PROVINCIA DI NOVARA

MANUALE DI GESTIONE DEI FLUSSI DOCUMENTALI

Approvato con Decreto n. 153 in data 19 dicembre 2025

SEZIONE I - DEFINIZIONI E AMBITO DI APPLICAZIONE

Articolo 1 – Ambito di applicazione

Il presente Manuale è adottato a seguito e per effetto delle regole tecniche in materia di formazione, gestione e conservazione dei documenti analogici e digitali di cui alle Linee guida AGID del maggio 2021 e s.m.i.

Il Manuale descrive e disciplina la gestione dei flussi documentali della Provincia di Novara e l'attività di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti.

Il Manuale è rivolto agli utenti interni ovvero a tutti i soggetti che operano all'interno della Provincia di Novara e agli utenti esterni, cittadini, imprese, enti che si rapportano con l'Amministrazione.

Articolo 2 – Definizioni

Ai fini del presente Manuale s'intende:

1. ***Amministrazione***, la Provincia di Novara;
2. ***Archivio***, complesso ordinato degli atti spediti, ricevuti o comunque formati e prodotti dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione/Area Organizzativa Omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, viene suddiviso in tre sezioni: corrente, di deposito e storico;
   - ***Archivio corrente,*** documentazione relativa ad affari e procedimenti in corso di trattazione o comunque verso i quali sussiste un interesse corrente; ne fanno parte anche le banche dati e i sistemi informativi che trattino dati e informazioni utilizzati per lo svolgimento dell'attività amministrativa;
   - ***Archivio di deposito***, documentazione relativa ad affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso, ma non ancora destinata istituzionalmente alla conservazione permanente;
   - ***Archivio storico***, complesso dei documenti relativi ad affari e procedimenti amministrativi conclusi da più di quarant'anni, selezionati e destinati, previe operazioni di selezione e scarto, alla conservazione permanente per garantirne in forma adeguata la consultazione;
3. ***Area Organizzativa Omogenea (AOO)***, insieme definito di unità organizzative di una amministrazione, che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. In particolare una AOO utilizza per il servizio di protocollazione un'unica sequenza numerica, rinnovata ogni anno solare;
4. ***Assegnazione***, operazione che individua il Settore e l'Ufficio competenti per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
5. ***Classificazione***, operazione che consente di organizzare i documenti in relazione alle funzioni ed alle modalità operative dell'Amministrazione, in base al titolario di classificazione;
6. ***Codice dell'Amministrazione Digitale (CAD)***, il testo unico sulle disposizioni relative alla digitalizzazione dell'amministrazione approvato con il decreto legislativo 7 marzo 2005 n. 82 e s.m.i;
7. ***Documento amministrativo***, ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;

8. ***Documento informatico***, documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
9. ***Fascicolo***, aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento;
10. ***Fascicolazione***, operazione di assegnazione di un documento a una definitiva unità archivistica generalmente indicata con il termine fascicolo.
11. ***Firma digitale***, particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate fra loro che consente al titolare, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità del documento informatico o di un insieme di documenti informatici;
12. ***Firma elettronica***, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*;*
13. ***Flusso documentale o workflow****,* movimento dei documenti sia all'interno dell'AOO da un Settore a un altro sia all'interno dell'archivio (dalla fase formativa dell'archivio corrente a quella conservativa dell'archivio storico);
14. ***Gestione dei documenti***, insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, alla fascicolazione, alla assegnazione, al reperimento, alla conservazione e all'accesso dei documenti amministrativi formati o acquisiti dall'Amministrazione;
15. ***Interoperabilità****,* capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi;
16. ***Piano di conservazione degli archivi***, piano integrato con il piano di classificazione e con il piano di fascicolazione, che contiene i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di beni culturali;
17. ***Piano di classificazione o titolario****,* struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata;
18. ***Piano di fascicolazione***, strumento di organizzazione dell'archivio che predispone l'organizzazione dei fascicoli rispecchiando la struttura del Piano di classificazione o titolario integrandosi con esso;
19. ***Posta elettronica certificata (PEC)****,* particolare modalità di invio di posta elettronica prevista per legge per le comunicazioni che necessitano di una ricevuta d'invio e una ricevuta di consegna, che equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta;
20. ***Registro di protocollo informatico****,* atto pubblico di fede privilegiata dell'effettivo ricevimento e spedizione di un documento, idoneo a produrre effetti giuridici. Il registro di protocollo informatico garantisce le operazioni di registrazione, classificazione e gestione dei flussi documentali;
21. ***Scarto***, insieme delle operazioni volte ad identificare i diversi tempi di conservazione delle serie archivistiche prodotte dall'Ente (selezione) e ad eliminare, tramite distruzione, quelle che hanno raggiunto la scadenza dei tempi minimi di conservazione dal punto di vista amministrativo e che non rivestono interesse storico. Il procedimento relativo comporta la redazione di un apposito elenco di scarto che deve essere sottoposto all'autorizzazione della Soprintendenza archivistica competente;
22. ***Segnatura di protocollo***, apposizione all'originale del documento in forma permanente e non modificabile delle informazioni riguardanti il documento stesso;
23. ***Sistema di conservazione dei documenti informatici****,* il sistema che assicura l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o

dell'area organizzativa omogenea, l'integrità, la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari, ed infine il rispetto delle misure di sicurezza previste dalle normative vigenti;
24. ***Sistema gestione informatica dei documenti***, insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati per la gestione dei documenti;
25. ***SPID***, il Sistema Pubblico di Identità Digitale è il sistema unico di accesso con identità digitale ai servizi online della pubblica amministrazione e dei soggetti privati aderenti con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone;
26. ***Testo unico***, il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, pubblicato con DPR 28 dicembre 2000, n. 445 e s.m.i;
27. ***Versamento***, passaggio di custodia, di proprietà e/o di responsabilità dei documenti.

SEZIONE II - FORMAZIONE DEGLI ATTI E DOCUMENTI

Articolo 3 – Modalità di formazione di atti e documenti informatici

La Provincia forma gli originali dei propri documenti in prevalenza secondo le seguenti modalità:

- utilizzo di applicativi di videoscrittura;
- utilizzo di appositi strumenti software;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici;
- presentazione telematica di dati mediante moduli standard o formulari;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni provenienti da una o più basi dati, anche in modalità interoperativa;
- utilizzo di posta elettronica certificata e ordinaria;
- acquisizione ottica interattiva con l'ausilio di scanner di documenti in formato analogico (corrispondenza pervenuta in cartaceo) e conseguente protocollazione sull'applicativo dedicato.

Gli atti formati con strumenti informatici, i dati e i documenti informatici dell'Ente costituiscono informazione primaria da cui è possibile effettuare, su diversi tipi di supporto, copie e duplicati per gli usi consentiti dalla legge.

Articolo 4 – Contenuti minimi degli atti e dei documenti prodotti dalla Provincia

I documenti dell'Amministrazione sono di norma prodotti nativamente in formato digitale.
Gli atti di natura provvedimentale sono redatti utilizzando il software dedicato che rende disponibile, per ogni tipologia di atto, lo schema tipo (uniforme per tutto l'Ente) da completare a cura del redattore della proposta.
Per la corrispondenza destinata all'esterno, è data disposizione agli Uffici di utilizzare (tramite l'editor di testo configurato nell'apposito applicativo) uno schema di lettera univoco ("modello di lettera") contenente le necessarie informazioni basilari.
Per i casi residuali in cui non dovesse essere utilizzato il "modello lettera" andranno comunque riportate le medesime informazioni essenziali.

Articolo 5 – Formato degli atti e documenti informatici
La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.
Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.
Ai fini della formazione, gestione e conservazione, è necessario scegliere formati che possano garantire la leggibilità e la reperibilità del file nel suo ciclo di vita. A tal fine i dipendenti provinciali sono tenuti ad utilizzare formati ricompresi nel disciplinare tecnico del Conservatore dei documenti informatici dell'Ente.

Articolo 6 – Sottoscrizione dei provvedimenti
I provvedimenti (deliberazioni di Consiglio e Assemblea dei Sindaci, decreti del Presidente, determinazioni dirigenziali, ordinanze et similia) sono sottoscritti con firma digitale. Il dispositivo di firma digitale viene consegnato al Presidente ed al Vice Presidente, al Segretario Generale, a tutti i Dirigenti, agli Incaricati di Elevata Qualificazione e a tutti coloro che hanno potere di firma per funzioni loro delegate.
I pareri prescritti per detti atti di natura provvedimentale vengono parimenti apposti con firma digitale con le modalità consentite dal software in uso, il quale prevede altresì la c.d. "firma debole" da parte del Funzionario intermedio che esegue il controllo (quest'ultima individuabile attraverso il flusso informatico delle proposte).

Articolo 7 – Sottoscrizione dei documenti informatici
La sottoscrizione dei documenti informatici è ottenuta con firma digitale riportando in calce apposita annotazione indicante che trattasi di documento sottoscritto con tale modalità.

Articolo 8 – Formazione di documenti analogici e spedizione in formato analogico di documenti digitali
La redazione di documenti originali in formato analogico è eccezionalmente consentita, salve norme speciali di legge, solo nei casi in cui risulti necessaria data l'impossibilità di utilizzare strumenti informatici e comunque nel rispetto del principio dell'economicità dell'azione amministrativa.
In assenza di domicilio digitale del cittadino, qualora si renda necessario spedire tramite il servizio postale documenti nativi digitali in formato analogico, i documenti da spedire saranno convertiti da originali informatici in copie analogiche. In tale caso è preferibile venga riportata sulla copia cartacea un'annotazione che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto ed è disponibile presso l'Amministrazione.
Si suggerisce pertanto la seguente dicitura: "Riproduzione cartacea del documento informatico sottoscritto digitalmente"; la firma autografa è sostituita dall'indicazione a stampa del nome, cognome del firmatario.

Articolo 9 – Gestione informatica degli ordinativi di incasso e pagamento
Gli ordinativi di incasso e pagamento (reversali e mandati) sono gestiti attraverso appositi applicativi software, e firmati digitalmente.
Sono sottoscritti dal Responsabile del servizio finanziario o da suo sostituto.
La conservazione degli stessi è effettuata in base alle disposizioni della normativa vigente in materia da un soggetto che possegga le caratteristiche tecniche e professionali tali da garantire il servizio.

Articolo 10 – Gestione della fattura elettronica
In base a quanto previsto dalla normativa vigente, le fatture sono ricevute nel formato "FatturaPA" e trattate esclusivamente in modalità digitale con utilizzo del gestionale in uso.
Le fatture in ingresso riportano solitamente i codici IPA dei Settori della Provincia ai fini della corretta imputazione e del corretto smistamento agli uffici competenti in sede di protocollo. Gli utenti abilitati degli Uffici destinatari possono procedere all'accettazione o al rifiuto della fattura entro 15 giorni. Scaduti i 15 giorni la fattura si considera accettata.

SEZIONE III - FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Articolo 11 – Flusso di lavorazione dei documenti
Le fasi della gestione dei documenti sono:
a) ricezione/spedizione;
b) registrazione e segnatura di protocollo;
c) classificazione;
d) assegnazione;
e) fascicolazione dei documenti.

Articolo 12 – Area Organizzativa Omogenea
La Provincia di Novara individua una sola Area Organizzativa Omogenea (AOO), articolata nell'insieme di tutti i suoi Settori e Uffici come indicati e definiti negli strumenti di programmazione dell'Ente.
All'interno della AOO il sistema di protocollazione è unico e accentrato presso l'Ufficio Archivio e Protocollo per la corrispondenza in arrivo, mentre è decentrato per la corrispondenza in uscita e interna.

Articolo 13 – Tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
All'interno dell'Area Organizzativa Omogenea l'attività connessa alla tenuta del protocollo informatico ed alla gestione degli archivi è funzionalmente ricondotta alla Struttura facente capo al Segretario Generale, nel cui ambito è individuato l'Ufficio "Archivio e Protocollo" preposto alla gestione e tenuta dei documenti prodotti o ricevuti dall'Ente nel corso dell'attività amministrativa.

Articolo 14 – Unicità dell'Archivio
L'Archivio della Provincia è unico e indivisibile, ma si distinguono tre fasi di gestione legate all'utilizzo dei documenti ad esso afferenti: archivio corrente, archivio di deposito e archivio storico.

Articolo 15 – Unicità del protocollo informatico
Nell'ambito dell'Area Organizzativa Omogenea la numerazione delle registrazioni di protocollo è unica e rigidamente progressiva e nella stessa numerazione confluiscono anche i protocolli riservati.
Essa si chiude al 31 dicembre e ricomincia da 1 all'inizio di ogni anno.
Il numero di protocollo è costituito da sette cifre numeriche.

Articolo 16 – Protocollo riservato
L'applicativo di protocollo consente di valorizzare l'opzione documento riservato. Il protocollo riservato è sottratto a qualsiasi consultazione dei non abilitati ed è destinato a documenti relativi a vicende di persone, fatti privati o particolari, a provvedimenti disciplinari, ad attività di polizia giudiziaria ed a quelle riservate del Presidente.

Articolo 17 – Registro di protocollo
Tutti i documenti in entrata e in uscita devono essere protocollati, salvo i casi di esclusione o di registrazione particolare.
Il registro di protocollo, dal punto di vista giuridico, è un atto pubblico destinato a far fede del ricevimento o della spedizione dei documenti trattati dalla Provincia di Novara ed ivi registrati.
La Provincia adotta il sigillo elettronico qualificato nel registro di protocollo sia per le registrazioni in uscita che per quelle in entrata.

Articolo 18 – Gestione protocollazione in entrata, in partenza e interna
Gli utenti del protocollo vengono preliminarmente profilati in conformità a quanto indicato nel manuale per gli utenti della Ditta fornitrice del software in uso onde garantire la protocollazione in entrata, in partenza e interna.
La protocollazione in entrata, fatta eccezione per i documenti ricevuti mediante piattaforme online, viene gestita esclusivamente dall'Ufficio Protocollo, a cui viene collegata la PEC istituzionale: protocollo@provincia.novara.sistemapiemonte.it .
La gestione della protocollazione in partenza e interna risulta decentrata.
Per la corrispondenza in partenza a firma del Presidente e/o dei Consiglieri delegati è richiesto il controllo preventivo del Dirigente competente per materia o suo delegato.
L'invio PEC viene prodotto unicamente dalla casella istituzionale dell'Ente, fatta eccezione per le comunicazioni degli Avvocati dell'Ufficio Unico Avvocatura che, con riferimento all'attività processuale e agli atti giudiziari, si avvalgono dei propri indirizzi di PEC comunicati all'Ordine Professionale di appartenenza e censiti nel Registro Generale degli Indirizzi Elettronici (RegIndE) ai sensi del D.M. 21 febbraio 2011 n. 44.

