LA CONSERVAZIONE DIGITALE NEGLI STUDI PROFESSIONALI

Tra obblighi e opportunità

Centro Studi Nazionale ANCL
29 luglio 2024

DI COSA DISCUTEREMO OGGI:

1. CONSERVAZIONE DIGITALE DEI DOCUMENTI E DEI DATI
2. MODALITÀ E PROCEDURE DI CONSERVAZIONE INFORMATIZZATA DEI DATI DELLA CLIENTELA
3. NUOVE MODALITÀ DI COMUNICAZIONE DENTRO E FUORI LO STUDIO PROFESSIONALE:
   a) COMUNICAZIONE INTERNA E GESTIONE DELLE INFORMAZIONI
   b) COMUNICAZIONE EFFICACE ED EFFICIENTE CON IL CLIENTE
4. SFRUTTIAMO I DATI: AUTOMATIZZARE I PROCESSI E ANALISI DEI DATI
5. DIGITALIZZAZIONE E PRIVACY: LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI
6. DATA BREACH: QUANDO SI CONFIGURA

BARBARA GARBELLI

Consulente del Lavoro in Pavia
Membro del Centro Studi Nazionale ANCL
Componente Comitato Scientifico ASRI

La registrazione del webinar la trovi nell'area riservata ai soci di **www.ancl.it**

CONSERVAZIONE DIGITALE DEI DOCUMENTI

CONSERVAZIONE DIGITALE: PREMESSA

La **conservazione digitale** è un processo disciplinato che consente di mantenere i documenti in formato digitale. **Questo processo permette, nei casi previsti dalla norma, di eliminare l'originale cartaceo o di evitare la sua stampa**. Il suo scopo principale è garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti.
Con la **digitalizzazione delle imprese**, la **conservazione digitale dei documenti** è diventata una procedura della quale le aziende dei vari settori professionali non possono più fare a meno.
Negli ultimi anni, l'esigenza di ridurre tempi e costi e di ottimizzare gli spazi interni aziendali si è fatta sempre più sensibile. Non esiste quasi più, infatti, un'azienda che non si trovi a dover gestire non centinaia, ma addirittura migliaia, di documenti digitali.
Considerando i documenti nativamente digitali, e non più cartacei, la conservazione digitale, deve diventare una prassi.
Tutte le procedure e i processi di un'azienda moderna devono essere indirizzati all'ottimizzazione del lavoro e ad una sempre più rapida digitalizzazione dei processi, abbandonando le procedure analogiche e sfruttando i **documenti digitali**.

Vediamo, dunque, nel dettaglio, come applicare normative e regole che governano la formazione, la gestione e la conservazione dei documenti informatici

CONSERVAZIONE DIGITALE DEI DOCUMENTI

CONSERVAZIONE DIGITALE: DI COSA SI TRATTA

Per **conservazione digitale documenti** si intende, nello specifico, il processo grazie alla quale i documenti e i fascicoli informatici possono diventare accessibili, leggibili, autentici e legali.
Ogni documento elettronico contiene al suo interno una vasta gamma di metadati e, grazie alla **conservazione elettronica documenti**, qualsiasi informazione specifica può essere individuata nel giro di pochi secondi.
Una **conservazione digitale a norma**, ad esempio, consente alle aziende di poter gestire al meglio tutte le pratiche interne ed esterne, ottimizzando i tempi di ricerca e controllo dei documenti digitali, con l'assicurazione che essi siano integri, sicuri e legali.

Per assicurare il **digital trust** ovvero la fiducia nel digitale e nei suoi processi, la **conservazione documenti digitali** è fondamentale, proprio perché garantisce i criteri di certezza e sicurezza. La **conservazione digitale**, infatti, prevede che all'interno di ciascun documento digitale siano presenti delle informazioni essenziali, fondamentali per attestare l'autenticità e la validità legale del documento.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

CONSERVAZIONE DIGITALE: DI COSA SI TRATTA

Nel settore della **conservazione elettronica documenti**, i fattori che non possono mai mancare e che sono essenziali in questo campo sono:

A. la **firma digitale:** firma di tipo elettronico con lo stesso valore legale di un classico autografo su formato cartaceo;
B. la **marca temporale:** che attesta il momento esatto nel quale il documento è stato generato e redatto, in base a un processo informatico ben definito e normato;
C. il **formato:** essenziale per rendere un documento valido e può essere in:
    1. PDF
    2. TIFF
    3. JPG
    4. Office Open XML (OOXML)
    5. Open Document Format
    6. XML
    7. TXT
    8. formati di messaggi di posta elettronica (RFC 2822/MIME)

CONSERVAZIONE DIGITALE DEI DOCUMENTI

CONSERVAZIONE DIGITALE: STRUMENTI DI CONSERVAZIONE

La sfera della **conservazione documenti informatici** è davvero molto ampia e racchiude al suo interno vari settori professionali. Dal riepilogo dei movimenti contabili alla definizione di introiti e perdite finanziarie, dalla situazione del magazzino all'insieme dei beni aziendali e sui quali effettuare l'ammortamento, senza dimenticare le fatture emesse, i modelli F23 e F24, la dichiarazione dei redditi e il versamento delle imposte, ciascun dettaglio può essere soggetto a questa procedura.

La conservazione digitale implica la **sostituzione dei documenti cartacei con documenti digitali equivalenti**, i quali mantengono la loro validità legale in termini di forma, contenuto e tempo. Questo è **garantito attraverso l'uso di una firma digitale e di una marca temporale.** Questi due strumenti assicurano l'immutabilità, l'autenticità, la reperibilità, il valore legale, la sicurezza, la leggibilità e l'integrità dei documenti conservati.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DIFFERENZA FRA ARCHIVIAZIONE DIGITALE E SOSTITUTIVA

ARCHIVIAZIONE SOSTITUTIVA

- Dematerializzazione del documento.
- Quest'ultimo viene convertito dal vecchio formato cartaceo a quello digitale, ma senza alcun tipo di validità giuridica obbligatoria.
- Ad oggi tale processo viene considerato obsoleto, dal momento che la validità giuridica risulta, oggi, essere essenziale.

ARCHIVIAZIONE DIGITALE

- contiene i moduli che già in origine erano disponibili in formato digitale. Grazie alla conservazione digitale, quindi, ogni documento elettronico è rivestito di un significato ancora più importante rispetto al passato.
- È di fondamentale importanza considerare la conservazione dei documenti informatici, come processo basilare per l'ottimizzazione e la messa in sicurezza di tutte le operazioni di una qualsiasi realtà aziendale, sia pubblica che privata

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DIFFERENZA FRA ARCHIVIAZIONE DIGITALE E SOSTITUTIVA, RIFLESSIONI

Per comprendere appieno la **conservazione digitale**, bisogna conoscere questo settore in maniera ancora più precisa. A tal proposito, chiedersi **cos'è la conservazione sostitutiva** e capire le sue differenze orientative rispetto a quella digitale, può fare la differenza e garantire, ad una realtà aziendale, un insieme di vantaggi pratici non di poco conto.

Ancora oggi, molti operatori del settore non conoscono la differenza tra **conservazione digitale e sostitutiva.** Si tratta di un errore di una certa rilevanza, dato che le differenze tra i due elementi sono notevoli. Chiariamo, dunque, la **differenza tra conservazione digitale e la conservazione sostitutiva.**

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DIFFERENZA FRA ARCHIVIAZIONE DIGITALE E SOSTITUTIVA, RIFLESSIONI

La **conservazione sostitutiva** non è altro che la **dematerializzazione di un documento**. Quest'ultimo viene convertito dal vecchio formato cartaceo a quello digitale, ma senza alcun tipo di **validità giuridica obbligatoria**. Ormai tale processo viene considerato obsoleto, dal momento che la validità giuridica risulta, oggi, essere essenziale.

La **conservazione digitale dei documenti** si è rivelata, d'altro canto, un passaggio fondamentale ai fini della produttività aziendale e della corretta gestione di ciascuna impresa.Questa, infatti, non si limita alla mera archiviazione di documenti nati in formato cartaceo, ma contiene anche i moduli che già in origine erano disponibili in formato digitale. Grazie alla **conservazione digitale**, quindi, ogni documento elettronico è rivestito di un significato ancora più importante rispetto al passato.

