registro Cloud (RC)
Unidos Request (UR)
USyncro (US)
Amministrazione Trasparente Web (AmmTrasp)
Albo Pretorio On-Line (Albo)
M@ilFax (MF)
Unidos Conservazione Automatica (UCA)
Unidos SMS (USM)
Unidos WhatsApp (UWP)

Unidos APP per cellulari e tablet
Space APP (SPAPP)
Firma PDF tablet (SignPDF)
Controllo Accessi alunni
Altro software sviluppato

L'elenco dei software è soggetto a revisione.

Modalità di trattamento dei dati e procedimenti

Il documento definisce le procedure, le figure e le relative responsabilità:

> Conservazione a norma dei documenti digitali del cliente;

Nel rispetto di quanto previsto da Agid il sistema di conservazione adottato in Segreteria Cloud garantisce autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, come previsto dal CAD (art.44).
AgID definisce le modalità operative per realizzare l'attività di conservazione. Si tratta delle definizioni di natura e funzione del sistema, modelli organizzativi, ruoli e funzioni dei soggetti coinvolti, descrizione del processo.

Le indicazioni di dettaglio delle regole tecniche sono raccolte in specifici allegati che ampliano il quadro di riferimento dell'attività di conservazione.

In particolare:

Glossario/Definizioni
Formati
Standard e Specifiche tecniche
Specifiche tecniche del pacchetto di archiviazione
Metadati

A partire dall'11 ottobre 2015 le Pubbliche Amministrazioni sono tenute, in base all'articolo 7, comma 5 delle Regole tecniche per il Protocollo informatico, ad inviare in conservazione il registro giornaliero di protocollo entro la giornata lavorativa successiva. A tal proposito, sono disponibili Istruzioni per la produzione e conservazione del registro giornaliero di protocollo.

Il 10 dicembre 2015 sono state pubblicate le linee guida sulla conservazione dei documenti informatici, tale documento, indirizzato in particolare alle P.A., è da intendersi come documento dinamico attualmente in fase di sviluppo. Osservazioni e contributi possono essere inviati alla casella di posta elettronica forum_conservatori@agid.gov.it

Presentazioni:
Nuove regole tecniche conservazione e accreditamento conservatori
Conservazione dei documenti informatici delle P.A. Conservazione dei documenti informatici delle P.A._ver_acc Brochure conservazione
Documenti d'indirizzo:

Modello di Manuale di conservazione per le università e per gli enti di ricerca di Procedamus

Normativa

Circolari e deliberazioni

- Circolare 10 aprile 2014, n. 65 - Accreditamento e vigilanza conservatori
- Circolare 29 dicembre 2011, n.59 - Accreditamento conservatori
- Delibera Cnipa 19 febbraio 11/2004- Regole tecniche per la riproduzione e conservazione

Leggi decreti e direttive

- DPCM 3 dicembre 2013 - Regole tecniche sistema conservazione

Elenco conservatori accreditati

Segreteria Cloud adotta il sistema di conservazione a norma di **Aruba Posta Elettronica Certificata S.p.a** con sede in Via San Clemente n. 53 – 24036 Ponte San Pietro (BG) legale rappresentante Simone Braccagni, Manuale conservazione Aruba ver. 1.2
Il versamento in conservazione dei file avviene secondo le specifiche tecniche previste da AgID.

Segreteria Cloud è un "sistema di gestione informatica dei documenti", o sistema di protocollo informatico, è rappresentato dall'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati da una Pubblica Amministrazione per la gestione dei documenti, ossia per lo svolgimento delle attività finalizzate alla formazione, ricezione, spedizione, registrazione, classificazione, fascicolazione, assegnazione, gestione e reperimento dei documenti amministrativi formati o acquisiti da un ente, nell'ambito del sistema di classificazione d'archivio adottato.
In particolare, esso deve garantire la produzione e l'archiviazione del registro informatico di protocollo nel rispetto dei requisiti di natura giuridica che fanno di questo documento un atto pubblico di fede privilegiata. Non si tratta quindi di un generico sistema informatico sul quale memorizzare i dati identificativi dei documenti ricevuti o spediti, bensì di un sistema idoneo allo svolgimento di operazioni giuridicamente rilevanti ed essenziali per la formazione dell'archivio digitale. In quest'ottica, si comprendono i requisiti minimi di sicurezza riportati nell'articolo 7 del DPCM 3 dicembre 2013, che obbligano le Pubbliche Amministrazioni ad utilizzare sistemi di protocollo informatico capaci di assicurare:

a) l'univoca identificazione e autenticazione degli utenti. Al riguardo, si ricorda che l'uso delle credenziali di accesso, genericamente rappresentate da user-id e password o di account G Suite di Google, equivale ad apporre una firma elettronica sulle registrazioni effettuate. Una firma elettronica che, ai sensi dell'articolo 21, c. 1 del Codice dell'Amministrazione Digitale (CAD), sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità;

b) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, effettuata in modo da garantire l'identificazione dell'autore e impedire qualsiasi modifica non autorizzata;

c) il tracciamento di qualsiasi evento di modifica delle informazioni trattate con l'individuazione dell'autore. In un sistema di protocollo informatico a norma, quindi, ogni utente deve avere le credenziali di identificazione con associato un profilo di accessibilità, che specifica le operazioni che può compiere sul sistema.