Articolo 19 – Processo di assegnazione dei documenti
L'assegnazione dei documenti può essere effettuata per conoscenza o per competenza.
Le assegnazioni vengono attuate, di norma, individuando la cosiddetta "Funzione", destinataria del documento, cui si riconduce la responsabilità del procedimento amministrativo.
A tale assegnazione può seguire, da parte del soggetto preposto (di massima Incaricato/a di Elevata Qualificazione), la presa in carico ovvero la sub-assegnazione del documento ad un Ufficio/Dipendente dell'Ente.
I termini per la definizione del procedimento amministrativo che si avvia con l'assegnazione del documento decorrono comunque dalla data di protocollazione.
Il sistema memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, nonché la data di esecuzione.

Articolo 20 – Tutela dei dati personali
La Provincia di Novara garantisce tutte le misure previste per la tutela dei dati personali in accordo con la normativa vigente e la regolamentazione interna.

Per ogni documento, all'atto della registrazione, il sistema consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso, nel rispetto della normativa in materia di trattamento e tutela dei dati personali.
Ogni dipendente dell'Ente può consultare i documenti relativi ad affari di propria competenza assegnati all'Ufficio di appartenenza e quei documenti necessari per l'esercizio dell'attività amministrativa per i quali è stata accordata la visibilità e l'accesso.

Articolo 21 – Originali, duplicati e copie
Si definisce "originale" il documento nella sua redazione definitiva, perfetta ed autentica completo degli elementi sostanziali e formali di cui deve essere garantita la non modificabilità.
I dati e i documenti, comunque detenuti dall'Amministrazione, costituiscono informazione primaria da cui è possibile effettuare, su diversi tipi di supporto, duplicati, copie ed estratti, nei termini e per gli usi consentiti dalla legge.
Le copie, così come gli estratti, hanno la stessa efficacia probatoria dell'originale da cui sono tratte, qualora risulti attestata nelle forme previste dalla normativa vigente.

SEZIONE IV - RICEZIONE DEI DOCUMENTI

Articolo 22 – Sistemi di ricezione dei documenti su supporto analogico/cartaceo
I documenti su supporto analogico/cartaceo possono pervenire attraverso:
- il servizio postale tradizionale, corrieri autorizzati o agenzie di recapito;
- la consegna diretta agli Uffici dell'Ente.

Articolo 23 – Procedimento per ricezione dei documenti su supporto analogico/cartaceo
La documentazione indirizzata alla Provincia, proveniente dal servizio postale tradizionale, oppure da corrieri autorizzati o agenzie di recapito, viene consegnata all'Ufficio Archivio e Protocollo, che provvede a:
1. scansione ed acquisizione in copia digitale conformemente alle modalità indicate dalle Linee guida AGID;
2. registrazione al protocollo;
3. assegnazione e al successivo inoltro agli Uffici competenti.

L'Ufficio Archivio e Protocollo è tenuto alla registrazione di tutti i documenti (completi delle caratteristiche necessarie) e quindi alla apertura dei relativi plichi consegnati da soggetti terzi, senza distinguo o verifiche preventive e nei tempi previsti.
Il personale provvede con cura alla custodia della documentazione ricevuta al fine di garantire la sicurezza e l'integrità dei documenti e dei dati ivi contenuti.
La posta indirizzata nominativamente al personale della Provincia viene regolarmente aperta e registrata al protocollo, a meno che sulla busta, oltre al nominativo, sia riportata la dicitura "personale"/"riservato". Analogamente eventuali documenti di tipo strettamente personale destinati in particolare a Presidente e Consiglieri provinciali non vengono aperti solo se riportanti sulla busta, oltre al nominativo del destinatario, anche la dicitura "personale"/"riservato". In questo caso la posta è considerata al di fuori dell'attività istituzionale e quindi non riconducibile alle attività dell'Ente. Eventuali comunicazioni di interesse dell'Ente inoltrate impropriamente come "personali" dovranno essere consegnate senza ritardo al protocollo, direttamente e sotto la responsabilità del destinatario, una volta

verificato il contenuto della documentazione e la necessità di acquisizione al protocollo generale dell'Ente.

Articolo 24 – Scansione dei documenti analogici

Per le esigenze di lavoro e di consultazione, i documenti cartacei trasmessi all'Ente vengono di norma scansionati e acquisiti in copia digitale "semplice".

Qualora tuttavia sia necessario garantire la medesima efficacia giuridico-probatoria riconosciuta al documento analogico originale, il Dirigente o il Funzionario all'uopo delegato, che agisce in veste di pubblico ufficiale, archivia il documento analogico e appone sulla copia informatica, la propria firma elettronica, previa iscrizione sul documento di dicitura del seguente tenore:

"*Io sottoscritto/a, ai sensi dell'art. 22, co. 2, d.lgs. n. 82/2005, attesto che la presente copia per immagine è conforme in ogni sua parte al documento originale analogico dal quale è stata estratta.* [indicare: nome e cognome, nome ente e ufficio, data e luogo]."

Nel caso sia necessario attestare la conformità all'originale di più documenti, acquisiti per copia di immagine, ferma restando la necessità di effettuare il raffronto per ogni documento originale scansionato, è possibile effettuare un'unica attestazione di conformità, su foglio separato e collegato alle copie informatiche, da sottoscrivere digitalmente, contenente l'indicazione delle impronte hash associata a ciascuna copia informatica.

L'attestazione di conformità della copia per immagine al documento originale analogico è richiesta nei casi in cui vi sia l'esigenza di assicurare che la copia abbia la medesima efficacia giuridico-probatoria del documento originale. Così deve avvenire, ad esempio:

- quando si deve provvedere a notificazione via PEC di documento (o allegato a documento) sottoscritto in originale analogico. In questi casi la conformità della copia informatica all'originale analogico è attestata dal Responsabile del procedimento;
- quando si deve formare un contratto tra l'Ente e un privato che sottoscrive con firma autografa (formazione di contratti ibridi). In questi casi il pubblico ufficiale acquisisce la scansione del documento firmato in originale cartaceo dal privato e, previo raffronto, attesta la conformità della copia digitale (con le modalità sopra indicate). Infine, il soggetto competente alla stipula sottoscrive la copia con la propria firma digitale, così perfezionando il contratto. Quando il pubblico ufficiale, che attesta la conformità della copia, ed il soggetto competente alla stipula coincidono, è sufficiente apporre un'unica firma digitale. Al fine di escludere il rischio di disconoscimento della firma, è preferibile che il pubblico ufficiale provveda contestualmente all'attestazione di conformità della copia digitale e all'autenticazione della sottoscrizione analogica ivi contenuta;
- quando, ai fini della conservazione digitale dei documenti, si intende sostituire l'originale analogico con la copia informatica.

I documenti scansionati per mere esigenze di uso lavoro e consultazione non richiedono attestazione di conformità all'originale, ferma restando la necessità di conservare il documento originale analogico.

Articolo 25 – Ricezione dei documenti informatici

La ricezione dei documenti informatici soggetti alla registrazione di protocollo è assicurata tramite la casella di posta elettronica certificata istituzionale (PEC) riservata a questa funzione ed accessibile per la ricezione solo all'Ufficio Protocollo.

L'indirizzo di tale casella di posta elettronica (PEC) è: protocollo@provincia.novara.sistemapiemonte.it

L'indirizzo della casella PEC istituzionale suindicato è reperibile nell'"Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi" (IPA)

http://www.indicepa.it ed è pubblicato sul sito web istituzionale http://www.provincia.novara.it
Nel caso in cui il file del documento pervenuto alla casella PEC sia danneggiato o non leggibile, non si procederà alla protocollazione e verrà inviato un avviso al mittente.
Il documento informatico, oltre che a mezzo PEC, può essere recapitato anche a mezzo di servizio online e interoperabilità tra sistemi.
La ricezione di documenti informatici tramite la casella di posta elettronica ordinaria, nominativa o d'ufficio è sconsigliata e può essere utilizzata solo in via eccezionale per lo scambio di messaggi destinati alla protocollazione. In tali casi residuali, i messaggi che devono essere protocollati, sono inoltrati alla casella PEC dell'Ente. Conseguentemente l'Ufficio Archivio e Protocollo, che accede alla casella PEC, allega al protocollo, oltre all'email originale in formato .eml, anche i file contenuti ed allegati nell'email stessa. Il mittente da indicare in fase di protocollazione è quello indicato nell'email pervenuta all'Ente.

Articolo 26 – Metadati del documento informatico
Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'allegato 5 alle Linee guida dell'AGID. Ulteriori metadati facoltativi possono essere associati a particolari tipologie di documenti, secondo le indicazioni dei Responsabili dei servizi e in conformità alle Linee guida.
L'associazione dei metadati al documento è effettuata tramite le apposite funzioni per la formazione degli atti del sistema di gestione documentale. A tal fine, il Responsabile della gestione documentale verifica la conformità degli strumenti software utilizzati e, eventualmente, richiede al fornitore i necessari interventi evolutivi.
I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di immodificabilità e integrità, dunque prima della sottoscrizione o del versamento in conservazione.

Articolo 27 – Rilascio di ricevuta attestante la registrazione dei documenti
L'applicativo di protocollo consente di selezionare, fra le funzionalità disponibili, l'opzione "Stampa ricevuta". Essa genera la "ricevuta di protocollo" contenente indicazioni dell'avvenuta registrazione.

Articolo 28 – Rilascio di copie analogiche di documenti informatici protocollati
Il documento informatico corredato da stringa di protocollo può essere rilasciato in formato cartaceo, con apposita dicitura che ne attesti la conformità all'originale a cura del Dirigente o altro soggetto dal medesimo delegato.

Articolo 29 – Servizi online con autenticazione
1. Il ricorso a procedure on-line tramite apposite piattaforme di condivisione istanze/documenti/dati deve garantire il diritto di accesso ai destinatari del servizio con autenticazione tramite la propria identità digitale.
2. Le piattaforme on-line utilizzate dall'Ente, di proprietà ovvero gestite da altre PA, devono garantire la protezione dei dati e della privacy secondo la vigente normativa.
3. Gli invii e le ricezioni dei documenti scambiati mediante piattaforme on-line può avvenire:
   - tramite interconnessione diretta con la procedura di protocollo dell'Ente;
   - tramite protocollazione a carico degli Uffici competenti.

SEZIONE V - REGISTRAZIONE DEI DOCUMENTI

Articolo 30 – Documenti soggetti a registrazione di protocollo

I documenti ricevuti e prodotti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati nell'articolo successivo, sono registrati nel sistema di gestione del protocollo informatico.

Articolo 31 – Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo:

a) Pubblicazioni:
- Gazzette ufficiali;
- Bollettini ufficiali di Amministrazioni pubbliche;
- Notiziari di Amministrazioni pubbliche (ad es. Newsletter Lexitalia);
- Giornali;
- Riviste;
- Libri;
- Pubblicazioni varie.

b) Note di ricezione:
- Notifiche di presa in carico di richieste di inserzione avvisi pubblicazione;
- Notifiche relative a profilazioni nuove utenze;
- Note relative a documenti informatici ricevuti o inviati nell'ambito di sistemi dedicati allo scambio o alla consultazione di dati su piattaforma online (ad es. richieste di durc);
- Notifiche di avvenuta registrazione.

c) Atti preparatori interni:
- Atti di gestione interna del personale (richieste ferie, permessi, certificati di malattia, richieste di rimborso spese e missioni, altra documentazione inerente congedi, assenze, ecc.);
- Convocazioni ad incontri o riunioni o corsi di formazione interni;
- Offerte e listini prezzi promozionali comunque al di fuori di procedimenti di gara in quanto materiali pubblicitari;
- Atti interni privi di rilevanza esterna nei procedimenti amministrativi.

d) Materiale statistico e pubblicitario;

e) Inviti a manifestazioni che non attivino procedimenti amministrativi;

f) Documenti di occasione, di interesse effimero:
- Ringraziamenti;
- Congratulazioni varie;
- Condoglianze.

Articolo 32 – Documenti esclusi dalla registrazione di protocollo perché soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo i documenti già soggetti a registrazione particolare dell'Amministrazione. Tali documenti non vengono registrati in quanto costituiscono delle serie archivistiche, ciascuna delle quali è corredata da un repertorio o registro particolare contenente le seguenti informazioni:
- i dati identificativi di ciascun atto;
- il numero progressivo annuale di repertorio/registro.

I repertori o registri particolari sono gestiti, di norma, in modalità informatica.

Essi riguardano:
- Deliberazioni del Consiglio Provinciale;

- Deliberazioni dell'Assemblea dei Sindaci;
- Decreti del Presidente;
- Determinazioni dirigenziali;
- Ordinanze et similia;
- Notifiche;
- Verbali:
  Verbali dell'Organismo Indipendente di Valutazione delle Performance;
  Verbali del Collegio dei Revisori;
  Verbali lavori Ufficio Elettorale;
  Verbali della Polizia Provinciale;
  Verbali delle Conferenze dei Servizi, dei tavoli tecnici, di sopralluogo;
- Conferme di ricezione istanze relative a pratiche per danni provocati dalla fauna all'agricoltura su modulo della Regione Piemonte acquisite dall'Ufficio Caccia;
- Rapporti di servizio della Polizia Provinciale.

Articolo 33 – Registrazione di protocollo dei documenti ricevuti e spediti

Per ogni documento ricevuto o spedito, ad eccezione di quelli esclusi, è effettuata una registrazione di protocollo con il sistema di gestione informatica dei documenti.

A ciascuna registrazione di protocollo vengono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione.

Le lettere, le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.

Per ciascuna registrazione di protocollo sono inseriti i metadati obbligatori definiti dalla normativa vigente come segnatura di protocollo, e cioè:

a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) mittente per i documenti ricevuti o, in alternativa, destinatario o destinatari per i documenti spediti non modificabile;
d) oggetto del documento;
e) data e numero di protocollo del documento ricevuto, se disponibili;
f) impronta del documento informatico registrato in forma non modificabile.

L'operazione di registrazione prevede l'assegnazione della documentazione protocollata.