È chiaro, dunque, che al giorno d'oggi sia di fondamentale importanza considerare la **conservazione dei documenti informatici**, come processo basilare per l'ottimizzazione e la messa in sicurezza di tutte le operazioni di una qualsiasi realtà aziendale, sia pubblica che privata.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

PER QUALI DOCUMENTI E' NECESSARIA LA CONSERVAZIONE DIGITALE?

Quando si parla di **conservazione digitale** è lecito chiedersi quali documenti abbiano bisogno di essere conservati digitalmente. A tal fine, sarà utile introdurre il **concetto di conservazione digitale a norma**.

Considerato il fatto che ormai, in qualsiasi tipo di impresa, procedure e documenti sono per la maggior parte digitali, bisogna capire e distinguere i diversi tipi di documenti impiegati. All'interno di un'impresa, ad esempio, si lavora con diversi tipi di documenti che, per intenderci, divideremo in due categorie: **documenti senza valenza legale** e **documenti con valenza legale**.

I **documenti senza valenza legale** sono, per l'appunto, quei documenti che non sono giuridicamente vincolanti. **All'interno di un'impresa, ad esempio, sono documenti senza valenza legale: foto (jpeg), documenti interni e procedure come le ISO 9001. Per questi tipi di documenti non occorre la conservazione digitale, non necessitando, infatti, di validità legale e nel tempo.**

I **documenti con valenza legale**, come da definizione, sono **giuridicamente vincolanti e sono, ad esempio: documenti fiscali, documenti contabili e i contratti. Le caratteristiche principali di un documento digitale con valenza legale sono l'autenticità, la sicurezza, la validità nel tempo e l'opponibilità a terzi. Va da sé che i documenti con valenza legale vanno conservati digitalmente, seguendo norme e regole del processo.**

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: QUALI DOCUMENTI DEVONO OBBLIGATORIAMENTE ESSERE CONSERVATI DIGITALMENTE?

La prima cosa da sapere: quando la conservazione digitale è obbligatoria? I documenti da conservare obbligatoriamente secondo le metodologie e gli strumenti della conservazione digitale sono da ricondurre a quattro macrocategorie:

1. I documenti della pubblica amministrazione;
2. Le fatture elettroniche (aspetto che sarà approfondito in seguito);
3. Le email inviate tramite posta elettronica certificata (la PEC);
4. I contratti digitali ai quali sia stata apposta una firma digitale.

Chi, a vario titolo, sia nel settore pubblico sia nel settore privato, fosse il responsabile della conservazione di questi documenti, deve ricorrere alla conservazione digitale. Il che significa poter contare su competenze di un certo tipo, nonché poter disporre di specifiche tecnologie e metodologie.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

QUALI DOCUMENTI INVECE SI POSSONO CONSERVARE MEDIANTE LA CONSERVAZIONE DIGITALE?

1. **È necessario distinguere i documenti non unici** (fatture emesse e ricevute, scritture contabili, DDT, CU, note spese e giustificativi, LUL etc etc) per i quali è possibile sempre effettuare la conservazione sostitutiva o digitale a norma,
2. **dai documenti originali unici**, ossia cartacei con firme autografe, per i quali, invece, è necessaria una preventiva certificazione di processo,
3. **da quei documenti unici direttamente conservabili** come le PEC.

Esistono, inoltre, casi in cui la conservazione digitale a norma non è ammessa per la natura vincolante del documento, come, ad esempio, quelli di notevole interesse storico, oppure altri in cui vi è un obbligo di legge, come nel caso delle fatture elettroniche verso SdI.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

COME CONSERVARE UN DOCUMENTO DIGITALE

Per conservare digitalmente un documento, fondamentalmente, si seguono 3 step:

1. Il documento viene generato dal produttore che lo trasforma in un **pacchetto di versamento (PdV)**; viene apposta
   a) la firma digitale e
   b) la marca temporale sul PdV e
   c) viene consegnato al responsabile del servizio di conservazione.

2. Il responsabile della conservazione, firma e appone la marca temporale sul pacchetto di versamento, e lo converte in un **pacchetto di conservazione**.

3. Il sistema di conservazione mette a disposizione dei fruitori interessati il cosiddetto **pacchetto di distribuzione,** che contiene tutte le informazioni (metadati) che servono alla consultazione dei documenti contenuti nel pacchetto.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

CONSERVAZIONE O ARCHIVIAZIONE? LE DIFFERENZE

Come per qualsiasi documento digitale, sarà bene non confondere l'**archiviazione digitale** con la **conservazione digitale dei documenti**
Archiviare un documento digitale non equivale a salvarlo digitalmente.
La **conservazione digitale,** infatti, comprende un insieme di procedure tecniche, informatiche e giuridiche che non sono minimamente paragonabili a quelle della semplice **archiviazione digitale** .

Perchè?
L'**archiviazione digitale dei documenti** consiste nel **trasferire i documenti in cloud, o in un qualsiasi server dotato di un software di controllo. Questa procedura, però, può essere paragonata al mero "salvataggio" dei documenti e non alla conservazione.**
L'**archiviazione digitale**, pertanto, non riesce a garantire quelle che sono autenticità, leggibilità, integrità, valenza legale e la reperibilità di qualsiasi documento digitale, tutti elementi che, invece, sono assicurati dalla **conservazione digitale**.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

COSA E' E A COSA SERVE UN SISTEMA DI CONSERVAZIONE DIGITALE

Riassumendo tutto ciò di cui si è parlato finora, per rispondere alla domanda **cosa di intende per sistema di conservazione digitale,** si potrà dire che:
Un **sistema di conservazione digitale dei documenti** è l'insieme di quelle attività normativizzate, volte a **conservare, proteggere e custodire nel tempo**, tutti i **documenti digitali con valenza legale**, dell'impresa (pubblica o privata) presa in considerazione. Lo scopo fondamentale della **conservazione digitale** è quello di garantire autenticità, leggibilità, integrità, valenza legale e la reperibilità di qualsiasi documento digitale soggetto a tale processo.

A COSA SERVE LA CONSERVAZIONE DIGITALE

La **conservazione digitale dei documenti** serve a garantire soprattutto la **valenza nel tempo di un documento**, in ottemperanza all'obbligo di conservare a norma di legge, i documenti e le pratiche della sua attività per la durata stabilita dalla normativa (o dal singolo utente), nel rispetto dei precetti del GDPR.
La **conservazione digitale**, assicurando l'autenticità, l'integrità, la leggibilità, la reperibilità e la valenza legale, assicura difatti la **durata legale nel tempo di tutti i documenti adeguatamente conservati.**
Tutto ciò concorre a tutelare gli interessi sia dei clienti che delle imprese esercenti.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

ISTRUZIONI OPERATIVE PER LA CONSERVAZIONE DIGITALE DEL DATO

Nello specifico, il processo di conservazione elettronica deve presidiare sia la cosiddetta ***bit preservation***, cioè la capacità di **preservare i bit come erano stati originariamente registrati**, ma soprattutto la ***logical preservation***, intesa come la **possibilità di comprendere e utilizzare anche in futuro le informazioni contenute nel documento**. In argomento, però, occorre precisare che il riferimento al "documento informatico", ovviamente, **non può essere inteso solo in riferimento a un .pdf o all'immagine digitale di un documento cartaceo acquisita con lo scanner**, ma – in un'ottica dinamica, strutturata e multicanale – sono da considerare documenti informatici anche i flussi informativi di dati giuridicamente rilevanti, ovviamente opportunamente resi statici e immodificabili, anche attraverso sistemi di conservazione.
In tal senso, anche l'art. 3 di eIDAS (Regolamento 910/2014/UE) definisce un **documento elettronico come "qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva".**

CONSERVAZIONE DIGITALE DEI DOCUMENTI

NORMATIVA SULLA CONSERVAZIONE DIGITALE

La **conservazione digitale dei documenti** deve tutelare la valenza legale e la sicurezza di questi ultimi. A tal fine, la conservazione digitale viene regolata da specifiche norme e leggi ad essa dedicate.
Esistono, infatti, delle norme, europee e italiane, che è bene seguire per attuare la **conservazione digitale a norma**.
Esse sono:

1. Il **regolamento eiDAS**, atto a fornire la base normativa per interazioni elettroniche sicure tra i membri, quali che siano cittadini, pubbliche amministrazioni e imprese, dell'Unione Europea.
2. **Linee guida AgID,** che indicano le modalità di formazione, gestione e conservazione dei documenti informatici.
3. Il **CAD** (Codice dell'Amministrazione Digitale), un testo unico che organizza le norme che riguardano l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese.