Ogni accesso e ogni operazione eseguita sarà tracciata in modo da individuare i soggetti che le eseguono e quindi attribuire le responsabilità in caso di irregolarità accertate o gravi errori di trattazione. In queste circostanze, si applicherà il citato articolo 21, c. 1, del Codice dell'Amministrazione Digitale e quindi in sede giuridica sarà valutato il livello di sicurezza ed affidabilità delle credenziali di accesso, nonché delle misure adottate per garantire l'integrità e l'immodificabilità delle registrazioni, e si procederà di conseguenza all'attribuzione delle responsabilità personali. Tra i requisiti minimi di sicurezza, il legislatore ha indicato anche il controllo differenziato dell'accesso alle risorse del sistema di protocollo informatico per ciascun utente o gruppi di utenti, rendendo obbligatoria l'adozione delle misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al Decreto Legislativo n. 196/2003(3).

A queste disposizioni, già in vigore da anni, l'articolo 7 del DPCM 3 dicembre 2013 aggiunge l'obbligo di trasmettere il registro giornaliero di protocollo, entro la giornata lavorativa successiva, al sistema di conservazione, garantendo l'immodificabilità del contenuto. In definitiva, al sistema di protocollo informatico sono richieste funzionalità tali da garantire la registrazione dei dati identificativi dei documenti (numero e data di protocollo, oggetto, mittente o destinatario) in un'unica operazione, la produzione giornaliera del registro di protocollo informatico e la sua trasmissione ad un sistema di conservazione digitale a norma.
La gestione dei documenti informatici, sia in entrata che in uscita, rende necessarie funzionalità specifiche per la loro ricezione e trasmissione attraverso il canale della posta elettronica certificata, nonché per la registrazione e segnatura informatica di protocollo. Innanzitutto, anche in considerazione di quanto stabilito dall'articolo 18, c. 2, del DPCM 3/12/2013, che impone alle Pubbliche Amministrazioni l'obbligo di istituire una casella di Posta Elettronica Certificata (PEC) per ogni AOO direttamente associata al registro di protocollo generale, si rileva l'opportunità dell'integrazione funzionale tra il servizio di PEC e il sistema di protocollo informatico, che permetta di acquisire automaticamente i messaggi in entrata e formare quelli in uscita, allegandovi i documenti con le relative segnature di protocollo.

Responsabilità del servizio di conservazione

La Unidos S.r.l. si assume la responsabilità di garantire la registrazione e la successiva trasmissione al sistema di conservazione di **Aruba Posta Elettronica Certificata S.p.a** secondo quanto previsto dalla normativa. La responsabilità del mancato versamento è a capo degli amministratori della Unidos S.r.l.
In caso di mancata trasmissione per eventi tecnici di forza maggiore la Unidos S.r.l. provvede a far redigere un apposito verbale nel quale il Dirigente scolastico, in qualità di responsabile della conservazione motiva l'anomalia tecnica che ha comportato il mancato versamento.
Il Dirigente scolastico, in generale il legale rappresentate non ha alcuna responsabilità sulle modalità di conservazione del dato che sono a carico di Unidos S.r.l. per il procedimento di versamento e di **Aruba Posta Elettronica Certificata S.p.a** per il procedimento di conservazione a norma**.**

Conservazione digitale e archiviazione elettronica dei dati informatici del cliente

La Unidos S.r.l. adotta un primo livello di archiviazione digitale del documento su server dedicati situati presso la struttura di **Aruba Posta Elettronica Certificata S.p.a,** un secondo livello di archiviazione digitale del documento presso la struttura di **Google GSuite drive** un terzo livello di archiviazione digitale del documento presso la propria struttura su server dedicati e supporti NAS a caldo e un quarto livello di archiviazione digitale del documento presso la struttura **OneDrive di Microsoft Office 365.**
Schema grafico dell'archiviazione digitale del documento protocollato in Segreteria Cloud:

File ⇨ Protocollo ⇨ Server Web di Aruba ⇨ Google Drive ⇨ Unidos S.r.l. ⇨ Microsoft