I messaggi di posta elettronica (e-mail) pervenuti alla casella di posta elettronica certificata (PEC), anche se non corredati da firma digitale vengono registrati al protocollo generale. La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica sulla casella PEC è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati.

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo o al momento dell'inserimento negli appositi repertori informatici.

Alla fase di registrazione e protocollazione occorre dedicare particolare attenzione, al fine di agevolare le operazioni di successiva ricerca e fruibilità del documento; in particolare occorre che gli oggetti vengano inseriti senza acronimi e siano quanto più possibile chiari e sintetici.

Articolo 34 – Registrazione di protocollo dei documenti interni

È effettuata la registrazione di protocollo anche per i documenti interni prodotti dagli Uffici provinciali, quindi non spediti a soggetti esterni alla Provincia e non rientranti nelle categorie

di documenti esclusi dalla registrazione, indipendentemente dal supporto sul quale sono formati.

Articolo 35 – Segnatura di protocollo

L'operazione di segnatura di protocollo va effettuata contemporaneamente all'operazione di registrazione di protocollo.

Le informazioni apposte od associate al documento sia per quanto riguarda la corrispondenza in arrivo che per quella in partenza mediante l'operazione di segnatura sono:

- identificazione in forma sintetica dell'Amministrazione;
- codice identificativo del registro;
- progressivo di protocollo;
- data e ora di protocollo.

Articolo 36 – Annullamento e modifica delle registrazioni di protocollo

L'applicativo consente la specifica procedura per gestire le richieste di annullamento dei protocolli. L'annullamento richiede la preventiva autorizzazione del Responsabile della gestione documentale.

Articolo 37 – Registro giornaliero di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede fino a querela di falso circa la data e l'effettivo ricevimento o spedizione di un documento, di qualsiasi forma e contenuto ed è idoneo a produrre effetti giuridici tra le parti.

Il registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno, ivi comprese le registrazioni annullate o modificate in quella medesima data.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione.

Il registro giornaliero di protocollo viene prodotto in forma automatizzata direttamente dal software di gestione ed inviato in conservazione.

Articolo 38 – Registro di emergenza

Il Responsabile della gestione documentale autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.

Si applicano le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico come qui a seguito indicato:

a) sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale può autorizzare l'uso del registro di emergenza. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione;
c) per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate;
d) la sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati;

e) le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, senza ritardo al ripristino delle funzionalità del sistema.

Per meglio garantire quanto affermato nei punti precedenti viene individuato quale unico Ufficio abilitato alla registrazione dei documenti sui registri di emergenza l'Ufficio Protocollo.

Articolo 39 – Documenti inerenti a gare d'appalto

Per l'espletamento delle procedure di gara l'Ente utilizza le piattaforme telematiche e gli strumenti di e-procurement in uso secondo la normativa vigente.

Articolo 40 – Atti giudiziari

Il protocollo di atti giudiziari è assegnato all'unità organizzativa competente e all'Ufficio Avvocatura.

Gli Avvocati dell'Ufficio Unico Avvocatura nell'ambito del contenzioso seguito si avvalgono degli appositi strumenti necessari per operare nel Processo Telematico ai sensi delle vigenti disposizioni normative in materia.

Articolo 41 – Lettere anonime e documenti non firmati

Le lettere anonime sono soggette a registrazione di protocollo.

La *ratio* che deve governare il comportamento di un operatore durante la fase di registrazione di un documento in arrivo deve infatti essere improntata all'avalutatività. In altre parole, l'operatore di protocollo deve attestare che un determinato documento, così come si è registrato, è pervenuto. Si tratta di una delicata competenza di tipo certificativo, attestante la certezza giuridica di data, forma e provenienza per ogni documento.

Nella procedura informatica per la gestione documentale il mittente è indicato nell'anagrafica con la dicitura "Anonimo". Se il documento anonimo è pervenuto a mezzo PEC si lascia come mittente l'indirizzo PEC.

Il documento deve essere assegnato al Dirigente dell'Ufficio competente o al Segretario Generale.

Articolo 42 – Documenti ricevuti da casella di posta elettronica e, successivamente, in originale su supporto cartaceo

Qualora ai documenti ricevuti da casella di posta elettronica segua un inoltro con posta tradizionale, agli originali saranno attribuiti lo stesso numero e la stessa data di protocollo assegnati alla precedente comunicazione tramite mail.

Qualora non si riscontrasse la registrazione della mail o il documento inviato per posta risultasse difforme da quello inviato precedentemente si procede ad una registrazione di protocollo anche per il documento giunto per posta.

Articolo 43 – Documenti di competenza di altre Amministrazioni o di altri soggetti

Qualora pervenga alla Provincia un documento di competenza di un altro ente, altra persona fisica o giuridica, lo stesso viene restituito al mittente; diversamente può essere trasmesso a chi di competenza, se individuabile.

Nel caso in cui un documento della fattispecie sopra indicata venga erroneamente registrato al protocollo, questi verrà spedito a chi di competenza, oppure restituito al mittente, procedendo ad una annotazione nella registrazione con riportati gli estremi della spedizione e la motivazione.

Articolo 44 – Integrazioni documentarie e procedimentali
Gli addetti al protocollo non sono tenuti a controllare la completezza formale e sostanziale della documentazione pervenuta, ma sono tenuti a registrare il documento e gli eventuali allegati.
Tale verifica spetta al Dirigente/Incaricato di Elevata Qualificazione/Responsabile del procedimento, che deve comunicare all'interessato la necessità di eventuali integrazioni e valutare se l'assenza della documentazione comporta interruzione o sospensione del procedimento.
I documenti presentati ad integrazione devono essere protocollati al momento dell'arrivo, con l'attribuzione di un nuovo numero di protocollo.

SEZIONE VI - CLASSIFICAZIONE DEI DOCUMENTI

Articolo 45 – Titolario (Piano di classificazione)
Il titolario, il piano di classificazione dell'archivio provinciale, è riportato nell'allegato n. 1.
Il titolario è soggetto ad aggiornamenti periodici.
Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno seguente alla loro approvazione.
La sostituzione di voci di titolario comporta l'impossibilità di aprire nuovi fascicoli nelle voci precedenti a partire dalla data di attivazione delle nuove voci.

Articolo 46 – Classificazione dei documenti
La classificazione dei documenti è un processo fondamentale nella gestione documentale per gestire in modo efficace le informazioni all'interno dell'Ente. E' il processo di organizzazione e categorizzazione dei documenti in base a criteri specifici per facilitarne la gestione, l'archiviazione e il recupero. Aiuta a garantire che i documenti siano facilmente accessibili, protetti e ben organizzati, supportando così le operazioni quotidiane, la conformità normativa e la sicurezza delle informazioni.
Pertanto tutti i documenti ricevuti e prodotti all'interno dell'Area Organizzativa Omogenea, indipendentemente dal supporto sul quale vengono formati, devono essere classificati in base al titolario di cui all'articolo precedente.
Nel momento in cui è effettuata la segnatura di protocollo deve inoltre essere apposta al documento la classificazione, sia per quanto riguarda la corrispondenza in arrivo che per quella in partenza.

SEZIONE VII – MODELLO ORGANIZZATIVO – PROTOCOLLO INFORMATICO E ASSEGNAZIONE DEI DOCUMENTI

Articolo 47 – Assegnazioni e operazioni correlate
La procedura informatica in uso prevede che i documenti visualizzabili dagli utenti sulla propria scrivania virtuale di appartenenza (smart desktop) possano essere gestiti con le seguenti opzioni:

Prendi in carico: l'attività di presa in carico riproporrà sulla scrivania virtuale dell'utente lo stesso documento nello stato "in carico", con possibilità di modifica da parte dell'utente destinatario;
Smista: permette agli utenti abilitati di aggiungere uno o più smistamenti in competenza o conoscenza;
Prendi in carico ed esegui: permette la presa in carico e l'esecuzione del documento selezionato, chiudendo di fatto lo smistamento e ponendo lo stato dello stesso ad "Eseguito" ovvero concluso; quindi trattasi di opzione che rispetto alla semplice presa in carico introduce l'esecuzione dell'attività che toglie la stessa dalla scrivania virtuale dell'utente.
Prendi in carico, esegui e smista: in questo caso oltre a dichiarare la presa in carico del documento si provvede ad eseguire lo smistamento valorizzando i dati di esecuzione;
Prendi in carico ed inoltra: oltre alla presa in carico dei documenti selezionati viene proposta la scelta di una o più unità di destinazione. L'utente che effettua l'inoltro perde in questo caso il diritto di modifica del documento. Sarà comunque possibile continuare a visualizzare il documento dalle ricerche del sistema documentale.

Articolo 47 – Recapito dei documenti ricevuti ai Settori/Uffici
I documenti informatici ricevuti per via telematica e le immagini digitali dei documenti scansionati sono resi disponibili agli utenti, attraverso il sistema di gestione documentale dell'Amministrazione, immediatamente dopo l'operazione di assegnazione.
I documenti ricevuti dall'Area Organizzativa Omogenea su supporto cartaceo, anche se acquisiti in formato immagine con l'ausilio di scanner, sono consegnati materialmente agli Uffici di competenza.

SEZIONE VIII - FASCICOLAZIONE DEI DOCUMENTI

Articolo 48 – Identificazione dei fascicoli e loro formazione
I documenti classificati, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli.
La formazione di un nuovo fascicolo avviene attraverso *l'operazione di apertura* gestita dal sistema informatico di protocollazione.
La numerazione del fascicolo è unica all'interno della stessa classificazione per anno di apertura.

Articolo 49 – Tipologie di fascicoli
Si distinguono le seguenti tipologie di fascicolo:
- fascicolo per affare;
- fascicolo per attività;
- fascicolo per procedimento amministrativo;
- fascicolo per persona fisica;
- fascicolo per persona giuridica.

Fascicolo per affare:
conserva i documenti relativi a una competenza non proceduralizzata. Per gli affari non esiste un termine previsto da norme per la conclusione.

Fascicolo per attività:
conserva i documenti relativi a una competenza proceduralizzata per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque prevista l'adozione di un provvedimento finale.
Fascicolo per procedimento amministrativo:
conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.
Fascicolo per persona fisica:
conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'Ente.
Fascicolo per persona giuridica:
conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica.

Articolo 50 – Piano di fascicolazione
Il Piano di fascicolazione è lo strumento di gestione e reperimento dei fascicoli. La struttura del Piano rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo. Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'Ente può esercitare in base alle proprie funzioni istituzionali, il Piano rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.
Il Piano di fascicolazione della Provincia di Novara è redatto come da schema allegato (allegato n. 6).

Articolo 51 – Chiusura dei fascicoli
Il Responsabile del procedimento o altro soggetto dal medesimo autorizzato deve provvedere alla chiusura del fascicolo tramite le apposite funzionalità del protocollo informatico quando l'affare o la pratica a cui si riferisce è terminata.

SEZIONE IX - SPEDIZIONE DEI DOCUMENTI

Articolo 52 – Modalità di spedizione dei documenti informatici
Per la spedizione dei documenti informatici l'Amministrazione si avvale della casella di posta elettronica certificata (PEC) collegata al sistema di protocollo, che provvede ad effettuare l'invio telematico.
I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, che può corrispondere ad una casella PEC o mail (non certificata) nel caso di privati non provvisti di PEC.
Il sistema consente di verificare e accertare l'avvenuta consegna del documento nel caso in cui il destinatario riporti un indirizzo di posta elettronica certificata.

Articolo 53 – Spedizione dei documenti su supporto cartaceo
La trasmissione dei documenti all'esterno dell'Area Organizzativa Omogenea può avvenire, in assenza di un domicilio digitale del destinatario, per mezzo di:
- servizio di posta tradizionale;
- consegna diretta al cittadino;

- notifiche secondo la normativa del Codice di Procedura Civile.

Nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere o altro mezzo che richieda una documentazione da allegare alla busta, la relativa modulistica viene compilata a cura degli Uffici che richiedono tale operazione.
I documenti da spedire su supporto cartaceo sono trasmessi all'ufficio postale abilitato alla spedizione "fisica" della corrispondenza.
Per la spedizione di copia analogica di documento informatico si rinvia alle indicazioni del precedente articolo 8.

SEZIONE X – ARCHIVIAZIONE E CONSERVAZIONE DEI DOCUMENTI

Articolo 54 – Conservazione di documenti e fascicoli informatici

Per la conservazione di documenti e fascicoli informatici la Provincia di Novara si avvale di Soggetti esterni.
Il versamento dei documenti in conservazione avviene attraverso un apposito collegamento informatico tra i software gestionali dell'Ente e la piattaforma di gestione documentale con la piattaforma di conservazione; il trasferimento deve essere effettuato periodicamente mentre il registro giornaliero di protocollo è versato in conservazione quotidianamente.
Le modalità di conservazione e accesso ai documenti sono specificati nei manuali di conservazione degli Outsourcer.
Per quanto sopra non indicato si rinvia anche al Manuale di conservazione, il cui schema risulta in allegato (allegato 8).

Articolo 55 – Versamento dei fascicoli cartacei e delle serie documentarie nell'archivio di deposito

I fascicoli dell'archivio corrente sono formati e conservati presso l'Ufficio Archivio e Protocollo, oltre che presso i vari Uffici cui sono state assegnate le pratiche, fino al versamento nell'archivio di deposito.
Periodicamente, di norma una volta all'anno, gli Uffici individuano i fascicoli che dall'archivio corrente sono da versare nell'archivio di deposito in quanto relativi ad affari o procedimenti conclusi, o comunque non più necessari allo svolgimento delle attività correnti.
Dopo di che, provvedono allo sfoltimento del fascicolo eliminando le bozze, fotocopie e altro materiale che non deve essere conservato, e li inviano all'archivio di deposito curandone il trasferimento fisico, come da Linee guida allegate (allegato n. 3).
Il trasferimento deve essere effettuato rispettando l'organizzazione che le pratiche e le serie avevano nell'archivio corrente.

Articolo 56 – Selezione e scarto archivistico

Le operazioni di scarto comportano che venga prodotto l'elenco dei documenti e dei fascicoli per i quali è trascorso il periodo obbligatorio di conservazione e che quindi sono suscettibili di scarto archivistico, in coerenza con il Massimario di selezione e scarto di cui all'allegato n. 2.
L'elenco di scarto (allegato n. 4) deve essere trasmesso alla Soprintendenza Archivistica competente per territorio, per la concessione della necessaria autorizzazione.
Analogamente, per quanto riguarda i documenti in formato elettronico registrati con l'apposito applicativo, ferma restando la competenza della Soprintendenza nell'autorizzarne lo scarto, occorre tenere presente che:

- i limiti di tenuta e conservazione dei documenti informatici sono analoghi a quelli stabiliti dal Massimario per i documenti in formato cartaceo;
- la valutazione sui limiti di conservabilità del documento informatico deve tener conto dei principi e della vigente disciplina per il trattamento dei dati personali.