Esiste, dunque,
una conservazione digitale
normativa che, tramite norme e
leggi, assicura la legalità e la
sicurezza dei documenti digitali,
sia per le pubbliche
amministrazione che per i privati.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

IL DOCUMENTO AGID SULLA CONSERVAZIONE DIGITALE DEI DATI

Il Le nuove Linee Guida sono disponibili sul sito di AgID e sono operative dal 1° Gennaio 2022.

Da questa data sono soggette alle nuove regole:
- **tutte le PA** italiane;
- i **soggetti privati** che trattano documenti informatici, ove non diversamente previsto.

Le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, hanno **carattere vincolante** e assumono valenza erga omnes.
Le "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" hanno sostituito le seguenti norme:

1. il DPCM 13 novembre 2014, contenente Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici;
2. il DPCM 3 dicembre 2013, contenente Regole tecniche in materia di sistema di conservazione;
3. il DPCM 3 dicembre 2013, contenente Regole tecniche per il protocollo informatico.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

IL DOCUMENTO AGID SULLA CONSERVAZIONE DIGITALE DEI DATI

Per applicare le nuove norme le Pubbliche Amministrazioni e gli operatori privati devono:

1. Nominare il **Responsabile della Conservazione** che opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD,
   predispone il Manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
2. Dotarsi di un **proprio Manuale di conservazione**
   1. dove illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione;
   2. nel manuale si potranno descrivere anche le attività del processo di conservazione affidate al Conservatore, in conformità con il contenuto del Manuale del servizio di Conservazione predisposto da quest'ultimo.
3. Nominare la **Nuova figura Titolare dell'oggetto della conservazione** identificato come la persona fisica o giuridica che ha la responsabilità di conservare per legge un documento, che corrisponde al soggetto detentore dell'Archivio.

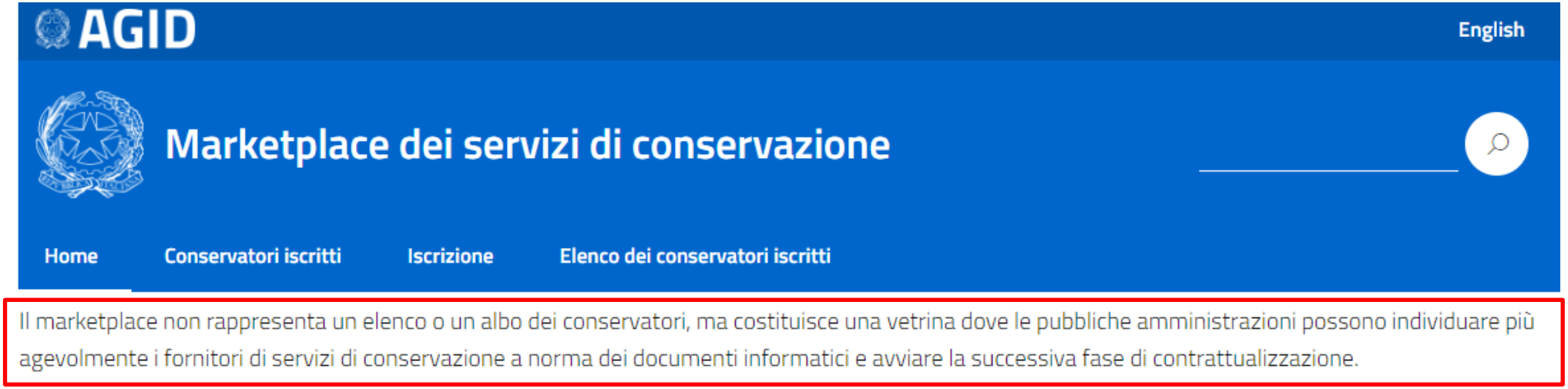
CONSERVAZIONE DIGITALE DEI DOCUMENTI

IL DOCUMENTO AGID SULLA CONSERVAZIONE DIGITALE DEI DATI

4. Eseguire le operazioni di **selezione e scarto** dei documenti informatici e, se conservati, dei Pacchetti di Archiviazione.
   Nel caso di archivi pubblici, o privati per i quali sia intervenuta una dichiarazione di **particolare interesse storico**, sarà richiesto al Titolare dell'oggetto della conservazione di inviare il nulla osta per lo scarto al responsabile del servizio di conservazione (conservatore accreditato ove presente) rilasciata ai sensi della normativa vigente in materia di beni culturali.
5. Stabilire i **formati dei file e i metadati** per la conservazione e il riversamento, come riportato nell'allegato 2 delle linee Guida.
6. Redigere/Aggiornare il **Manuale di Gestione documentale** che descrive il sistema di gestione informatica dei documenti, fornendo le istruzioni per il corretto funzionamento del servizio e per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
7. Nominare e attribuire compiti ad altri soggetti quali: **delegato del responsabile della conservazione**, **responsabile produttore**, **responsabile amministrativo**, **responsabile tecnico**.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

IL DOCUMENTO AGID SULLA CONSERVAZIONE DIGITALE DEI DATI



CONSERVAZIONE DIGITALE DEI DOCUMENTI

LA FIGURA DEL RESPONSABILE DELLA CONSERVAZIONE DIGITALE DEL DATO

«Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia»

Il Responsabile della Conservazione ha il compito di **definire la struttura del processo di conservazione** e far sì che vengano messe in atto tutte le **regole per l'archiviazione e la gestione documentale** a norma di legge.
Sempre a proposito di legge, **il suo ruolo è obbligatorio ove si decida di fare conservazione sostitutiva**.
Nel caso della Pubblica Amministrazione questo ruolo è assegnato a un dirigente della stessa mentre, **in caso di aziende, il Responsabile della conservazione può essere:**

- Un collaboratore **interno** (dipendente, socio, amministratore).
- Un collaboratore **esterno** (conservazione sostitutiva in outsourcing con delega), a patto che questi non corrisponda con il conservatore.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

LA FIGURA DEL RESPONSABILE DELLA CONSERVAZIONE DIGITALE DEL DATO

Tutto quello che occorre sapere sul Responsabile della Conservazione lo possiamo trovare nell'**articolo 7 del D.P.C.M. 3 dicembre 2013**. In particolare nel comma 1 troveremo definiti i suoi compiti.

Ecco un *breve estratto del comma 1:*
1.Il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi che, nel caso delle pubbliche amministrazioni centrali, coincide con il responsabile dell'ufficio di cui all'art. 17 del Codice, oltre che con il responsabile della gestione documentale ovvero con il coordinatore della gestione documentale ove nominato, per quanto attiene alle pubbliche amministrazioni.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

LA FIGURA DEL RESPONSABILE DELLA CONSERVAZIONE DIGITALE DEL DATO

In particolare il responsabile della conservazione:
a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

CONSERVAZIONE DIGITALE DEI DOCUMENTI

LA FIGURA DEL RESPONSABILE DELLA CONSERVAZIONE DIGITALE DEL DATO

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

IL MANUALE DELLA CONSERVAZIONE DEI DATI

Uno dei **compiti del Responsabile Conservazione** è quello di **redigere e mettere in atto le regole operative** che vengono **definite nel Manuale della Conservazione**, documento informatico **obbligatorio** che descrive l'intera organizzazione del processo di conservazione, la descrizione delle infrastrutture e dell'architettura informatica, inclusi i sistemi di sicurezza, i nominativi delle persone coinvolte nell'intero processo e i loro ruoli operativi.

Il Manuale della Conservazione è un documento che descrive l'organizzazione, in un'azienda, del processo di Conservazione digitale a norma. Contiene i soggetti che ne sono coinvolti, i ruoli, le responsabilità, il modello di funzionamento, la descrizione del processo, le architetture e le infrastrutture in uso, le misure di sicurezza e tutte le altre informazioni utili alla gestione e alla verifica del funzionamento del sistema di Conservazione.

La normativa prevede l'obbligo di conservazione per tutti i documenti validi ai fini fiscali.
In ambito aziendale, perciò, è obbligatorio conservare:
PEC (10 anni)
Fatture (10 anni)
Scritture contabili (10 anni)
Chi non conserva le fatture e i documenti contabili obbligatori è responsabile penalmente e incorre nel reato di distruzione di documenti contabili

CONSERVAZIONE DIGITALE DEI DOCUMENTI

QUALI ALTRE FIGURE IN AZIENDA?