I procedimenti utilizzano crittografia a norma e trasporto dei dati attraverso protocolli di sicurezza SSL.
Il terzo e il quarto livello sono di backup.
Informazioni sul trattamento da parte di Google dei dati sono reperibili all'indirizzo https://www.google.it/intl/it/policies/privacy/ e https://privacy.google.com/?hl=it

Responsabilità del servizio di archiviazione elettronica dei dati informatici del cliente

La Unidos S.r.l. si assume la responsabilità sul trattamento dei dati e sui procedimenti di conservazione elettronica dei dati.
Si esonera il cliente dalla diffusione o perdita accidentale del dato archiviato digitalmente nell'uso dei prodotti Unidos S.r.l.

Modalità del trattamento informatico dei dati informatici del cliente

Ai sensi ed agli effetti del 'Codice in materia di protezione dei dati personali' - D.Lgs. 30 giugno 2003 n.196 - la Unidos Srl., in qualità di Titolare del Trattamento, la informa che i suoi dati personali sono trattati esclusivamente per le finalità strettamente attinenti alla gestione e/o esecuzione dei rapporti contrattuali in base a quanto previsto dal Testo unico in materia di trattamento dei dati personali.

Unidos S.r.l. dichiara che i suoi dati personali sono raccolti presso la sede a seguito della ricezione di proposte d'acquisto effettuate mediante rete internet e/o mediante personale dei propri rivenditori e che, in ogni caso, tali dati personali sono trattati nel pieno rispetto degli obblighi di correttezza, liceità e trasparenza imposti dalla citata normativa a tutela della sua riservatezza e suoi diritti.

Premesso che ai fini del Codice per:

"**trattamento**" si intende, qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati;

"**dato personale**" si intende, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

"**dati sensibili**" si intendono, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazione a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"**dati giudiziari**" si intendono, i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.,

Finalità del trattamento:

I suoi dati personali sono trattati per l'esclusivo assolvimento degli obblighi contrattuali e per finalità strettamente connesse e strumentali alla gestione dei contratti.
Unidos S.r.l. intende raccogliere, mantenere e trattare i suoi dati personali esclusivamente per le seguenti finalità:

- Fornire servizi di assistenza alla clientela, come il rilascio dei codici di attivazione dei programmi, visualizzazione dello status degli ordini inevasi, di quelli già forniti e la relativa fatturazione.
- Fornire servizi di assistenza on line alla clientela.
- Facilitare e soddisfare le sue ricerche e richieste di informazioni su prodotti e servizi offerti
- Fornire informazioni relativamente ai prodotti e servizi più recenti, ivi inclusi aggiornamenti e offerte speciali alle quali lei potrebbe essere interessato.
- Inviare, tramite posta elettronica, informazioni sugli aggiornamenti dei prodotti software.
- Organizzare offerte promozionali.

Trasparenza e sicurezza informatica dei procedimenti

Unidos S.r.l. adotta e rispetta il **Regolamento generale per la protezione dei dati personali** n. 2016/679 (General Data Protection Regulation o **GDPR**) e la normativa di riforma della legislazione europea in materia di protezione dei dati.
Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016.
Si deve precisare che la sua attuazione avverrà il **25 maggio 2018**.

I dati i dati personali sono **trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato, ribadendo quei principi di liceità, correttezza e trasparenza che assumono un'importanza cruciale nell'era tecnologica.

La Unidos S.r.l. è disponibile, nella propria sede, su richiesta del cliente a mostrare i documenti di sviluppo e funzionali di ciascun prodotto realizzato.

Posizione geografica dei server sui quali sono archiviati i dati informatici del cliente;

Aruba S.pa. – https://www.datacenter.it/home.aspx
Posizione dei server Unidos S.r.l. – Milano.

G. Suite di Google - https://gsuite.google.it/intl/it/faq/security/

Personale incaricato al trattamento;

La Unidos S.r.l. si avvale di figure professionali e specializzate per ciascun settore, di seguito l'organico

Nicola Palladino
Amministratore delegato con poter limitati.
Fabiana Pasqualone
Responsabile della formazione
Salvatore Rauso
Responsabile del call center
Responsabile dell'ufficio commerciale
Giuseppe Cornacchione
Account Commerciale e vendite
Italo Rosario Amorosa
Responsabile progetto Google G. Suite e Microsoft Office 365
Vicenzina Ianiero
Addetta al call center
Supporto e consulenza normativo e contabile
Daniela Barresi
Addetta al call center
Supporto e consulenza normativo e contabile
Marino Fusaro
Responsabile del settore Tecnico
Tecnico informatico
Responsabile interventi tecnici on-site
Marino Battista
Tecnico informatico
Andrea Salvatore
Sviluppatore software e development architect
Daniele Romanella
Sviluppatore software e development architect
Giuseppe Russo
Sviluppatore software e development architect
Domenico Pinto
Responsabile dello Sviluppo
Sviluppatore software e development architect
Rocco Caruso
Sviluppatore software e development architect
Flavio Mastrangelo
Sviluppatore software e responsabile del progetto Registro Cloud