SEZIONE XI – ACCESSO E SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Articolo 57 – Accesso da parte degli utenti appartenenti alla Provincia di Novara

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili con diversi privilegi d'accesso e adeguati sistemi di autenticazione dell'utente (username e password).
La Provincia ha provveduto a disciplinare la procedura per la gestione dei casi di violazione dei dati personali (data breach) a mezzo di apposito provvedimento cui si rinvia (decreto presidenziale n. 61/2021, riprodotto quale allegato n. 7 del presente manuale).

Articolo 58 – Accesso esterno

Tutte le informazioni necessarie e sufficienti a garantire l'esercizio del diritto di accesso ai documenti amministrativi sono rese disponibili all'utenza esterna.
Per quanto concerne i documenti sottratti all'accesso, si rinvia allo specifico Regolamento sull'accesso ai documenti amministrativi.

Articolo 59 – Attività in regime di smart working

In occasione di lavoro agile e smart working è vietato portare all'esterno degli Uffici dell'Ente documenti analogici in originale o depositare stabilmente copie di documenti originali informatici su dispositivi portatili; la fruizione dei documenti informatici è garantita mediante l'accesso al sistema di protocollo informatico e gestione documentale.
Il dipendente, anche se presta servizio in modalità smart, è tenuto alla massima cura delle pratiche gestite nello svolgimento dell'attività di competenza.
Il dipendente è altresì tenuto alla massima diligenza nelle attività di archiviazione delle pratiche gestite, affinché sia garantita ed agevole la loro rintracciabilità.
Al fine di assicurare la tracciabilità dei processi decisionali, i dipendenti sono tenuti inoltre a garantire un adeguato supporto documentale, che consenta la possibilità di riprodurre il medesimo processo decisionale anche per le prestazioni in presenza.

SEZIONE XII – PUBBLICAZIONI ALL'ALBO PRETORIO

Articolo 60 – Albo Pretorio

L'Albo Pretorio online è la sezione del sito web istituzionale della Provincia di Novara, dedicata alla pubblicazione in forma digitale dei documenti relativi ad atti e provvedimenti che, in base alla normativa vigente o per scelta dell'Amministrazione, devono essere resi potenzialmente conoscibili a chiunque.
Linee guida sull'argomento risultano in allegato (allegato n. 5).

SEZIONE XIII – UTILIZZO PORTALE PAGOPA, MEPA

Articolo 61 – PAGOPA

E' stato attivato sul sito della Provincia il portale PAGOPA da utilizzarsi da parte dei contribuenti/utenti esterni. Tale collegamento può essere attivato attraverso il logo presente sul sito.
I servizi di incasso, a seguito dell'introduzione di PAGOPA sono stati implementati, secondo le richieste dei singoli Uffici e sono state create le credenziali di accesso al portale per tutti gli Uffici per i quali sono stati configurati tali servizi.

Articolo 62 – Gestione procedure per affidamenti di lavori, servizi e forniture

Gli Uffici della Provincia utilizzano prioritariamente il portale acquisti in rete della Pubblica Amministrazione, il portale Anac e le procedure "Appalti e contratti" per gli affidamenti di lavori, sevizi e forniture in modo trasparente.

SEZIONE XIV – DISPOSIZIONI GENERALI E FINALI

Articolo 63 – Demanialità dell'archivio

I singoli documenti e l'archivio della Provincia di Novara sono beni culturali assoggettati al regime proprio del demanio pubblico.
All'Archivio, considerato unitariamente come bene culturale dalla fase corrente a quella storica, si applicano le norme previste dal Codice dei beni culturali.
La Soprintendenza archivistica e bibliografica del Piemonte e Valle d'Aosta svolge compiti di tutela e vigilanza sull'Archivio.
Tutti gli interventi sugli archivi devono essere autorizzati dalla Soprintendenza, in particolare:

- le procedure di scarto;
- il conferimento a terzi dell'archivio;
- lo spostamento o cambiamento di sede dell'archivio storico o di deposito;
- tutte le attività di natura tecnico scientifica relative a: riordino, inventariazione, restauro, digitalizzazione;
- il prestito a terzi di documenti.

La Provincia assicura e sostiene la conservazione del patrimonio culturale e ne favorisce la pubblica fruizione e la valorizzazione.
La tutela e la valorizzazione del patrimonio culturale concorrono a preservare la memoria della comunità nazionale e del suo territorio e a promuovere lo sviluppo della cultura.

Articolo 64 – Il Responsabile della gestione documentale

Il Responsabile della gestione documentale, ovvero dei flussi documentali, quando non diversamente individuato, è il Segretario Generale dell'Ente.

Articolo 65 – Norme finali

Per quanto non espressamente indicato nel presente Manuale si rinvia alle disposizioni normative in materia, anche sopravvenute, se ed in quanto applicabili.
Gli allegati al presente Manuale richiamati ai paragrafi precedenti ne fanno parte integrante e sostanziale.

Elenco allegati al Manuale di Gestione

Allegato 1 _Titolario

Allegato 2 _Massimario

Allegato 3 _Versamento fascicoli

Allegato 4 _Prospetto per scarto

Allegato 5 _Pubblicazione Albo (Linee guida per la pubblicazione all'Albo Pretorio online)

Allegato 6 _Piano di fascicolazione *(schema)*

Allegato 7 _Decreto presidenziale n. 61/2021 (data breach)

Allegato 8_Schema manuale di conservazione

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 1

Titolario (= Piano di classificazione) per l'Archivio della Provincia di Novara

Amministrazione: p_no - Provincia di Novara

Titolario - Area Organizzativa: PROVINCIA DI NOVARA

CODICE DESCRIZIONE

01 ORDINAMENTO AMMINISTRATIVO: ATTI FONDAMENTALI, ORGANI E ORGANIZZAZIONE

01.01 AFFARI GENERALI
01.02 DENOMINAZIONE, TERRITORIO E CONFINI
01.03 STEMMA, GONFALONE, BANDIERA, LOGO - PATROCINI
01.04 STATUTO E REGOLAMENTI
01.05 AMMINISTRAZIONE PROVINCIALE: ORGANI (PRESIDENTE - CONSIGLIO - ASSEMBLEA SINDACI - COMMISSIONI CONSILIARI - MOZIONI - INTERPELLANZE - INTERROGAZIONI)
01.06 ELEZIONI PROVINCIALI
01.07 ORDINAMENTO UFFICI E SERVIZI PROVINCIALI - SEGRETARIO PROVINCIALE
01.08 CONTENZIOSO - AVVOCATURA
01.09 ANTICORRUZIONE - TRASPARENZA

02 RAPPORTI ISTITUZIONALI

02.01 AFFARI GENERALI
02.02 RELAZIONI INTERNAZIONALI, COMUNITA' - EUROPEA (POLITICHE COMUNITARIE - PROGETTI EUROPEI), REGIO INSUBRICA
02.03 STATO: AUTORITA' E UFFICI GOVERNATIVI LOCALI (PREFETTURA - FORZE DELL'ORDINE, ECC.)
02.04 REGIONE - CAL CONSIGLIO DELLE AUTONOMIE LOCALI
02.05 ENTI LOCALI (COMUNI) - ANCI - UPI UNIONE PROVINCE D'ITALIA
02.06 SOCIETÀ PARTECIPATE - ASSOCIAZIONI - RAPPRESENTANTI PROVINCIALI PRESSO ENTI VARI – IPAB

03 RISORSE INFORMATIVE

03.01 AFFARI GENERALI
03.02 ARCHIVIO E PROTOCOLLO
03.03 COMUNICAZIONE PUBBLICA (STAMPA, INFORMAZIONE, COMUNICAZIONE, SITO WEB, ALBO PRETORIO)
03.04 SERVIZI E SISTEMI INFORMATICI - STATISTICA
03.05 TUTELA DATI PERSONALI

04 PERSONALE

04.01 AFFARI GENERALI
04.02 CONCORSI - MOBILITA' - SELEZIONI E ASSUNZIONI
04.03 PERSONALE - PIANTA ORGANICA - INQUADRAMENTO GIURIDICO E CONTRATTI DI LAVORO E NUCLEO DI VALUTAZIONE/OIV
04.04 RETRIBUZIONI E COMPENSI ASSISTENZA E PREVIDENZA (INPS - ADEMPIMENTI FISCALI - CONTRIBUTIVI E ASSICURATIVI)
04.05 CORSI DI FORMAZIONE E AGGIORNAMENTO PROFESSIONALE
04.06 SINDACATI E SCIOPERI
04.07 TUTELA DELLA SALUTE E DELLA SICUREZZA NEI LUOGHI DI LAVORO (D.LGS N. 81 DEL 09/04/2008 - MEDICO LEGALE)

05 RISORSE FINANZIARIE E BILANCIO
05.01 AFFARI GENERALI (FATTURE - FALLIMENTI)
05.02 CONTROLLI DI GESTIONE - REVISORI DEL CONTO - CORTE DEI CONTI
05.03 BILANCI - CONTI - PEG
05.04 MUTUI
05.05 TRIBUTI E CONTRIBUTI (PORTI DI GENOVA E SAVONA)
05.06 TESORERIA

06 EDILIZIA PATRIMONIO E RISORSE STRUMENTALI
06.01 AFFARI GENERALI (ALBO FORNITORI - PRELAZIONI)
06.02 PATRIMONIO (INVENTARIO BENI PROV.LI - PARCO MACCHINE)
06.03 ASSICURAZIONI
06.04 EDIFICI PROVINCIALI - COSTRUZIONE
06.05 EDIFICI PROVINCIALI - MANUTENZIONE
06.06 EDILIZIA SCOLASTICA - COSTRUZIONE
06.07 EDILIZIA SCOLASTICA - MANUTENZIONE
06.08 AFFITTI - CONCESSIONE IN USO DI LOCALI PROVINCIALI

07 CACCIA - PESCA - PARCHI
07.01 AFFARI GENERALI
07.02 CACCIA
07.03 PESCA
07.04 PARCHI – RISERVE NATURALI - GEV (GUARDIE ECOLOGICHE VOLONTARIE)

08 LAVORI PUBBLICI/STAZIONE UNICA APPALTANTE - CONTRATTI
08.01 AFFARI GENERALI
08.02 APPALTI - LAVORI PUBBLICI
08.03 STAZIONE UNICA APPALTANTE
08.04 CONTRATTI

09 VIABILITA' - CONCESSIONI - TRASPORTI ECCEZIONALI
09.01 AFFARI GENERALI (ALBO FORNITORI)
09.02 STRADE PROV.LI E REGIONALI GESTITE - MANUTENZIONE E SEGNALETICA - PONTI E PASSAGGI A LIVELLO
09.03 STRADE PROVINCIALI COSTRUZIONE
09.04 ESPROPRI
09.05 NULLA OSTA CIRCOLAZIONE E REGOLAMENTAZIONE TRAFFICO - CONCESSIONI PER LAVORI E OCCUPAZIONE SUOLO
09.06 CARTELLI PUBBLICITARI E INSEGNE DI ESERCIZIO
09.07 ACCESSI CARRAI (TOSAP)
09.08 TRASPORTI ECCEZIONALI

10 AMBIENTE
10.01 AFFARI GENERALI (ATO - TUTELA E VALORIZZAZIONE AMBIENTALE - EDUCAZIONE AMBIENTALE E SOSTENIBILITA')
10.02 AUTORIZZAZIONI AMBIENTALI - MONITORAGGI (AUA IMPATTO ACUSTICO - ARIA - EMISSIONI - SCARICHI)
10.03 VIA (VALUTAZIONE DI IMPATTO AMBIENTALE) E VAS (VALUTAZIONE AMBIENTALE STRATEGICA)
10.04 RIFIUTI - INQUINAMENTO - BONIFICHE - OSSERVATORIO PROVINCIALE

10.05 ACQUA (IMPIANTI IDRICI - DERIVAZIONI - POZZI)
10.06 CAVE
10.07 ENERGIA (IMPIANTI ENERGETICI - TERMICI - OLI MINERALI)

11 ISTRUZIONE E SERVIZI ALLA PERSONA
11.01 AFFARI GENERALI
11.02 SCUOLE DI ISTRUZIONE SECONDARIA (DIMENSIONAMENTO SCOLASTICO - L.R.28/07 - INIZIATIVE CULTURALI PER STUDENTI)
11.03 UNIVERSITÀ
11.04 PARI OPPORTUNITA' (CENTRO SERVIZI - FAMILY AUDIT - CONSIGLIERA DI PARITÀ - ANTIDISCRIMINAZIONE - ORGANISMO COMPOSIZIONE CRISI)
11.05 POLITICHE GIOVANILI - SERVIZIO CIVILE VOLONTARIO

12 POLIZIA PROVINCIALE
12.01 AFFARI GENERALI
12.02 ATTIVITA' DI CONTROLLO POLIZIA PROVINCIALE

13 URBANISTICA - PIANIFICAZIONE TERRITORIALE
13.01 AFFARI GENERALI
13.02 PIANI REGOLATORI - VINCOLO IDROGEOLOGICO
13.03 SENTIERI - CARTOGRAFIE - PISTE CICLABILI - CONTRATTO DI FIUME - CONTRATTO DI LAGO

14 TRASPORTI E COMUNICAZIONI
14.01 AFFARI GENERALI (AEROPORTI)
14.02 T.P.L. TRASPORTO PUBBLICO LOCALE - TESSERE LIBERA CIRCOLAZIONE
14.03 ALBO AUTOTRASPORTATORI - AUTOSCUOLE
14.04 REVISIONI VEICOLI (OFFICINE)
14.05 NAVIGAZIONE

15 TURISMO - SPORT - CULTURA
15.01 AFFARI GENERALI
15.02 ATTIVITA' TURISTICHE
15.03 ATTIVITA' SPORTIVE
15.04 ATTIVITA' CULTURALI