Ma questo povero responsabile deve fare tutto da solo o può avvalersi di altre fidate persone che collaborano con lui nella gestione del processo di conservazione sostitutiva?
La risposta è ovviamente no, questa figura **può essere affiancato da altre** importanti figure, anche queste definite nell'articolo 7 del D.P.C.M. 3 dicembre 2013.

Queste figure sono:

- ❑ Il responsabile del trattamento dei dati personali
- ❑ Il responsabile della sicurezza
- ❑ Il responsabile dei sistemi informativi
- ❑ Il responsabile della gestione documentale

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: CHE VALORE HA UNA FIRMA SCANSIONATA?

Il valore della firma scansionata varia a seconda del tipo di documento.

Nel caso di un atto pubblico, il problema non si pone in assoluto, nessun Pubblico ufficiale, come potrebbe essere un Notaio, accetterebbe mai la firma scansionata e inviata da un soggetto del quale né possa accertare l'identità, né possa accertare l'effettiva volontà manifestata con la firma appunto.

La questione circa il valore della firma scansionata si pone quindi solo ed esclusivamente in ambito privato e porta a diverse conclusioni a seconda della situazione specifica.

Secondo l'articolo 2702 del Codice civile, infatti, la scrittura privata fa piena prova della provenienza delle dichiarazioni da chi l'ha sottoscritta se colui contro il quale la scrittura venga prodotta ne riconosce la sottoscrizione e così, tutte le volte in cui non sia richiesta per legge una sottoscrizione fatta di pugno, a parere di chi scrive qualunque segno grafico, anche precedentemente scansionato, può assolvere alla funzione di sottoscrizione.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: CHE VALORE HA UNA FIRMA SCANSIONATA?

La questione si pone quindi prevalentemente per una questione di tutela di chi il documento con la firma scansionata lo riceva, più che per chi lo invii.
Si pensi alla sottoscrizione di un abbonamento e al successivo sorgere di un contenzioso dovuto all'inadempimento del cliente.

Nel caso in cui quest'ultimo disconosca la firma, magari sostenendo che sia stata estrapolata da un diverso documento, il valore della firma scansionata e dell'intero documento su cui sia stata apposta sarebbe pari a zero e quindi ben si comprende come e perché nessuno accetterebbe o dovrebbe mai accettare un documento con firma scansionata.

Nuovi strumenti come la PEC e la firma digitale permettono non solo di accertare l'identità di un soggetto (come peraltro lo SPID) ma anche di dare prova dell'invio da un soggetto (certo) a un altro soggetto (certo) di un determinato contenuto (testo, scansione o altro) sul quale sia stata apposta la firma digitale (diversa dalla firma scansionata!).

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: CHE VALORE HA UNA FIRMA SCANSIONATA?

IN SINTESI

➢ Caratteristiche

Come suggerisce il nome, si tratta dell'***immagine*** **digitale di una firma autografa**.

La firma scansionata si ottiene attraverso una **procedura di digitalizzazione** (o scansione) di un documento cartaceo firmato previamente a mano e convertito in formato digitale (.doc, .pdf, ecc.).

🚨 La firma autografa scansionata non ha **alcun valore legale** per diversi motivi:

•non è possibile verificare l'identità del firmatario

•non è possibile dimostrare il consenso agli obblighi derivanti dal documento

➢ Livello di sicurezza

In termini di livello di sicurezza, questo tipo di firma è facilmente falsificabile.

In **assenza di prove**, la firma scansionata è considerata come **una copia** e non come una firma autentica! Non ha pertanto validità legale, in particolare per quanto riguarda i processi contrattuali aziendali.

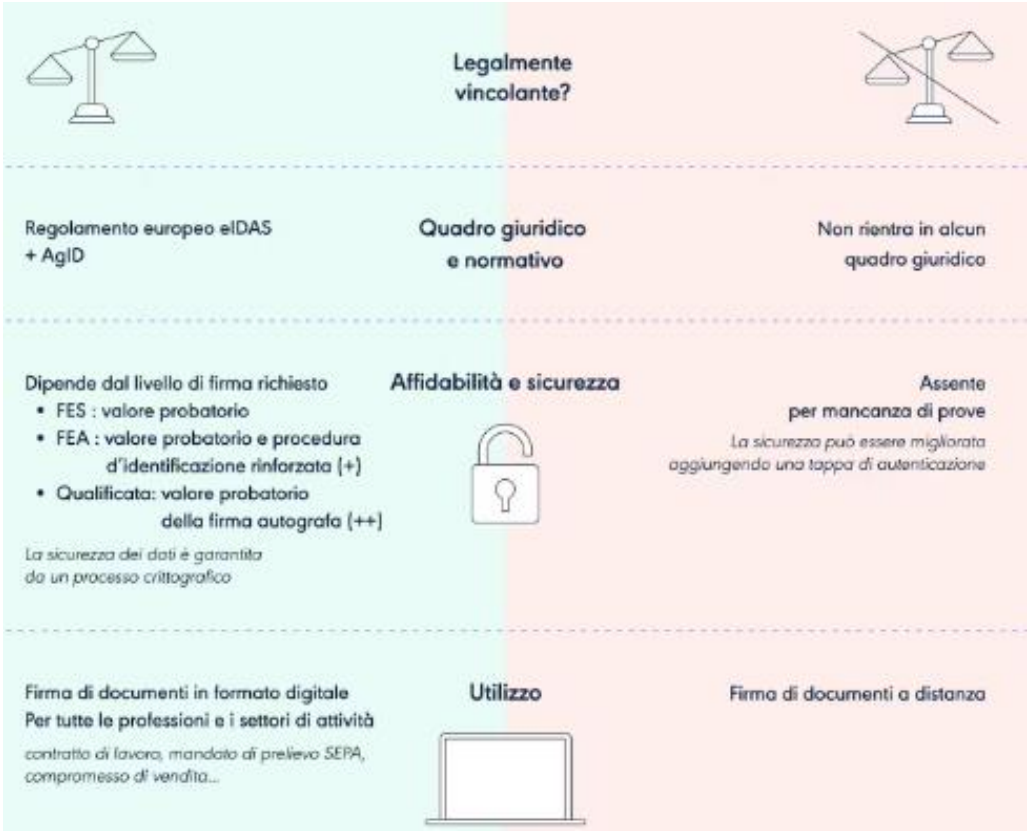
Nota*: anche nel caso si aggiunga una fase di autenticazione dell'identità del firmatario (ad esempio mediante un codice via SMS), la firma scansionata è comunque rischiosa, poiché non garantisce l'integrità del documento firmato.*

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI:
DIFFERENZA FRA FIRMA SCANSIONATA ED ELETTRONICA

La firma elettronica utilizza una procedura di crittografia a chiave pubblica collegando un certificato elettronico ai dati firmati.

È sempre possibile apporre la firma autografa direttamente sul documento stampato.
Una volta firmato e scannerizzato, deve essere inviato al destinatario tramite PEC o Raccomandata A/R.
La firma, così apposta, ha pieno valore legale.
N.B. Mai usare la scansione della firma.
La scansione della firma "incollata" sui documenti non ha infatti valore legale.



CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: CHE VALORE HA UN DOCUMENTO CON FIRMA AUTOGRAFA E DIGITALE?

Si può dire che un contratto di lavoro firmato dal datore di lavoro con firma digitale e dal lavoratore con firma autografa è giuridicamente valido e produce i suoi effetti?
In linea di principio, nulla vieta di formare un documento "misto": l'art. 7, comma 1, del Testo unico sulla documentazione amministrativa dice che "*I decreti, gli atti ricevuti dai notai, tutti gli altri atti pubblici, e le certificazioni sono redatti, anche promiscuamente, con qualunque mezzo idoneo, atto a garantirne la conservazione nel tempo*".
Non si vede il motivo per cui la forma promiscua non possa essere adottata anche per altri tipi di documenti.
Tuttavia, allo stato attuale della normativa, in molti casi questo principio può essere difficile o addirittura impossibile da applicare.
Se infatti un contratto deve risultare da un unico documento, esso non può essere contemporaneamente cartaceo e informatico: o l'uno, o l'altro. Nel caso esposto, il documento finale (cartaceo) non contiene le due sottoscrizioni, quella del datore di lavoro e quella del dipendente, ma la prima è sostituita dall'attestazione dell'esistenza di un documento informatico. Si tratta in sostanza di una sottoscrizione apposta a un documento diverso (copia asseverata da un pubblico dipendente) da quello originale.
La validità di un siffatto documento è legata alla possibilità che un contratto di lavoro possa essere costituito da due atti separati e la questione esula dal nostro campo di interesse.
Quello dei documenti "promiscui" è uno dei tanti problemi che dovranno essere risolti da legislatore.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: COME GESTIRE UN ARCHIVIO IBRIDO?