Avv Michele Barisciano dello studio Barisciano
Recupero crediti e consulenza normativa

Guido Palladino
Consulente esterno con contratto di supporto normativo e di controllo
Amministratore di sistema
Antonio Esempio
DPO - RPD

Procedure di disaster recovery

Il CAD sancisce che gli uffici pubblici devono essere organizzati in modo che sia garantita la digitalizzazione dei servizi (art. 15 "Digitalizzazione e riorganizzazione"). Da tale indicazione consegue, per la Pubblica Amministrazione (nel prosieguo PA), anche l'obbligo di assicurare la continuità dei processi che presiedono alla erogazione dei propri servizi, quale presupposto per garantire il corretto e regolare svolgimento della vita nel Paese.
Come detto i dati, le informazioni e le applicazioni che li trattano sono ormai parte essenziale ed indispensabile per lo svolgimento delle funzioni istituzionali di un ente/organizzazione ed è necessario quindi garantirne la salvaguardia, la disponibilità, la sicurezza, unitamente a confidenzialità ed integrità: il tema della continuità operativa deve quindi essere parte integrante dei processi e delle politiche di sicurezza di un'organizzazione. In quest'ottica l'attuazione degli obblighi imposti dal l'art. 50 bis del CAD conduce le Amministrazioni ad adottare un percorso complessivo in materia di sicurezza di tutta l'organizzazione.
A titolo esemplificativo, la compromissione della continuità di un sistema informatico, può essere conseguenza di:

- errori/malfunzionamenti dei processi (il processo organizzativo che usa il servizio ICT non ha funzionato come avrebbe dovuto per errori materiali, errori nell'applicazione di norme ovvero per il verificarsi di circostanze non adeguatamente previste dalle stesse);
- malfunzionamento dei sistemi, delle applicazioni e delle infrastrutture;
- attacchi o eventi naturali di tipo accidentale;
- disastri.

La Continuità Operativa ICT riguarda il processo critico ICT che, nel caso di grave e prolungata indisponibilità dei sistemi informativi (disservizio incompatibile con le esigenze di continuità di funzionamento dell'Amministrazione), prevede anche il Disaster Recovery per garantire il ripristino dello stato del Sistema Informativo (o di parte di esso), per riportarlo alle condizioni di funzionamento e di operatività antecedenti all'evento disastroso.

Unidos S.r.l. adotta tutte le misure previste dalle linee guida DR di AgID, disponibili all'indirizzo http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf
La Unidos S.r.l. ha redatto il **Piano per la sicurezza informatica Disaster Recovery e continuità operativa** che pone l'accento sui seguenti obiettivi in accordo con le leggi e le regole interne:

a) per le risorse tecnologiche:
   - la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali, tramite la formulazione di appropriati piani di recupero delle funzionalità del sistema;
   - la continuità del servizio a copertura delle esigenze operative dell'ente

b) per i dati:
   - la riservatezza delle informazioni;
   - l'integrità delle informazioni;
   - la correttezza delle informazioni ritenute critiche per le eventuali conseguenze derivanti da una loro alterazione;
   - la disponibilità delle informazioni e delle relative applicazioni.

Procedure di backup

A prescindere dal software in uso presso l'ente il sistema di backup di Unidos S.r.l. garantisce la copia giornaliera delle basi di dati e consente il ripristino immediato delle informazioni.

Unidos S.r.l. non garantisce il salvataggio dei dati delle postazioni del cliente. A tale scopo è in via di sviluppo il progetto Unidos Backup per garantire la copia anche dei dati delle singole postazioni

Firme del documento

Il sottoscritto Nicola Palladino Amministratore della Unidos S.r.l. nato a Campobasso il 24/06/1949 CF: PLLNCL49H24B519Z consapevole delle sanzioni penali richiamate dall'art. 76 del D.P.R. 445 del 28 dicembre 2000 per i casi dichiarazioni non veritiere, di formazione o uso di atti falsi **dichiara che quanto riportato nel presente documento è conforme a verità ed esonera il cliente nella persona del rappresentante legale pro tempore da qualunque responsabilità in merito alle informazioni trattate ed elencate nel documento.**

Campobasso 15/09/2022

In fede

Nicola Palladino
Amministratore delegato