16 PROTEZIONE CIVILE
16.01 AFFARI GENERALI
16.02 CALAMITA' NATURALI

17 CENTRI PER L'IMPIEGO
17.01 AFFARI GENERALI
17.02 CPI NOVARA E BORGOMANERO
17.03 POLITICHE DEL LAVORO
17.04 FORMAZIONE PROFESSIONALE

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 2

Massimario

CATEGORIA 1 ORDINAMENTO AMMINISTRATIVO

CONSERVAZIONE SENZA LIMITI DI TEMPO

- STATUTI
- REGOLAMENTI
- CIRCOLARI DELLA PROVINCIA
- DECRETI, ORDINANZE, NULLA OSTA DEL PRESIDENTE
- DELIBERAZIONI DESTINATE A FORMARE LA RACCOLTA UFFICIALE DEL CONSIGLIO E DELLA GIUNTA (ORGANI ISTITUZIONALI PROVINCIALI)
- ATTI DEL CONSIGLIO (INTERPELLANZE, INTERROGAZIONI, MOZIONI E ORDINI DEL GIORNO)
- PROVVEDIMENTI DIRIGENZIALI (DETERMINE)
- CONVENZIONI, PROTOCOLLI D'INTESA
- VERBALI DELLE SEDUTE DEGLI ORGANI POLITICI – COMMISSIONI
- ELEZIONI AMMINISTRATIVE: VERBALI E LISTE DI CANDIDATURA CON PROGRAMMI (EVENTUALI RICORSI)
- GRUPPI CONSILIARI
- ATTI RELATIVI A CONTENZIOSO E AVVOCATURA (CON ITER GIUDIZIARIO)
- TUTELA LEGALE DELL'ENTE - AFFIDAMENTO INCARICHI A PROFESSIONISTI

VALIDITA' 10 ANNI

- DOCUMENTI RELATIVI A RICHIESTE E CONCESSIONI DI CONTRIBUTI E PATROCINI
- RICHIESTE INERENTI DIRITTO DI ACCESSO AGLI ATTI

- DOCUMENTAZIONE VARIA RELATIVA AD ELEZIONI AMMINISTRATIVE
- CARTEGGI DI LIQUIDAZIONI DELLE MISSIONI DEGLI AMMINISTRATORI, CON RELATIVE TABELLE E DOCUMENTAZIONI
- ATTI RELATIVI A CONTENZIOSO E AVVOCATURA (RISOLTI IN FORMA ORDINARIA)

VALIDITA' 5 ANNI

- PREMI COPPE MEDAGLIE - ACQUISTO E CONCESSIONE
- DOCUMENTAZIONE RELATIVA A RICHIESTA E/O PARTECIPAZIONE GONFALONE PROVINCIALE
- AVVISI DI CONVOCAZIONE DELLE SEDUTE DEGLI ORGANI COLLEGIALI RAPPRESENTATIVI DELLA PROVINCIA

CATEGORIA 2 RAPPORTI ISTITUZIONALI / POLITICHE COMUNITARIE

CONSERVAZIONE SENZA LIMITI DI TEMPO

- RAPPRESENTANTI PROVINCIALI PRESSO ENTI VARI, AZIENDE E ISTITUZIONI
- ATTI RELATIVI A PARTECIPAZIONI SOCIETARIE
- POLITICHE COMUNITARIE – PARTECIPAZIONE E/O PROMOZIONE A PROGETTI EUROPEI

VALIDITA' 5 ANNI

- COMUNICAZIONI PROVENIENTI DA UPI / UPP / CAL / ANCI / MINISTERO / REGIONI / COMUNI / ASSOCIAZIONI
- CORRISPONDENZA GENERALE RELATIVA A PROGETTI COMUNITARI
- INVITI ALLE CONFERENZE DEI SERVIZI E ALLE CONSULTE

CATEGORIA 3 RISORSE INFORMATIVE E ARCHIVIO

CONSERVAZIONE SENZA LIMITI DI TEMPO

- REGISTRI PROTOCOLLO DELLA CORRISPONDENZA DELLA PROVINCIA
- RESPONSABILE TUTELA DATI PERSONALI (PRIVACY)
- ATTI RELATIVI A RIORDINAMENTI E SCARTI ARCHIVISTICI

VALIDITA' 20 ANNI

- ACQUISTO DI PROCEDURE E SOFTWARE

VALIDITA' 10 ANNI

- SERVIZIO DI ASSISTENZA E MANUTENZIONE
- REGISTRO ALBO PRETORIO
- REGISTRO NOTIFICHE

CATEGORIA 4 PERSONALE

CONSERVAZIONE SENZA LIMITI DI TEMPO

- FASCICOLO PERSONALE (SFOLTIMENTO IN ITINERE)
- LIBRO MATRICOLA PERSONALE
- VERBALI DELLE COMMISSIONI DI CONCORSO E COPIA DEL BANDO
- PIANTA O DOTAZIONE ORGANICA, PIANO DEL FABBISOGNO DEL PERSONALE
- VERBALI NUCLEO DI VALUTAZIONE

VALIDITA' 10 ANNI

- PIANO DI FORMAZIONE DEL PERSONALE
- GESTIONE ORDINARIA DEL PERSONALE (ELENCO TURNI DI SERVIZIO E REPERIBILITA' DEL PERSONALE, CONGEDO ORDINARIO, PERMESSI SINDACALI, DOCUMENTAZIONE PROPEDEUTICA ALLA VALUTAZIONE DEL PERSONALE)
- PROVVEDIMENTI ECONOMICI PER IL PERSONALE - PROGETTI DI PERFORMANCE (ATTI RELATIVI ALLA REALIZZAZIONE DEGLI OBIETTIVI DI PERFORMANCE)
- RICHIESTE DI MOBILITA'
- GESTIONE FISCALE E ASSICURATIVA DEI DIPENDENTI E COLLABORATORI (CUD – 730 – INAIL – CEDOLINI – ETC)
- TUTELA DELLA SALUTE E DELLA SICUREZZA DEL LAVORO (D. LGS 81 DEL 09/04/2008)
- SINDACATI

VALIDITA' 5 ANNI

- GESTIONE DEL SERVIZIO MENSA (B U O N I P A S T O)

- STRAORDINARI, PERMESSI, PROSPETTO MISSIONI - TRASFERTE E PARTECIPAZIONE A CORSI / CONVEGNI / SEMINARI - AUTORIZZAZIONI ALL'USO DEL MEZZO PROPRIO
- RIEPILOGHI MENSILI E TIMBRATURE
- RICHIESTE APPLICAZIONE DETRAZIONI PER FAMILIARI A CARICO
- RICHIESTE ASSEGNI FAMILIARI
- CONGEDI PARENTALI
- VISITE FISCALI

CATEGORIA 5 FINANZE LOCALI

CONSERVAZIONE SENZA LIMITI DI TEMPO

- BILANCI
- RENDICONTI
- PIANO ESECUTIVO DI GESTIONE (PEG) – PIANO E RELAZIONE PERFORMANCE
- VERBALI DI CHIUSURA ESERCIZIO FINANZIARIO
- LIBRI CONTABILI DI SINTESI (MASTRI)
- APPALTO SERVIZI TESORERIA / ESATTORIA
- DONAZIONE E GESTIONE OPERE D'ARTE

VALIDITA' 40 ANNI

- ATTI RELATIVI A CONTENZIOSO TRIBUTARIO

VALIDITA' 20 ANNI

- GESTIONE TRIBUTI PASSIVI
- MANDATI DI PAGAMENTO
- RUOLI DELLE IMPOSTE / TASSE

VALIDITA' 10 ANNI

- FATTURE LIQUIDATE
- REVERSALI DI RISCOSSIONE
- CONTO CASSA ECONOMALE
- DICHIARAZIONE REDDITI DELL'ENTE (MODELLI 770)
- MUTUI ESTINTI

VALIDITA’ 5 ANNI

- ACQUISTO ATTREZZATURE PER UFFICI
- ABBONAMENTI E ACQUISTO PUBBLICAZIONI

CATEGORIA 6 EDILIZIA

CONSERVAZIONE SENZA LIMITI DI TEMPO

- PIANI DI SICUREZZA E DI EVACUAZIONE DEGLI EDIFICI
- INVENTARI DEI BENI MOBILI ED IMMOBILI
- BENI DEMANIALI E PATRIMONIALI (ACQUISIZIONE / ALIENAZIONI / PERMUTE)
- EDIFICI PROVINCIALI - GENERALITA'
- EDIFICI SCOLASTICI - GENERALITA'
- MANUTENZIONE STRAORDINARIA EDIFICI PROVINCIALI E SCOLASTICI

VALIDITA' 10 ANNI

- ATTI RELATIVI ALLA GESTIONE DEI BENI IMMOBILI – AFFITTI CONCLUSI – SERVIZI DI PULIZIA
- PARCO AUTOVEICOLI PROVINCIALI
- UTENZE RISCALDAMENTO – ENERGIA ELETTRICA ETC.
- ASSICURAZIONI FURTI, RC IMMOBILI PROVINCIALI, INCENDIO E PRATICHE PER SINISTRI

VALIDITA' 5 ANNI

- APPALTATORI - GESTIONE ALBO FORNITORI (RICHIESTE ISCRIZIONE / CANCELLAZIONE)
- LAVORI IN ECONOMIA
- GESTIONE SERVIZIO DI PULIZIA
- AUTORIZZAZIONI PER L'UTILIZZO DI SPAZIO E LOCALI DI PROPRIETA' PROVINCIALE
- MANUTENZIONE VERDE

- MANUTENZIONE ORDINARIA EDIFICI PROVINCIALI

CATEGORIA 7 CACCIA – PESCA - PARCHI

CONSERVAZIONE SENZA LIMITI DI TEMPO

- AMBITI TERRITORIALI DI CACCIA (A T C) - PARCHI, RISERVE NATURALI, AREE PROTETTE / NATURALISTICHE, COSTITUZIONE, VERBALI, STATUTI, REGOLAMENTI, PIANI E PROGETTI
- STUDI E RICERCHE NATURALISTICHE AMBIENTALI
- REGISTRI DELLE INFRAZIONI CACCIA / PESCA
- REGISTRI PESCATORI / CACCIATORI
- ABILITAZIONE VENATORIA: VERBALI, SEDUTE E ESAMI
- DOCUMENTI RELATIVI A TASSIDERMIA (ANIMALI IMBALSAMATI)
- DIRITTI ESCLUSIVI DI PESCA
- PIANO FAUNISTICO VENATORIO / CARTA ITTICA

VALIDITA' 20 ANNI

- GESTIONE IMPIANTI DI ALLEVAMENTO PER RIPOPOLAMENTO ITTICO/VENATORIO

VALIDITA' 10 ANNI

- DOMANDE DI AMMISSIONI AGLI ESAMI VENATORI E TESSERINI VENATORI
- CATTURE A SCOPO SCIENTIFICO ED ALLEVAMENTI A SCOPO ORNAMENTALE
- GUARDIE GIURATE / GEV (GUARDIE ECOLOGICHE VOLONTARIE) – GIV (GUARDIE ITTICHE VENATORIE) dalla cessazione dell'incarico

VALIDITA' 5 ANNI

- CONVEGNI E INIZIATIVE PROMOZIONALI CACCIA / PESCA / PARCHI
- CONVOCAZIONI DEL COMITATO FAUNISTICO VENATORIO E DI COMMISSIONI DIVERSE
- PREVENZIONE E RISARCIMENTO DANNI CAUSATI DA FAUNA SELVATICA
- PIANI DI ABBATTIMENTO SELETTIVO (CINGHIALE, NUTRIE, COLOMBI, ETC)
- MANIFESTAZIONI CINOFILE
- RIPOPOLAMENTO ITTICO / FAUNISTICO
- CALENDARIO VENATORIO / ITTICO
- DOMANDE DI LICENZA DI PESCA
- AUTORIZZAZIONE MESSA IN SECCA - FINI ITTICI - CORPI IDRICI

CATEGORIA 8 LAVORI PUBBLICI - STAZIONE UNICA APPALTANTE - CONTRATTI

CONSERVAZIONE SENZA LIMITI DI TEMPO

- CONTRATTI E RELATIVI REPERTORI

VALIDITA' 10 ANNI

- DOCUMENTAZIONE RELATIVA ALL'ENTE E ALLA SUA (STAZIONE UNICA APPALTANTE)
- DOCUMENTI DI QUALIFICAZIONE DITTE APPALTATRICI
- OFFERTE DI PARTECIPAZIONE DITTE NON AGGIUDICATARIE A GARA E RELATIVA DOCUMENTAZIONE

VALIDITA' 5 ANNI

- PUBBLICAZIONI INDIZIONI / ESITI GARE D'APPALTO (ENTE / SUA)
- ISTANZA DI PARTECIPAZIONE A GARE D'APPALTO (ENTE / SUA)

CATEGORIA 9 VIABILITA' – CONCESSIONI – TRANSITI

CONSERVAZIONE SENZA LIMITI DI TEMPO

- FASCICOLI RELATIVI A GENERALITA' DELLE STRADE
- PROGETTAZIONE E REALIZZAZIONE NUOVE OPERE STRADALI
- MANUTENZIONE STRAORDINARIA OPERE STRADALI, PONTI, PASSAGGI A LIVELLO ETC…
- ESPROPRI
- CONCESSIONI / ACCESSI CARRAI
- AUTORIZZAZIONI PER OCCUPAZIONI PERMANENTI SUOLO PUBBLICO

VALIDITA' 10 ANNI

- CONCESSIONI RELATIVE A CARTELLI PUBBLICITARI
- MANUTENZIONE ORDINARIA STRADE PROVINCIALI

VALIDITA' 5 ANNI

- ORDINANZE E LIMITAZIONI AL TRAFFICO
- AUTORIZZAZIONI TRASPORTI E TRANSITI ECCEZIONALI
- NULLA OSTA PER OCCUPAZIONE TEMPORANEA SUOLO PUBBLICO

CATEGORIA 10 AMBIENTE

CONSERVAZIONE SENZA LIMITI DI TEMPO

- CONCESSIONI DERIVAZIONI ACQUE SOTTERRANEE (POZZI)
- AUTORIZZAZIONI STOCCAGGIO OLI MINERALI
- CAVE - ATTI DI AUTORIZZAZIONE IN MATERIA DI ATTIVITA' ESTRATTIVA
- ESPOSTI IN MATERIA AMBIENTALE E NOTIZIE DI REATO
- DISCARICHE (SMALTIMENTO RIFIUTI)
- VALUTAZIONE IMPATTO AMBIENTALE (V.I.A.) E VALUTAZIONE AMBIENTALE STRATEGICA (V.A.S.) – ATTI RELATIVI
- PROGETTI DI OPERE IDRAULICHE
- AUTORIZZAZIONI LINEE ELETTRICHE ED ELETTRODOTTI - METANODOTTI
- PROGRAMMI PROVINCIALI DI DIFESA DEL SUOLO
- BONIFICHE AMBIENTALI
- AUTORIZZAZIONI IMPIANTI DISTRIBUZIONE CARBURANTE (salvo cessazione)