L'archivio ibrido indica un sistema all'interno del quale **coesistono sia i documenti in forma cartacea che i documenti digitali** ed è il tipico archivio che caratterizza questo particolare momento di transizione in attesa di un ufficio completamente *paperless*, una realtà destinata a verificarsi presto nell'ambito della conservazione documentale.

Il concetto di archivio ibrido è nato a seguito alla **trasformazione digitale** degli ultimi anni.
Ciò si deve soprattutto all'utilizzo di nuovissimi **software** per la redazione e conservazione dei documenti.
In questo modo da una parte c'erano sempre i documenti cartacei trasferiti sul digitale, mentre dall'altra hanno iniziato a nascere documenti già in formato digitale.
Le **difficoltà** date dalla presenza in azienda di un archivio ibrido nascono però nel momento in cui si devono **gestire due forme di documento**. Tutto questo può causare ad esempio una grande perdita di tempo e di efficienza per la ricerca di informazioni.

- **Differenza da dematerializzazione e digitalizzazione dei documenti**

Dematerializzazione e digitalizzazione sono due fenomeni molto diversi tra loro. Nell'ambito di un archivio ibrido è bene conoscere entrambi questi fenomeni, in quanto è possibile che entrambi coesistono all'interno del medesimo archivio. Vediamo di cosa si tratta.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: COME GESTIRE UN ARCHIVIO IBRIDO?

Con la **dematerializzazione** si intende un determinato processo che ha come risultato finale la creazione di un documento digitale. Questo proviene da un documento cartaceo – ovvero analogico. Ad esempio fa parte della dematerializzazione il procedimento di acquisizione ottica di un documento cartaceo.
La **digitalizzazione** invece indica la creazione, la validazione e la conservazione di documenti che in origine sono già digitali. Non sussiste quindi il passaggio da cartaceo a digitale – il documento nasce già come digitale. La firma digitale ad esempio può essere considerata come un fenomeno di digitalizzazione, perché nasce già in forma digitale. Non si verifica infatti una trasposizione dalla firma autografa.
Un altro aspetto da considerare è che la gestione di un archivio riguarda la produzione di documenti e il loro uso quotidiano. Ma comprende anche la **conservazione** degli stessi.
Secondo infatti la vigente legislazione, non solo i documenti dematerializzati ma anche quelli digitalizzati devono obbligatoriamente essere conservati nel corso del tempo seguendo alcune precise regole. Alcuni di questi documenti possono essere scartati dopo alcuni anni, mentre altri invece devono essere conservati permanentemente. In quest'ultimo caso è assolutamente necessario utilizzare formati che non vadano incontro ad una obsolescenza tecnologica – e di conseguenza utilizzabili nel tempo.

Nel processo di **gestione dell'archivio ibrido**, devono essere perciò previsti fin da subito dei sistemi adeguati per la conservazione digitale dei documenti. È inoltre necessario che tali documenti digitali confluiscano all'interno di sistemi di conservazione. Essi devono essere conformi alle attuali Regole tecniche sulla conservazione digitale. Devono cioè essere inclusi in sistemi che siano in grado di assicurare la corretta conservazione dei documenti digitali.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: COME GESTIRE UN ARCHIVIO IBRIDO?

Per gestire correttamente un archivio ibrido è necessario **prevedere la presenza di almeno tre elementi**.

Innanzitutto bisogna considerare gli **aspetti organizzativi**, ovvero predisporre un'organizzazione dell'archivio che riesca a ricorrere a procedure e regole di gestione documentali che siano efficaci e condivise. Per definire quali siano le regole e le procedure di gestione, formazione e conservazione di documenti digitali e cartacei bisogna che il responsabile della gestione documentale rediga due manuali:

•Il manuale relativo alla gestione dei documenti;
•Il manuale relativo alla conservazione dei documenti.

C'è poi bisogno di un **sistema di classificazione** per creare un archivio ibrido ordinato, e quindi stabilire delle regole per la gestione, formazione e conservazione dei documenti. Con il termine di *sistema di classificazione* si indica uno strumento di gestione documentale. Esso è capace di aggregare correttamente i documenti sulla base di attività e funzioni che vengono svolte da un'azienda.

Infine è necessario un **sistema informatico** che consenta il controllo e la gestione di processi e documenti – probabilmente l'aspetto più complesso tra i tre. Devi sempre considerare che la gestione di un archivio ibrido comporta l'adozione di soluzioni che siano a supporto dei flussi e della gestione documentale e dell'organizzazione stessa. Sostanzialmente c'è bisogno di sistemi che:

•Catturano e acquisiscono documenti attraverso scanner e/o piattaforme professionali;
•Registrano, classificano e gestiscono documenti e flussi documentali attraverso dei sistemi di gestione informatica dei documenti;
•Conservano correttamente documenti cartacei e digitali.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: COME CONSERVARE DIGITALMENTE IL LUL?

La compilazione del LUL come documenti informatici su supporti magnetici deve garantire di generare documenti elettronici, statici e immodificabili, nei formati idonei PDF/A o in alternativa PDF ma solo se si utilizzano con caratteri tipografici interoperabili, emettendo i file LUL con l'apposizione del riferimento temporale e della firma digitale del tenutario (Consulente del Lavoro, datore di lavoro o associazione di categoria che elabora il LUL), al fine di garantirne l'attestazione della data, l'autenticità e l'integrità.

È assolutamente ammessa l'apposizione della firma digitale su più file o blocchi del LUL elaborato, anche se riferiti allo stesso periodo paghe (ad esempio quando per motivi gestionali o di dimensione il tenutario suddivide su più file il libro unico del singolo mese).

Nella memorizzazione e successiva conservazione dei LUL dovrà sempre essere garantita la leggibilità nel tempo dei file, purché rimanga sempre assicurato l'ordine cronologico e non vi sia soluzione di continuità per ciascun periodo di paga (va garantita consecutività e un "collegamento" tra le registrazioni precedenti e successive del LUL). Ogni pagina del layout del LUL riporta una numerazione progressiva rispetto alla precedente.

Inoltre, secondo il decreto ministeriale, il sistema deve consentire le funzioni di ricerca e di estrazione delle informazioni dagli archivi informatici in relazione al cognome e nome e al codice fiscale del lavoratore, alla data del LUL e alle associazioni logiche di tali dati.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

DOMANDE FREQUENTI: COME CONSERVARE DIGITALMENTE IL LUL?

Il processo di registrazione, ossia di compilazione e memorizzazione dei documenti del Libro Unico, dovrà avvenire entro la fine del mese successivo al periodo paga di competenza, così come anche il termine di conservazione digitale a norma dei LUL prodotti dovrà essere ultimato entro massimo la fine del mese successivo al periodo paga di competenza, con l'apposizione della firma digitale del Responsabile della Conservazione o di un suo delegato e della marca temporale al fine di associare una data certa opponibile ai terzi.

Quindi, facendo un riepilogo del processo operativo, il tenutario dovrà generare, attraverso software, un documento informatico o n documenti LUL contenenti i dati registrati del periodo paga, firmando digitalmente ciascun file, anche tramite una soluzione di firma digitale con procedura automatica, e inviandoli successivamente al sistema di conservazione, secondo le regole tecniche AgID in materia di conservazione dei documenti informatici.

Naturalmente il LUL può essere messo a disposizione del Lavoratore in una modalità digitale e tracciabile, in modo da non dover mai materializzare su carta il LUL.