VALIDITA' 20 ANNI

- AUTORIZZAZIONE UNICA AMBIENTALE (AUA) IN MATERIA DI EMISSIONI, SCARICHI, ETC…

VALIDITA' 10 ANNI

- CONTROLLO IMPIANTI TERMICI (CALDAIE)
- ANALISI PERIODICHE SU IMPIANTI / DEPURATORI

- AUTORIZZAZIONI IMPIANTI MOBILI PER RECUPERO RIFIUTI
- RIFIUTI TRANSFRONTALIERI
- AUTORITA' D'AMBITO (ATO): CONVOCAZIONI – VERBALI
- PRATICA PER LICENZA ANNUALE DI ATTINGIMENTO
- PROGRAMMA DI MANUTENZIONE IDRAULICA
- GESTIONE DEMANIO IDRICO E RISCOSSIONE RELATIVI CANONI
- DICHIARAZIONE VOLUMI D'ACQUA DERIVAZIONI/POZZI
- MONITORAGGIO QUALITA' ARIA – ACQUA
- AUTORIZZAZIONI SPANDIMENTI DI LETAME
- AUTORIZZAZIONI STOCCAGGIO OLI MINERALI (cessate/revocate)
- ATTIVITA' ORDINARIA/ GESTIONE: IMPIANTI DISTRIBUZIONE CARBURANTE CESSATI

CATEGORIA 11 ISTRUZIONE E SERVIZI ALLA PERSONA

CONSERVAZIONE SENZA LIMITI DI TEMPO

- INIZIATIVE CULTURALI E DIDATTICHE PER STUDENTI (ATTUATE DALLA PROVINCIA)
- DIMENSIONAMENTO SCOLASTICO
- ALBO ASSOCIAZIONI VOLONTARIATO
- GESTIONE/RIORDINO EX IPAB ISTITUZIONI DI ASSISTENZA E BENEFICENZA
- ASSISTENZA INFANZIA
- ASSISTENZA ILLEGITTIMI

VALIDITA' 20 ANNI

- ASSISTENZA ALUNNI DISABILI
- CORSI PER IMMIGRATI
- GESTIONE CENTRO SERVIZI – FAMILY AUDIT (CONCILIAZIONE FAMIGLIA/LAVORO) – ANTIDISCRIMINAZIONE (PARI OPPORTUNITA') – ORGANO COMPOSIZIONE CRISI (O.C.C.)
- SERVIZIO CIVILE NAZIONALE VOLONTARIO
- CONSIGLIERA DI PARITA' (CORRISPONDENZA RELATIVA)
- POLITICHE GIOVANILI – L. 16/78 – PROGETTI RELATIVI
- COORDINAMENTO ENTI LOCALI PER LA PACE

VALIDITA' 10 ANNI

- CANCELLAZIONE DALL'ALBO VOLONTARIATO, RENDICONTAZIONI E COMUNICAZIONI
- INIZIATIVE CULTURALI PER STUDENTI

- RICHIESTA DI CONTRIBUTI PER INIZIATIVE SCOLASTICHE
- RAPPORTI CON UNIVERSITA’
- IMMIGRAZIONE: DOMANDE DI CONTRIBUTO E RELATIVE LIQUIDAZIONI

CATEGORIA 12 POLIZIA PROVINCIALE

VALIDITA' 20 ANNI

- VERBALI / CONTRAVVENZIONI STRADALI (NON ASSOLTI)

VALIDITA' 5 ANNI

- VERBALI / CONTRAVVENZIONI (ASSOLTI)

CATEGORIA 13 URBANISTICA – PIANIFICAZIONE TERRITORIALE

CONSERVAZIONE SENZA LIMITI DI TEMPO

- URBANISTICA E PRGC
- PARERI PREVISTI DALLE NORME DEL PIANO DI BACINO
- PARERI PER OPERE ABUSIVE IN ZONE SOTTOPOSTE A VINCOLO IDROGEOLOGICO

VALIDITA' 20 ANNI

- SENTIERI – CARTOGRAFIE - PISTE CICLABILI

VALIDITA' 5 ANNI

- MANUTENZIONE E CENSIMENTO RETE SENTIERISTICA

CATEGORIA 14 TRASPORTI E COMUNICAZIONI

CONSERVAZIONE SENZA LIMITI DI TEMPO

- TPL: PIANI PER IL TRASPORTO PUBBLICO LOCALE, CONCESSIONI / AUTORIZZAZIONI, CONTROLLO E SANZIONI

VALIDITA' 40 ANNI

- ALBO AUTOTRASPORTATORI *
- AUTOSCUOLE *
- REVISIONE AUTOVEICOLI
- NAVIGAZIONE INTERNA SU LAGO MAGGIORE E LAGO D'ORTA
- CONTRASSEGNI NATANTI *

(*) CONSERVARE PER SOLI 5 ANNI SE SI E' VERIFICATA LA CANCELLAZIONE

VALIDITA' 10 ANNI

- PRATICHE CONTROLLO EMISSIONE AUTOVEICOLI - BOLLINI BLU
- TRASPORTO PUBBLICO LOCALE RELATIVAMENTE ALL'ATTIVITA' GIORNALIERA ORDINARIA
- AUTOSCUOLE RELATIVAMENTE ALL'ATTIVITA' GIORNALIERA ORDINARIA
- TESSERE LIBERA CIRCOLAZIONE (SMART CARD BIP)

CATEGORIA 15 TURISMO – SPORT – CULTURA

CONSERVAZIONE SENZA LIMITI DI TEMPO

- AGENZIE DI VIAGGIO *
- PRO-LOCO *
- PUBBLICAZIONI CURATE DALLA PROVINCIA
- INIZIATIVE CULTURALI DI RILIEVO

(*) CONSERVARE PER SOLI 5 ANNI SE SI E' VERIFICATA LA CHIUSURA

VALIDITA' 20 ANNI

- LR 49/91 - ATTIVITA' FORMATIVE NEL SETTORE BANDISTICO, CORALE, STRUMENTALE, DELLE ASSOCIAZIONI, SCUOLE ED ISTITUTI MUSICALI NELLA REGIONE PIEMONTE

VALIDITA' 10 ANNI

- CONTRIBUTI DI CARATTERE CULTURALE / TURISTICO / SPORTIVO / SOCIALE
- PARTECIPAZIONE AD INIZIATIVE CULTURALI DI CARATTERE OCCASIONALE O CONTINUATIVO

VALIDITA' 5 ANNI

- RILEVAZIONI STATISTICHE ALBERGHIERE
- ESAMI PROFESSIONI TURISTICHE / NATURALISTICHE

CATEGORIA 16 PROTEZIONE CIVILE

CONSERVAZIONE SENZA LIMITI DI TEMPO

- PROTEZIONE CIVILE - PROGRAMMI DI PREVISIONE E PREVENZIONE E PIANI DI EMERGENZA

VALIDITA' 20 ANNI

- CENSIMENTO DANNI / EVENTI CALAMITOSI
- PROGETTI CONNESSI A DISASTRI NATURALI

VALIDITA' 5 ANNI

- PROTEZIONE CIVILE: FORMAZIONE DEI VOLONTARI
- COMUNICAZIONI RELATIVE AL COC (Centro Operativo Comunale)

MATERIE NON PIU' DI COMPETENZA PROVINCIALE

CATEGORIA 17 CENTRI PER L'IMPIEGO - FORMAZIONE E LAVORO

<u>CENTRI PER L'IMPIEGO</u>

CONSERVAZIONE SENZA LIMITI DI TEMPO

- SCHEDE RIASSUNTIVE RELATIVE A COMUNICAZIONI DI ASSUNZIONE/ CESSAZIONE

VALIDITA' 10 ANNI

- RICHIESTE E CERTIFICATI RELATIVI ALLE LISTE DI COLLOCAMENTO
- RICHIESTA DI AVVIAMENTO A SELEZIONE PRESSO ENTI PUBBLICI
- DOMANDE DI INSERIMENTO LISTE DI MOBILITA'
- TRASFORMAZIONE DI RAPPORTI DI LAVORO E RAPPORTI DI APPRENDISTATO
- TRASFERIMENTI DI ISCRIZIONE COLLOCAMENTO ORDINARIO
- COMUNICAZIONE CON DITTE RELATIVE AL RISPETTO DELLA L. 68/99 SUL COLLOCAMENTO OBBLIGATORIO
- LAVORI SOCIALMENTE UTILI

FORMAZIONE E POLITICHE DEL LAVORO

CONSERVAZIONE SENZA LIMITI DI TEMPO

- ATTIVITA' RELATIVE A CORSI: VERBALI INIZI / FINE CORSI - VERBALI DEGLI ESAMI E RELATIVI ATTESTATI, VERBALI DI COMMISSIONI ESAMINATRICI D'ESAME, VERBALI CON RISULTANZE ESAMI FINALI E REGISTRI DEI CORSI
- MATERIALE AFFERENTE A SITUAZIONI DI IRREGOLARITÀ E/O CON PROCEDIMENTI GIUDIZIARI

VALIDITA' 15 ANNI

- L.R. 23/93 - NORME DI ATTUAZIONE PER LA PROMOZIONE E LO SVILUPPO DELLA COOPERAZIONE SOCIALE - PRATICHE DI CONTRIBUTI CONCESSI
- ATTIVITA' RELATIVE A CORSI REALIZZATE SU FINANZIAMENTI EUROPEI E NAZIONALI

VALIDITA' 10 ANNI

- ATTIVITA' RELATIVE A CORSI NON REALIZZATE (REVOCATE, SOSPESE, NON FINANZIATE) SU FINANZIAMENTI EUROPEI E NAZIONALI
- COMUNICAZIONI ASSUNZIONI, CESSAZIONI, TRASFORMAZIONI RAPPORTI DI LAVORO E DI APPRENDISTATO
- MATERIALE RELATIVO ALLA CASSA INTEGRAZIONE GUADAGNI, ALLA CREAZIONE D'IMPRESA (L.R. 34/2008), AI BANDI "ASILI NIDO" E, IN GENERALE, FINANZIATO IN BASE A NORMATIVA NAZIONALE E/O REGIONALE
- POR (PROGRAMMI OPERATIVI REGIONALI) CON DECORRENZA DALL'ANNO SUCCESSIVO ALLA

DICHIARAZIONE CHIUSURA ATTIVITA' DA PARTE DELLA COMMISSIONE EUROPEA:

POR 2000/2006 – CHIUSURA 2011 – SCARTO 2022

POR 2007/2013 – CHIUSURA 2018 – SCARTO 2029

VALIDITA' 5 ANNI

- DOMANDE PER CONTRIBUTI NON CONCESSI

AGRICOLTURA

CONSERVAZIONE SENZA LIMITI DI TEMPO

- ALLEVAMENTO: REGISTRI, RUBRICHE E FASCICOLI

VALIDITA' 20 ANNI

- QUOTE LATTE

VALIDITA' 10 ANNI

- USO PRODOTTI FITOSANITARI
- DOMANDE U.M.A. (UTENTI MACCHINE AGRICOLE) E RELATIVA MODULISTICA
- TAGLIO ALBERI IN ZONE SOGGETTE A VINCOLO IDROGEOLOGICO
- VITICOLTURA - ESTIRPAZIONE VIGNETI
- APICOLTURA - REGISTRO ARNIE
- FLORICOLTURA
- ASSEGNAZIONE QUOTE AGRICOLE (RISO, CEREALI, ETC.)
- RISICOLTURA – GENERALITA'
- RICHIESTE RISARCIMENTO DANNI ALLE COLTURE

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 3

Linee guida per il versamento dei fascicoli

Linee guida per la chiusura e il versamento dei fascicoli in archivio di deposito

Le indicazioni fornite di seguito si applicano al versamento dei fascicoli analogici, ibridi e, per quanto compatibili, digitali.

Se per i fascicoli cartacei occorre organizzare la consegna ed il trasferimento fisico dei documenti, per i fascicoli digitali tale attività non è prevista in quanto la documentazione risulta già acquisita nel sistema di protocollo informatico e gestione documentale.

I fascicoli digitali vanno aperti, alimentati e chiusi conformemente alle modalità indicate nella manualistica resa disponibile dalla Ditta fornitrice del programma di protocollo.

1. **Verifica preliminare**

Tutti i documenti devono essere classificati e fascicolati a cura dell'Ufficio che li produce, di conseguenza la prima attività da fare per la chiusura dei fascicoli, è verificare che tutti i documenti assegnati siano stati classificati/fascicolati nel sistema di protocollo informatico.

Il fascicolo rappresenta l'unità archivistica ovvero l'elemento minimo di cui è composto l'archivio pertanto non è consentito inviare "agli atti" documenti "sciolti" cioè non contenuti nel proprio fascicolo o blocchi di documenti non ordinati.

2. **Lo sfoltimento del fascicolo**

Con riferimento ai fascicoli cartacei, prima della trasmissione all'archivio, gli uffici devono effettuare lo sfoltimento, ovvero eliminare tutto quel materiale che non è documentazione e che quindi può essere inviato al macero (appunti, fotocopie, bozze, brutte copie ecc.).

Devono essere inoltre eliminati elastici e plastiche che col tempo potrebbero degradarsi e danneggiare la documentazione.

Non rappresentano materiale documentale da conservare in archivio, pubblicazioni, libri, riviste, giornali, raccolte normative ecc., fatta salva la valutazione in ordine all'acquisizione di libri e pubblicazioni utili ad incrementare il fondo bibliotecario dell'ente.

Il fascicolo deve contenere documenti originali e al suo interno, i documenti devono essere posti in ordine cronologico, dal documento più datato a quello più recente.

Anche in caso di avvenuta scansione di documenti cartacei non è consentita la distruzione dell'originale che deve essere comunque conservato.

Di contro, non deve essere inserita nel fascicolo cartaceo la stampa di documenti firmati digitalmente.

Tutti i documenti informatici, e quindi a maggior ragione quelli firmati digitalmente, hanno valore legale solo in ambiente digitale, la semplice stampa degli stessi ai fini archivistici, non ha alcun valore e non deve essere conservata in archivio.

Non deve quindi essere inserita nel fascicolo la stampa degli atti dirigenziali sottoscritti con firma digitale.

Sempre a titolo esemplificativo non devono essere stampati:

- Fatture elettroniche;
- Durc;
- Certificati del casellario giudiziale;
- Certificati dell'Agenzia delle Entrate.

Non è corretto inoltre, stampare il documento firmato digitalmente per apporre la firma autografa, l'originale del documento rimane quello firmato digitalmente che deve essere acquisito nel sistema di gestione documentale.

Non è richiesto inserire nel fascicolo:

- la stampa delle ricevute generate dalla spedizione a mezzo PEC (accettazione, consegna, mancata consegna);
- la stampa della mail di trasmissione generate automaticamente dal sistema di protocollo informatico;
- la stampa di mail o schermate relative alla pubblicazione all'Albo Pretorio;
- la stampa di schermate delle piattaforme Mepa, Appalti e contratti et similia.

3. **Elenco dei documenti contenuti nel fascicolo**

Ogni fascicolo cartaceo deve essere accompagnato dall'elenco dei documenti in esso contenuti.
I documenti informatici non devono essere stampati, è fondamentale che il file sia caricato nel sistema di protocollo informatico per garantirne la validazione temporale e la conservazione digitale.
L'elenco ha lo scopo di documentare la composizione del fascicolo prima del suo versamento in archivio di deposito e deve essere allegato alla richiesta di versamento.

4. **Richiesta di versamento**

Il Dirigente/l'incaricato/a di elevata qualificazione redige la richiesta di versamento che dovrà essere firmata e trasmessa al Responsabile del Servizio Gestione documentale.
Per la predisposizione della richiesta utilizzare l'apposito modello riprodotto in coda al presente allegato.

5. **Chiusura dei fascicoli e verbale di versamento**

Con la chiusura del fascicolo ed il suo versamento in archivio di deposito, si realizza il passaggio di responsabilità tra l'Ufficio "titolare del fascicolo" ed il Responsabile dell'Archivio, che assume il compito di conservare la documentazione in maniera appropriata e di consentirne il reperimento e la consultazione nel tempo, nel rispetto della normativa vigente.
Si rammenta che il fascicolo chiuso non può essere riaperto e di conseguenza non sarà possibile inserire al suo interno altri documenti, e dall'anno di chiusura decorrono i termini di conservazione del fascicolo.
Per ciascun fascicolo sarà definito il tempo di conservazione al termine del quale si procederà allo scarto salvo i casi di conservazione permanente.
Per i fascicoli cartacei sulla camicia del fascicolo saranno annotati la data di chiusura e la data di versamento in archivio di deposito.

Richiesta di versamento

ALL'UFFICIO ARCHIVIO
S E D E

Si consegna allegato alla presente il seguente fascicolo da inviare all'archivio di deposito.

CLASSIFICAZIONE FASCICOLO **(a cura ufficio richiedente)**	**ID_ARCHIVIO FASCICOLO** **(a cura uff. richiedente)**	**OGGETTO FASCICOLO** **(a cura dell'ufficio richiedente)**

Al riguardo si dichiara:

- di aver verificato che la documentazione attinente a procedimenti con decorrenza successiva all'avvio della procedura di protocollo informatico sia stata acquisita, protocollata ed inserita in fascicoli in formato elettronico;

- di aver verificato che non siano presenti doppioni di lettere o documenti superflui già imputati e in carico ad altro responsabile di procedimento.

data firma p. Ufficio

NB. Il presente modulo debitamente sottoscritto dovrà essere consegnato in duplice copia all'ufficio archivio unitamente ai fascicoli da inviare all'archivio di deposito.

L'ufficio archivio ne restituirà una copia firmata per ricevuta e con l'indicazione della numerazione di archivio di deposito assegnata.

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 4

Fac simile *Elenco degli atti che si propongono per lo scarto*

ENTE: _____ **- ELENCO DEI DOCUMENTI CHE SI PROPONGONO PER LO SCARTO**

ALLEGATO ALLA NOTA PROT. N. _____ DEL _____ PAG. _____ DI _____

Numero d'ordine[1]	**Unita'**	**Categoria**	**classifica**	**Descrizione** [2]	**Estremi cronologici**[3]	**Quantità**[4]	**Motivazioni**[5]	**Note**

FIRMA DEL RESPONSABILE DELLA GESTIONE DOCUMENTALE (DPR 445/2000, art. 61 c. 2): _____

[1] Numerazione unica e progressiva dell'intero elenco di scarto, evitando di inserire sotto lo stesso numero tipi diversi di documenti
[2] Evitare le abbreviazioni, le sigle e le espressioni generiche o gergali
[3] Indicare l'anno più antico e l'anno più recente dei documenti
[4] Indicare il tipo di contenitori (fascicoli, faldoni, scatole …) e il numero dei medesimi
[5] Si vedano le istruzioni per la compilazione della proposta di scarto

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 5

Linee guida per la pubblicazione all'Albo Pretorio online

1. Oggetto ed ambito di applicazione

Il presente documento disciplina le modalità con le quali l'Ente organizza e gestisce l'Albo Pretorio online.
La pubblicazione all'Albo Pretorio online sostituisce ogni altra forma di pubblicazione legale, salvo i casi previsti da leggi o regolamenti ed è finalizzata a fornire presunzione di conoscenza legale dei documenti a qualunque effetto giuridico specifico essa assolva, e nei casi espressamente previsti dalla legge, ad integrarne la validità o l'efficacia.

2. Modalità di accesso

Sulla homepage del sito web istituzionale dell'Ente https://www.provincia.novara.it è disponibile il link "Albo pretorio" che consente l'accesso alla sezione dedicata alla pubblicazione dei documenti.
Per facilitare l'accessibilità alle diverse tipologie di atti pubblicati, l'Albo Pretorio online è suddiviso in specifiche sezioni, a seconda della tipologia documentale.
Limitatamente al periodo di pubblicazione, sono pubblicati i testi dei provvedimenti; trascorso tale periodo, in "Atti Archiviati" è possibile consultare solo gli estremi degli atti pubblicati.
I documenti pubblicati all'Albo Pretorio online sono elencati e visualizzati in ordine cronologico di pubblicazione con l'indicazione della data di inizio e fine del periodo di pubblicazione.
Il sistema consente all'utente ricerche dei documenti per tipo pubblicazione, oggetto, registro, settore proponente, numero, data di pubblicazione.
Limitatamente al periodo di pubblicazione, l'acquisizione da parte degli utenti dei documenti pubblicati dal sito web dell'Ente avviene gratuitamente e senza formalità.

3. Modalità di pubblicazione

La pubblicazione dei documenti avviene in forma integrale, per estratto o mediante avviso.

La pubblicazione integrale di un documento comporta la pubblicazione del documento principale e di tutti gli eventuali allegati.
Tutti gli allegati parte integrante di un provvedimento devono essere firmati digitalmente.

La pubblicazione per estratto o "con omissis" risulta necessaria per proteggere alcuni dati personali e informazioni contenute nel documento principale o nei suoi allegati.
L'estratto di un documento può essere definito come un nuovo documento nel quale si riportano o attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di una pubblica amministrazione, o comunque un documento nel quale sono omesse in maniera evidente alcune parti del documento originale.
Il documento con omissis e il documento originario nella versione integrale sono conservati nello stesso fascicolo informatico.

La pubblicazione mediante avviso risulta necessaria nel caso in cui occorre rinviare ad altro documento già oggetto di pubblicazione o nel caso in cui per caratteristiche oggettive dei documenti non fosse possibile procedere materialmente alla pubblicazione.
Qualora la tipologia (es. cartografie/planimetrie) e/o la consistenza e/o il numero degli atti da pubblicare, non ne consentano l'integrale affissione all'Albo Pretorio online, si procede come segue:
verrà predisposto a cura dell'Ufficio proponente un apposito avviso da pubblicare all'Albo Pretorio online in luogo e/o in aggiunta dell'atto da pubblicare, dal quale si evincano tutti gli elementi essenziali (ente ed organo da cui promana, l'oggetto, la data di adozione, il numero di protocollo ed ogni altro elemento utile) attraverso cui sia possibile individuare univocamente il documento e sinteticamente il contenuto, nonché l'Ufficio presso il quale lo stesso documento è consultabile integralmente e contemporaneamente, durante il periodo di pubblicazione del relativo avviso.

Le pubblicazioni all'Albo Pretorio online sono gestite in modalità parzialmente decentrata con responsabilità della pubblicazione in capo all'Unità organizzativa procedente.

4. Periodo di pubblicazione

Il periodo di pubblicazione è di quindici giorni interi e consecutivi, salvo termini diversi previsti da leggi, da regolamenti o stabiliti dall'Ente o dal richiedente la pubblicazione.

Di norma i documenti soggetti a termini di scadenza per la presentazione di istanze sono pubblicati sino al giorno della scadenza.

Per le pubblicazioni richieste da enti esterni la pubblicazione avviene secondo le date di inizio e di fine pubblicazione indicate nella richiesta restando a carico del richiedente la correttezza dei termini comunicati.

L'Albo Pretorio online è accessibile in tutti i giorni dell'anno, salvo interruzioni determinate da cause di forza maggiore ovvero interventi di manutenzione dell'infrastruttura informatica necessari ed indispensabili per il corretto funzionamento del sito informatico e dell'Albo adeguatamente segnalati sul sito dell'Ente.

Alla scadenza del periodo di pubblicazione i documenti pubblicati sono ritirati automaticamente e non più consultabili, rimangono a disposizione gli estremi della pubblicazione.

5. Formato dei documenti da pubblicare

Di norma i documenti da pubblicare sono sottoscritti con firma digitale, in via residuale si procede alla pubblicazione di documenti in formato pdf.

6. Gestione del servizio

La responsabilità del contenuto e la pertinenza dei dati pubblicati, anche ai fini delle disposizioni in materia di tutela dei dati personali, ricade esclusivamente in capo al Dirigente dell'Unità organizzativa che sottoscrive e adotta il provvedimento o al soggetto esterno che ne richiede la pubblicazione.

7. Certificazione di avvenuta pubblicazione

Il sistema informatico di gestione dell'Albo Pretorio online consente di generare le relate di pubblicazione che attestano l'avvenuta pubblicazione degli atti.

8. Pubblicazioni per conto di pubbliche amministrazioni o altri soggetti

Il servizio di anticamera dell'Ente provvede alla pubblicazione all'Albo Pretorio online dei documenti provenienti da altre pubbliche Amministrazioni o altri soggetti di natura pubblica che ne facciano richiesta.

I documenti dovranno essere in formato pdf preferibilmente sottoscritti con firma digitale.

Nella richiesta di pubblicazione dovranno essere specificati l'oggetto del documento ed il periodo di pubblicazione, se questo non è indicato si procederà con la pubblicazione per quindici giorni.

Di norma, salvo che non sia prevista da legge, o comunque espressamente richiesto, l'Ente non fornisce comunicazione scritta dell'avvenuta pubblicazione che potrà essere verificata tramite la consultazione del sito web.

A seguito di esplicita richiesta del richiedente, l'Ente provvede all'invio della relata di pubblicazione tramite posta elettronica certificata.

9. Sicurezza e riservatezza delle pubblicazioni

La pubblicazione è effettuata limitatamente al periodo previsto dall'ordinamento, per rispettare i principi di necessità, di proporzionalità, di temporaneità, di pertinenza e non eccedenza e per garantire il diritto all'oblio.

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 6

Il piano di fascicolazione è redatto conformemente allo schema di massima qui a seguito riportato:

Id	Classificazione e descrizione	Tipologia	Fascicolo sottofascicolo	Oggetto fascicolo/sottofascicolo	Tipologie di documenti presenti nel fascicolo/sottofascicolo	Ufficio Competenza	Tempi di Conservazione	Note di Scarto

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 7

Decreto del Presidente n. 61 del 29.04.2021

APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

PROVINCIA DI NOVARA

DECRETO DEL PRESIDENTE

Decreto n. 61 del 29/04/2021

OGGETTO: APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

L'anno duemilaventuno il giorno ventinove del mese di aprile in Novara e nel Palazzo della Provincia

IL PRESIDENTE

Ai sensi di quanto disposto dall'art. 1 comma 54 e 55 della Legge 56/2014 che stabilisce l'individuazione degli organi della Provincia nonché i poteri e le prerogative del Presidente della Provincia,

Con l'assistenza, per il presente atto, del Segretario Generale dott. ROSSI GIACOMO

ADOTTA

il provvedimento che segue:

Decreto n. 61 del 29/04/2021

Oggetto: APPROVAZIONE DELLA PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

IL PRESIDENTE

Premesso che:
- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

- la Provincia di Novara, in quanto Titolare del trattamento, è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (data breach), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

Visti:
- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");
- il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (di seguito "Codice");
- il decreto legislativo 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "d.lgs. n. 51/2018");
- le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;
- la "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities", adottata ai sensi dell'art. 64 del Regolamento, dal Comitato europeo per la protezione dei dati in data 12 marzo 2019;
- il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [doc-web n. 9126951];

Considerato che:

- in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (artt. 33 e 55 del

Regolamento, art. 2-bis del Codice);

- il titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero (artt. 26 e 37, comma 6, del d.lgs. n. 51/2018);
- per «violazione dei dati personali» (data breach) si intende 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 (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del d.lgs. n. 51/2018);
- per la omessa notifica di data breach all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative di cui all'art. 83 GDPR, nonché le misure correttive di cui all'art. 58 GDPR;
- inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno;

Ritenuto pertanto

a) di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (data breach policy). A tale riguardo si precisa che, presso il Titolare, sono già state attivate procedure a tutela della sicurezza dei dati, ed in particolare si richiama il decreto n. 47 del 2/04/2021 di approvazione del "Piano di Protezione e del Modello Organizzativo a tutela dei dati personali";

b) strategico per la Provincia:

    - sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
    - definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
    - definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
    - assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate;
    - stabilire che le procedure contemplate nell'approvando documento siano applicabili a tutte le attività svolte dal Titolare, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni;
    - stabilire che il rispetto dell'adottanda procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia. In particolare le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:

i. I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso del prestazioni richieste per conto del Titolare del trattamento;
ii. qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

Visto il Decreto del Presidente n. 75 in data 20/05/2020 con il quale è stato designato l'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO), nel rispetto della vigente normativa;

DECRETA

1. di approvare la procedura per la gestione dei casi di violazione dei dati personali (data breach) della Provincia di Novara, richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679), qui allegata quale parte integrante e sostanziale del presente decreto;

2. di inviare la procedura nel caso di violazione dei dati personali (data breach) della Provincia di Novara al Responsabile del Trattamento dei Dati personali già nominato, in persona dell'Avv. Massimo Ramello;

3. di disporre che al presente provvedimento venga assicurata:

a) la pubblicità legale con pubblicazione all'Albo Pretorio, nonché sul sito dell'Ente nell'Amministrazione Trasparente;

b) la massima diffusione presso tutto il personale operante presso la Provincia e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento;

4. di dare atto che il presente provvedimento è compatibile con gli stanziamenti di bilancio e con le regole di finanza pubblica;

5. di dichiarare il presente provvedimento immediatamente eseguibile ai sensi dell'art. 134, 4° comma, del D.lgs. 267/2000 e s.m.i..