In merito al luogo di tenuta e conservazione, la norma stabilisce che il LUL debba essere conservato ed esibito agli organi di controllo presso il tenutario, che dovrà rendere disponibili i documenti, anche tramite modalità telematica, ad esempio attraverso il download e l'esibizione dei pacchetti di distribuzione dal servizio di conservazione adottato.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

I VANTAGGI DELL' ARCHIVIAZIONE DIGITALE

MAGGIORE EFFICIENZA	MINORI COSTI E OTTIMIZZAZIONE DELLE RISORSE
Evoluzione processi amministrativi imprese	Eliminazione degli archivi cartacei
Collaborazione cliente/fornitore	Riutilizzo dello spazio recuperato
Immediato reperimento documenti	Paperless
Svincolo da postazioni fisiche di lavoro	Saving di budget
Sicurezza dati processati	Saving imposta di bollo sul libro giornale
Eliminazione vincoli durante le fasi di esibizione alle autorità di controllo	Personale riconvertito a maggior professionalità
	Scelta green

CONSERVAZIONE DIGITALE DEI DOCUMENTI

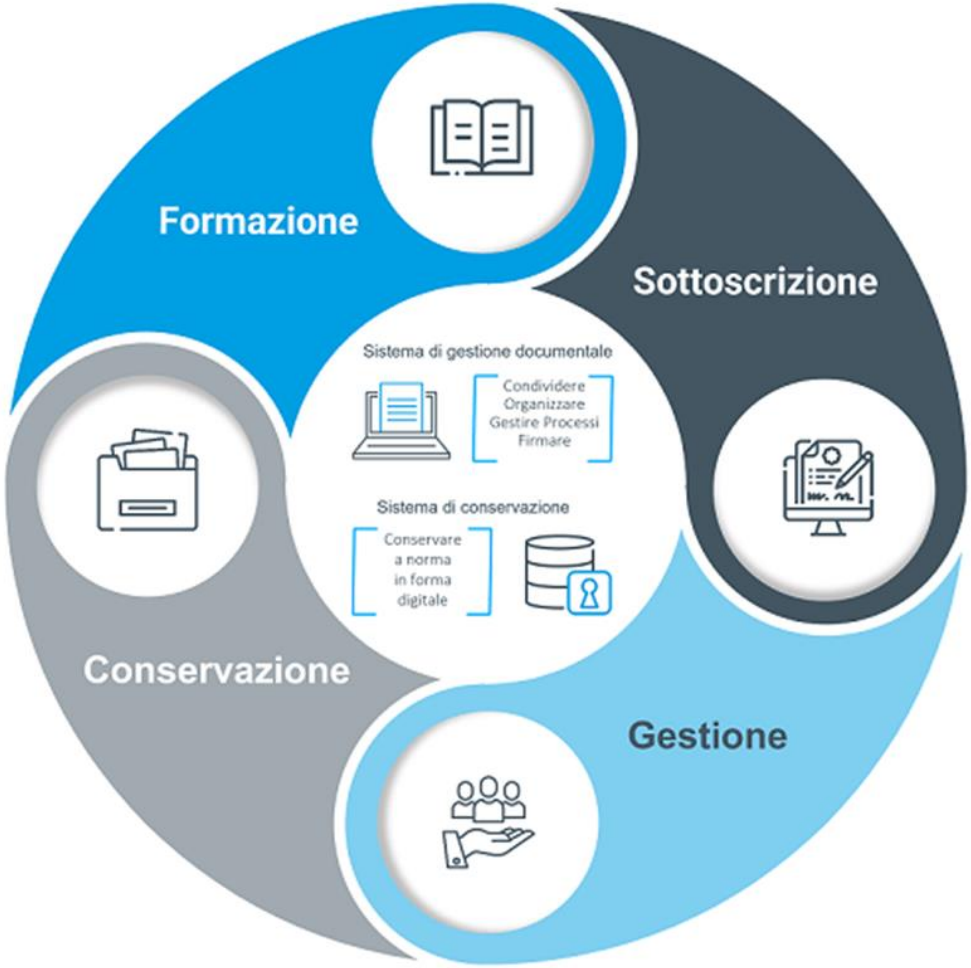
PER RIASSUMERE

La conservazione digitale rientra in un più ampio processo di gestione documentale aziendale ed è un'attività ben distinta dall'archiviazione elettronica che prevede la memorizzazione non normata di contenuti su un personal computer oppure su un supporto esterno.
Per conservazione digitale si intende quel processo che subentra dopo l'archiviazione, normato dall'art. 44 del Codice dell'Amministrazione digitale, e che mira a conservare nel tempo le informazioni, con la sottoscrizione elettronica e l'apposizione della marca temporale, garantendo l'accessibilità dei dati. **Il processo di conservazione digitale differisce da quello di archiviazione per le garanzie civilistiche che offre.**

Fra i vantaggi principali della conservazione digitale, troviamo, sicuramente, ***il risparmio di tempo*** **perché c'è una maggiore velocità nella ricerca dei documenti e** ***la riduzione dei costi di gestione*** **degli archivi cartacei.**
Parliamo di processi che mirano a conservare nel tempo documenti e contratti, ottimizzando i processi aziendali e garantendo una maggiore sicurezza e riservatezza delle informazioni contenute al loro interno.

CONSERVAZIONE DIGITALE DEI DOCUMENTI

PER RIASSUMERE



NUOVE MODALITÀ DI COMUNICAZIONE DENTRO E FUORI LO STUDIO PROFESSIONALE

INSERIMENTO e CONSULTAZIONE, CONSERVAZIONE ANALOGICA DI: DATI, DOCUMENTI, INFORMAZIONI (3X3)

GESTIONE ANALOGICA	INSERIMENTO DATI	CONSULTAZIONE	CONSERVAZIONE
CONSULENTE	X	X	X
CLIENTE	X	X	X
DIPENDENTE	X	X	X

INSERIMENTO e CONSULTAZIONE, CONSERVAZIONE DIGITALE DI: DATI, DOCUMENTI, INFORMAZIONI (3X1)

GESTIONE DIGITALE	INSERIMENTO DATI	CONSULTAZIONE	CONSERVAZIONE
CONSULENTE	X	X	X
CLIENTE			
DIPENDENTE			

NUOVE MODALITÀ DI COMUNICAZIONE DENTRO E FUORI LO STUDIO PROFESSIONALE

1. Il **dato digitale** è **inserito una sola volta** e può essere **consultato da un numero illimitato di utenti**;
2. L'utilizzo del dato nativo **digitale evita gli errori di trascrizione**;
3. Elaborazione, consultazione, archiviazione **da chiunque**;
4. Elaborazione consultazione archiviazione **da ovunque**;
5. Elaborazione consultazione archiviazione **in tempo reale**;
6. **Riduzione telefonate per richieste** informative e documentali;
7. **Guadagno di tempo** per svolgere attività maggiormente remunerative;
8. **Possibilità di** svolgere l'attività lavorativa in **smart working** per i collaboratori;
9. **No mobili**e fabbricati **per archivio**;
10. Non è necessario fare gli **aggiornamenti al software;**
11. **Miglioramento della produttività** e del comfort lavorativo;
12. **Acquisizione di clienti digitali**, maggiormente organizzati;
13. **Acquisizione clienti da ovunque** oltre il proprio territorio;
14. **Migliora la *brand reputation* nei confronti dei clienti e degli stakeholders**, in particolare dei collaboratori (per molti candidati rappresenta un'opportunità acquisire competenze digitali);
15. Meno tempo impiegato in attività usuali;
16. Più tempo da dedicare in **FORMAZIONE** per aggiungere competenze adeguate ai nuovi bisogni delle aziende.

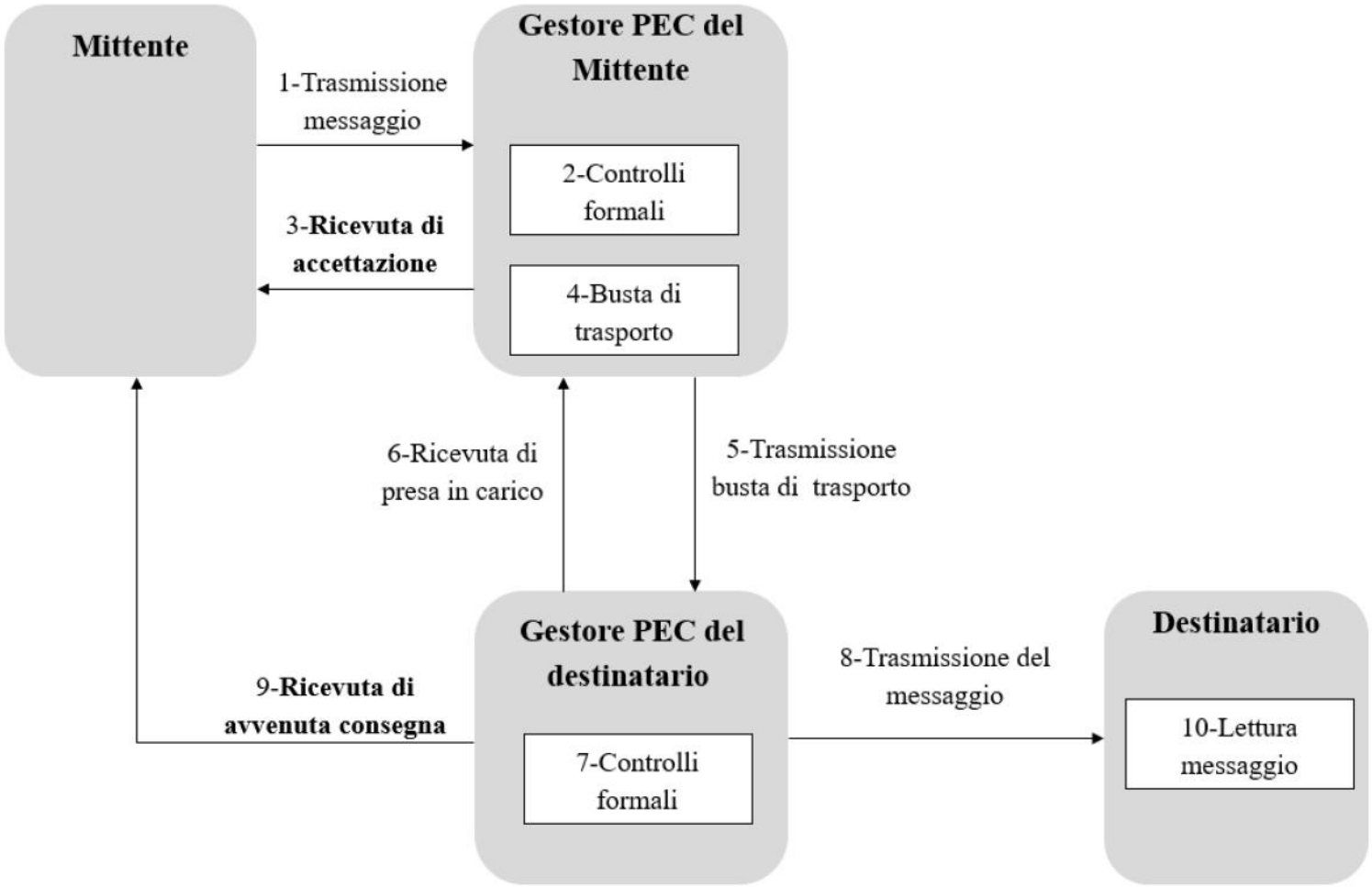
NUOVE MODALITÀ DI COMUNICAZIONE DENTRO E FUORI LO STUDIO PROFESSIONALE

Digitalizzazione processi interni

Offerta di nuovi servizi di consulenza a valore

Collaborazione con aziende e dipendenti

DIGITALIZZAZIONE E PRIVACY: LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI



POSTA ELETTRONICA CERTIFICATA: CONSERVAZIONE E PUNTI DI ATTENZIONE

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA CERTIFICATA: CONSERVAZIONE E PUNTI DI ATTENZIONE

Le firme apposte dai gestori PEC ai messaggi (ricevute, avvisi, buste), sono **firme elettroniche avanzate** basate su sistemi a chiavi asimmetriche al fine garantire l'autenticità e l'integrità dei messaggi trasmessi nel sistema di comunicazione PEC;
•Sui singoli messaggi (ricevute, avvisi, buste) il gestore PEC appone un **riferimento temporale** e quotidianamente una **marca temporale sui log dei messaggi**;

Per tutte le attività eseguite durante la fase di trasmissione del messaggio vengono creati appositi **log** delle operazioni svolte che saranno conservati dai gestori PEC in appositi registri per **trenta mesi** e che sono: il codice identificativo univoco assegnato al messaggio originale (Message ID);
la data e l'ora dell'evento;
il mittente del messaggio originale;
i destinatari del messaggio originale;
l'oggetto del messaggio originale;
il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.)
il gestore mittente

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA CERTIFICATA: CONSERVAZIONE E PUNTI DI ATTENZIONE

L'art.6 del decreto 2 novembre 2005, prevede tre diverse tipologie di **ricevuta di avvenuta consegna**: completa, breve e sintetica.
Ricevuta di avvenuta consegna **completa**, costituita da un messaggio con allegato due file: il file "**daticert.xml**" contenente il mittente, il destinatario, l'oggetto, la data ed ora di accettazione, e l'identificativo del messaggio;
il file "**postacert.eml**" che è il messaggio originale trasmesso completo (headere testo) e comprensivo anche degli **eventuali allegati** (fatture, contratti, ecc);

Ricevuta di avvenuta consegna **breve**, costituita da un messaggio con allegato due file: il file "**daticert.xml**" contenente il mittente, il destinatario, l'oggetto, la data ed ora di accettazione, e l'identificativo del messaggio;
il file "**postacert.eml**" che è il messaggio originale trasmesso completo (headere testo) e **l'impronta di eventuali allegati**;

Ricevuta di avvenuta consegna **sintetica**, costituita da un messaggio contenente il solo file "**daticert.xml**" riportante il mittente, il destinatario, l'oggetto, la data ed ora di accettazione, e l'identificativo del messaggio.

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA CERTIFICATA: LE SENTENZE DELLA CASSAZIONE

- **Il messaggio PEC non è stato letto perché è finito nello spam**

Il titolare dell'account PEC ha il dovere di controllare tutta la posta in arrivo, ivi compresa quella considerata dal programma utilizzato come "posta indesiderata".
*"I programmi di posta elettronica non sono in grado di individuare, con esattezza, i messaggi da qualificarsi come spam, e –pertanto –**rientra nella diligenza ordinaria dell'addetto alla ricezione della posta elettronica il controllo anche della cartella della posta indesiderata**, atteso che in tale cartella ben possono essere automaticamente inseriti messaggi provenienti da mittenti sicuri e attendibili e non contenenti alcun allegato pregiudizievole per il destinatario"*
(Cassazione n.17968 del 23 giugno 2021)

- **Il messaggio PEC non è stato letto perché la casella PEC era piena**

Deve ritenersi regolarmente perfezionata la comunicazione inviata via PEC se la mancata consegna è dovuta alla "casella piena" del destinatario e, pertanto, a una causa a lui imputabile;
*"La notificazione di un atto eseguita ad un soggetto, obbligato per legge a munirsi di un indirizzo di posta elettronica certificata, **si ha per perfezionata con la ricevuta con cui l'operatore attesta di avere rinvenuto la cd. casella PEC del destinatario "piena", da considerarsi equiparata alla ricevuta di avvenuta consegna,** in quanto il mancato inserimento nella casella di posta per saturazione della capienza rappresenta un evento imputabile al destinatario, per l'inadeguata gestione dello spazio per l'archiviazione e la ricezione di nuovi messaggi"* (Cassazione n.3164 del 11 febbraio 2020)

- **Il messaggio PEC ha un allegato illeggibile**

Se il messaggio PEC ha un allegato in tutto o in parte illeggibile, sta al destinatario informare il mittente incolpevole delle difficoltà della visualizzazione del contenuto della PEC.
"***Spetta al destinatario, in un'ottica collaborativa, rendere edotto il mittente** incolpevole delle difficoltà di cognizione del contenuto della comunicazione legale all'utilizzo dello strumento telematico"*(Cassazione n.25819 del 31 ottobre 2017)

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA CERTIFICATA: RICORDA!

1. I messaggi PEC devono essere conservati in modalità digitale
2. La PEC non può sostituire la firma digitale
3. La PEC non può sostituire la marca temporale
4. Verificare periodicamente lo spazio disponibile della casella PEC
5. È il gestore PEC che stabilisce il n. max dei destinatari e la dimensione max dei messaggi
6. INI-PEC per reperire gli indirizzi PEC (www.inipec.gov.it)

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA: MISURE DI ORGANIZZAZIONE E PRIVACY

Il titolare del trattamento può controllare la mail aziendale dei lavoratori?

Già nel 2007 il Garante della privacy era intervenuto sulla questione, specificando che "*i datori di lavoro pubblici e privati non possono controllare la posta elettronica e la navigazione in Internet dei dipendenti, se non in casi eccezionali; spetta dunque al datore di lavoro definire le modalità d'uso di tali strumenti ma tenendo conto dei diritti dei lavoratori e della disciplina in tema di relazioni sindacali*".

L'Autorità ha fornito alcune indicazioni attraverso le **linee guida per posta elettronica e internet,** tutt'oggi ancora valide e applicabili.
Le linee guida sono disponibili al seguente link:
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1387978

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA: MISURE DI ORGANIZZAZIONE E PRIVACY

Come prima cosa, il Garante ha stabilito che i datori di lavoro (o committenti) sono tenuti ad informare con chiarezza e in modo dettagliato i lavoratori circa le modalità di utilizzo della posta elettronica e circa la possibilità che vengano effettuati dei controlli.

Il Garante ha inoltre vietato la lettura e la registrazione sistematica delle e-mail, in quanto ciò significherebbe un controllo a distanza dell'attività lavorativa, precluso altresì dallo Statuto dei lavoratori, in caso di controllo svolto sui lavoratori dipendenti.

Quali possono essere i punti di attenzione da non trascurare nella gestione della posta elettronica aziendale?
Un esempio è fornito dagli account di posta aziendale composti da nome e cognome, che sebbene accompagnati dal dominio aziendale sono a tutti gli effetti dati personali e per questo motivo richiedono la corretta applicazione delle tutele imposte dalla normativa in materia di privacy.

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA: MISURE DI ORGANIZZAZIONE E PRIVACY

Il Garante stesso nelle sue linee guida consiglia al titolare del trattamento:

- di mettere a disposizione anche indirizzi condivisi tra più lavoratori (info@ente.it; urp@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;
- valutare la possibilità di attribuire al lavoratore un altro indirizzo (oltre quello di lavoro), destinato ad un uso personale;
- prevedere, in caso di assenza del lavoratore, messaggi di risposta automatica con le coordinate di altri lavoratori cui rivolgersi;
- dare la possibilità al dipendente di delegare un altro lavoratore di fiducia (formalmente identificato) a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al titolare quelli ritenuti rilevanti per l'ufficio, ciò in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa.

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA: MISURE DI ORGANIZZAZIONE E PRIVACY

Attribuire ai lavoratori account di posta nominativi non è una scelta da escludere a priori, ma deve semplicemente essere ben regolamentata per non incorrere in problematiche future.

Per fare ciò sarebbe auspicabile la **redazione di una *policy* aziendale** che deve tener conto della realtà lavorativa, delle effettive esigenze aziendali e soprattutto della normativa in materia di privacy.

DIGITALIZZAZIONE E PRIVACY: LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

Policy aziendale, un esempio

Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità del Titolare del Trattamento del dato e in stretta connessione con l'effettiva attività e mansioni del lavoratore che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza della struttura e di prevenire conseguenze legali a carico del Titolare del Trattamento del dato, bisogna adottare le seguenti norme comportamentali:

1. *Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;*
2. *È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;*
3. *La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione; tale operazione deve essere svolta mensilmente ed in funzione delle modalità di trattamento del dato stabilito dalla presente policy.*
4. *Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:*
   a. *l'indirizzo del destinatario sia stato correttamente digitato,*
   b. *l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;*
   c. *nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;*
   d. *ove il documento contenente dati particolari sia un allegato alla mail, questo deve essere protetto da password, precedentemente concordata con il destinatario e comunicata tramite indirizzo PEC; l'elenco delle password assegnate sarà salvato in apposita cartella nel server cloud dell'Azienda (percorso: _indicare il percorso_);*

al fine di analizzare e valutare eventuali data breach, è stata applicata un'impostazione che prevede l'invio in copia conoscenza al Titolare del Trattamento del dato di tutti i messaggi di posta elettronica in uscita; tale impostazione è automatica, pertanto l'incaricato non dovrà intervenire manualmente; inoltre tale disposizione non rileva ai fini del controllo delle attività del lavoratore e non può comportare eventuali richiami disciplinari, nel rispetto delle previsioni della L. 300/1970

DIGITALIZZAZIONE E PRIVACY:
LA GESTIONE DELLA POSTA ELETTRONICA, DEGLI ARCHIVI DIGITALI E LA FORMAZIONE AI COLLABORATORI

POSTA ELETTRONICA: MISURE DI ORGANIZZAZIONE E PRIVACY

- **E I LAVORATORI CESSATI?**

Non solo le caselle di posta elettronica dei lavoratori in forza comporta la necessità di intervento e gestione da parte del titolare del trattamento del dato, ma anche quelle dei lavoratori non più in forza. **In caso di interruzione del rapporto di lavoro il Garante suggerisce di disattivare e rimuovere la casella aziendale**, predisponendo sistemi che prevengano la ricezione dei messaggi e informando i soggetti terzi, con sistemi automatici, che quell'account è stato disattivato (indicando nuovi recapiti alternativi).

L'autorità infatti, con un provvedimento del 4 dicembre 2019 ha ribadito che la società che mantiene attivo l'account di posta aziendale di un dipendente dopo l'interruzione del rapporto di lavoro e accede alle mail contenute nella sua casella di posta elettronica **commette un illecito**.

I principi sulla protezione dei dati impongono al datore di lavoro la tutela della riservatezza anche dell'ex dipendente: subito dopo la cessazione del rapporto di lavoro infatti un'azienda deve necessariamente rimuovere gli account di posta elettronica riconducibili al dipendente cessato, adottare sistemi automatici con indirizzi alternativi a chi contatta la casella di posta e introdurre accorgimenti tecnici per impedire la visualizzazione dei messaggi in arrivo.

LE CONSEGUENZE DELLA DIGITALIZZAZIONE: GESTIONE DEL DATA BREACH

Cos'è un *data breach*?

> **Art. 4, punto 12), del Regolamento**
>
> «***violazione dei dati personali***: *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (c.d. «data breach»)*

- Un incidente di sicurezza è un qualsiasi evento che può manifestarsi a seguito di un malfunzionamento *hardware* o *software*, di un attacco informatico o di un comportamento umano doloso o accidentale.
- Un *data breach* non è altro che un particolare tipo di incidente di sicurezza che coinvolge dati personali, in seguito al quale il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali previsti dal Regolamento.
- Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono violazioni di dati personali.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LE CONSEGUENZE DELLA DIGITALIZZAZIONE: GESTIONE DEL DATA BREACH

Cos'è un *data breach*?

Un *data breach* può essere classificato
in base ai tre principi della sicurezza delle informazioni

Violazione della disponibilità	Violazione dell'integrità	Violazione della riservatezza
distruzione o perdita non autorizzate di dati personali	*modifica non autorizzata di dati personali*	*divulgazione o accesso non autorizzati a dati personali*

- Un *data breach* può anche riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, oppure una combinazione delle stesse.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

LE CONSEGUENZE DELLA DIGITALIZZAZIONE: GESTIONE DEL DATA BREACH

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Cos'è un *data breach*?

Distruzione non autorizzata	indisponibilità definitiva di dati personali degli interessati con impossibilità di ripristino degli stessi
Perdita	perdita di un supporto fisico di memorizzazione contenente dati personali degli interessati oppure di documenti cartacei
Modifica non autorizzata	modifiche dei dati degli interessati effettuate da incaricati non autorizzati oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati
Divulgazione non autorizzata	distribuzione non autorizzata o illecita dei dati personali degli interessati verso terzi anche non precisamente identificabili
Accesso non autorizzato	accesso non autorizzato o improprio ai dati degli interessati oppure accesso ai dati avvenuto al di fuori dei processi di trattamento dei dati previsti e autorizzati

LE CONSEGUENZE DELLA DIGITALIZZAZIONE: GESTIONE DEL DATA BREACH

Cos'è un *data breach*?

Cons. 85 del Regolamento:

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

*«Una **violazione** dei dati personali **può**, se non affrontata in modo adeguato e tempestivo, **provocare danni fisici, materiali o immateriali alle persone fisiche**, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata* [...]»

GRAZIE PER L'ATTENZIONE

Dott.ssa Garbelli Barbara
Consulente del Lavoro in Pavia
Membro Centro Studi Nazionale ANCL
Componente Comitato Scientifico ASRI

Il presente materiale sarà disponibile su www.ancl.it