PROVINCIA DI NOVARA

Decreto n. 61 del 29/04/2021

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i. e contestualmente pubblicato all'albo pretorio per quindici giorni consecutivi dal 29.04.2021 al 14.05.2021.

IL Segretario Generale
ROSSI GIACOMO
sottoscritto con firma digitale

IL Presidente
BINATTI FEDERICO
sottoscritto con firma digitale

DISPOSIZIONI OPERATIVE
IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI (c.d. DATA BREACH)

Approvato con decreto n. del

Sommario

FINALITÀ E AMBITO DI APPLICAZIONE....3

DEFINIZIONI....5

PIANO DI AZIONE....7

PROCEDURA....8

1. Individuazione della violazione....9

2. Rilevazione della violazione....13

2.1. Acquisizione della notizia....13
2.2. Fonte della notizia....13
2.3. Il monitoraggio degli eventi di sicurezza con impatto sulla protezione dei dati personali....14
2.4. Trasmissione della notizia....15

3. Analisi e Valutazione della violazione....16

3.1. Analisi tecnica dell'evento....16
3.2. Valutazione della violazione al fine del rispetto degli obblighi di notifica e comunicazione....17
3.3. Valutazioni supplementari....22

4. Notifica della violazione dei dati personali all'Autorità di controllo....22

4.1. Quando effettuare la notificazione....22
4.2. Come effettuare la notificazione....23
4.3. Eventuali ulteriori notificazioni (o denunce)....24

5. Recepimento della eventuale risposta dell'Autorità di controllo....24

6. Comunicazione della violazione dei dati personali all'interessato....24

6.1. Quando effettuare la comunicazione....25
6.2. Come effettuare la comunicazione....25
6.3. Quali informazioni comunicare....26
6.4. Quando non effettuare la comunicazione....26

7. Altre segnalazioni....26

8. Documentazione della violazione....27

8.1. il Registro delle violazioni....27
8.2. Altri documenti ed informazioni....28

9. Fase di miglioramento....29

10. Fattispecie di contitolarità e responsabilità del trattamento....29

FONTI....30

FINALITÀ E AMBITO DI APPLICAZIONE

La Provincia di Novara ai sensi del Regolamento Europeo 2016/679 (da qui in avanti **GDPR**), in quanto Titolare del trattamento (di seguito, per brevità, "**Titolare del trattamento**" o anche solo "**Titolare**"), è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (di seguito, per comodità, "**data breach**"), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati.

Il **mancato rispetto** dell'obbligo di notifica ex articolo 33 del GDPR comporta l'applicabilità da parte dell'autorità di controllo delle **sanzioni amministrative** previste dall'art. 83, con la possibilità di infliggere sanzioni fino a 10.000.000 di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4). L'autorità potrebbe inoltre applicare le misure correttive previste dall'art. 58 GDPR e, quindi, rivolgere al titolare avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti provvisori o definiti al trattamento e di divieti, ordini di rettifica e cancellazione dei dati, revoche di certificazioni, ordini di sospendere i flussi di dati verso paesi terzi o organizzazioni internazionali.

Il GDPR prevede poi espressamente che al momento della decisione in merito alla sanzione amministrativa pecuniaria da infliggere ed alla definizione del suo ammontare, è necessario tenere conto nel caso concreto anche delle misure adottate dal titolare per attenuare il danno subito dagli interessati, come pure del grado di responsabilità del titolare (o del responsabile) alla luce delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32. La stessa mancata notifica all'autorità di controllo, e/o comunicazione all'interessato, potrebbero d'altro canto essere considerate nel caso specifico indici di una mancata adozione di misure di sicurezza che potrebbe portare all'irrogazione di specifiche sanzioni al riguardo.

Inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il **risarcimento del danno** dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

E' pertanto di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (**data breach policy**). A tale riguardo si precisa che, presso il Titolare, sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

- l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
- l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;
- la predisposizione di un sistema di protezione, mediante apposite misure tecniche (firewall, antivirus, …) dell'accesso a internet e ai dispositivi elettronici.

I dati oggetto di riferimento sono i dati personali trattati "*da* "e "*per conto*" del Titolare, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

Il presente documento ha lo scopo di indicare le **modalità di gestione di un data breach**, ovvero di un episodio di violazione di dati personali (come meglio spiegato nel prosieguo), nel rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 679/2016 sulla protezione dei dati personali (GDPR).

L'obiettivo del presente documento è, pertanto:

- sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
- assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate.

Le procedure qui contemplate sono applicabili a **tutte le attività svolte dal Titolare**, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni.

Le procedure descritte nel presente documento sono rivolte a **tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare**, quali:

a) I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;

b) qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

In questo documento si sintetizzano le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa nella gestione del data breach, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare del trattamento;
- valutazione dell'evento accaduto;
- modalità e profili di notificazione all'Autorità di controllo;
- eventuale comunicazione agli interessati

garantendo al tempo stesso:

- l'identificazione della violazione;

- l’analisi delle cause della violazione;
- la definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- la registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

DEFINIZIONI

Fermo restando che le uniche definizioni “ufficiali” e vincolanti sono quelle contenute nell’articolo 4 del GDPR e quelle contenute nel Codice per la protezione dei dati personali (D.Lgs. 30 giugno 2003 n. 196), si riporta la terminologia maggiormente utilizzata nel contesto del presente documento, per semplificarne la lettura.
«**GDPR**» o «**RGPD**» o «**Regolamento**»: il Regolamento (UE) n. 679/2016 “General Data Protection Regulation”, in italiano indicato come “Regolamento generale sulla protezione dei dati”;
«**CODICE PRIVACY**»: il Decreto Legislativo 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”;
«**DATO PERSONALE**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
«**CATEGORIE PARTICOLARI DI DATI PERSONALI**»: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
«**DATI RELATIVI ALLA SALUTE**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
«**DATI GENETICI**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
«**DATI BIOMETRICI**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
«**ARCHIVIO**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
«**TRATTAMENTO**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
«**PSEUDONIMIZZAZIONE**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a

condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
«**COMUNICAZIONE**»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies del Codice privacy, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
«**DIFFUSIONE**»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
«**INTERESSATO**»: la persona fisica cui si riferiscono i dati personali;
«**TITOLARE DEL TRATTAMENTO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
«**RESPONSABILE DEL TRATTAMENTO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
«**RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**» o «**DPO**»: soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire consulenza sugli obblighi derivanti dal GDPR e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (GDPR, art. 37, 38, 39);
«**DESTINATARIO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
«**TERZO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
«**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;
«**MINACCIA**»: una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale;
«**DANNO**»: conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto interessato;
«**MALWARE**»: software di tipo malevolo che causa danni ai sistemi informativi;
«**MISURA DI SICUREZZA**»: accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti;

«**CRITTOGRAFIA**»: tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario;
«**DECRITTOGRAFIA**»: il processo per "sbloccare" i dati criptati cioè cifrati;
«**AUTORITÀ DI CONTROLLO**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. In Italia, il Garante per la Protezione dei Dati Personali;
«**WP ARTICOLO 29**»: gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito della protezione dei dati personali e della vita privata, istituito ai sensi dell'art. 29 della direttiva 95/45/CE. A decorrere dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB) ai sensi del regolamento generale sulla protezione dei dati dell'UE (GDPR) (regolamento (UE) 2016/679);

PIANO DI AZIONE

Si individua il seguente piano d'azione per assicurare la conformità (compliance) del Titolare alle previsioni normative in tema di protezione dei dati personali. Il piano evidenzia in rosso le azioni "obbligatorie" ed in giallo quelle "non obbligatorie ma vivamente consigliate". Trattasi ovviamente di indicazioni di massima, debitamente integrate dalle regole contenute nel prosieguo del documento, che sono suscettibili di modifica ed integrazione in considerazione dell'evoluzione normativa e tecnica e delle peculiari caratteristiche organizzative del Titolare.

Azione	Annotazioni
Adottare una procedura interna di gestione dei data breach (obbligatorio)	Attraverso la presente policy sono definiti i ruoli e le responsabilità nella gestione degli incidenti e delle violazioni
Istruire il personale autorizzato al trattamento dei dati in materia di sicurezza e gestione di possibili violazioni (obbligatorio)	Il personale dev'essere in grado di identificare e gestire eventuali violazioni di dati personali
Verificare lo stato delle misure di sicurezza implementate presso l'Ente (consigliato)	Condurre audit sui sistemi informatici e non. Il GDPR richiede infatti che siano implementate tutte le misure tecnologiche ed organizzative per valutare se sia avvenuta una violazione di dati; tali misure aiutano anche a stabilire se sia necessaria o meno la notifica
Cifrare o pseudonimizzare i dati di cui agli articoli 9 e 10 del GDPR (obbligatorio)	
Limitare l'accesso ai dati personali solo al personale autorizzato (obbligatorio)	E' opportuno limitare l'accesso per ridurre le possibilità di eventuali violazioni, che spesso sono provocate anche da errore umano
Verificare le misure di sicurezza installate sui computer al fine di eliminare le vulnerabilità ed implementare misure di sicurezza logiche e fisiche adeguate (obbligatorio)	Occorre valutare le misure di sicurezza anche al fine di dimostrare la c.d. "accountability"
Preparare un piano di risposta alle violazioni (obbligatorio)	Il piano dovrebbe prevedere le seguenti azioni: – assicurare che i dati non siano più compressi; – mettere in sicurezza tutti i dati ed i sistemi;

	– identificare i dati compromessi, le categorie di Interessati coinvolte, la tipologia di violazione; – isolare i dati compromessi; – modificare le chiavi di codifica e le relative password immediatamente; – documentare tutte le fasi di gestione della violazione e tutte le informazioni relative alla violazione stessa; – determinare quando sia effettivamente avvenuta la violazione (al fine di notificare la violazione entro 72 ore)
Coinvolgere le autorità competenti ove si sospettino attività illecite (obbligatorio)	Non è strettamente richiesto dal GDPR, ma è opportuno notificare la violazione anche ad altre autorità, ove applicabile e richiesto dalla normativa vigente
Selezionare adeguatamente i fornitori che erogano attività che comportano un trattamento di dati (obbligatorio)	E' opportuno verificare e selezionare il fornitore e assicurare che la designazione come Responsabile contenga previsioni e istruzioni specifiche in materia di data breach
Conclusa la gestione urgente della violazione, valutare i "gaps" e l'efficacia dei sistemi interni, della formazione del personale e delle ulteriori procedure che mirano a tutelare i dati personali (obbligatorio)	Tale attività potrebbe essere inclusa in una fase di post-assessment
Testare frequentemente i sistemi interni (consigliato)	
Conservare un registro dei data breach ed aggiornarlo frequentemente (obbligatorio)	Il Titolare è tenuto a comunicare ogni informazione sulla violazione all'Autorità di controllo e per tale motivo è opportuno implementare un registro di data breach

PROCEDURA

Si individuano di seguito i soggetti coinvolti ed il flusso delle principali attività previste per la rilevazione e gestione di un incidente di sicurezza che possa comportare una violazione di dati personali.

La **tempestività** è un fattore determinante nella risposta agli incidenti sulla sicurezza ed ai data breach ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

La risposta a un Incidente sulla sicurezza o ad un data breach deve avvenire secondo le fasi descritte di seguito. Considerando, tuttavia, che gli Incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti. È tuttavia fatto obbligo ad ogni soggetto sotto la responsabilità del Titolare di collaborare e seguire le istruzioni che di volta in volta gli vengano fornite dallo stesso Titolare o dal DPO.

Considerati i rischi e, in caso di data breach, le ridotte tempistiche per effettuare la notifica e per la comunicazione agli interessati, occuparsi degli incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione. Nella gestione di un qualunque incidente di sicurezza devono essere considerate le seguenti due priorità:

o **prima priorità**: proteggere tutti gli assets del Titolare, incluse le risorse colpite dall'incidente, fino al ripristino della normale operatività;

o **seconda priorità**: raccogliere informazioni e prove per supportare le eventuali e appropriate azioni correttive, disciplinari o legali;

Tutti gli incidenti di sicurezza ed i data breach devono essere trattati con il **massimo livello di riservatezza**: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

Tutte le attività di gestione devono essere **tracciate e documentate** per quanto possibile a partire dall'istante di rilevazione.

Il **coordinamento delle attività di gestione** di una violazione di dati personali, con particolare riferimento agli obblighi di comunicazione e notifica imposti dal GDPR, è assicurato dal DPO con il supporto dell'Amministratore di sistema (od altra figura analoga), per gli aspetti tecnici e dell'Ufficio Legale per gli aspetti giuridici, nonché dal Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto. Il DPO ha comunque piena facoltà di convocare e coinvolgere altri soggetti che ritenga utili alle necessità del caso.

1. Individuazione della violazione

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.). **Tuttavia, come indicato all'articolo 4, punto 12, il GDPR si applica soltanto in caso di violazione di dati personali**.

La conseguenza di tale violazione è che il Titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

L'art. 33 del GDPR prescrive che "*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

Per *data breach* si intende quindi un evento in conseguenza del quale si verifica una "*violazione dei dati personali*". Nello specifico, l'articolo 4 punto 12 del GPDR definisce la violazione dei dati personali come "*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*". Non è quindi corretta la comune associazione tra data breach ed attacco o problema informatico poiché tale violazione può

avvenire anche (ad esempio) a causa di un dipendente infedele che sottragga documentazione cartacea ovvero la smarrisca.

Il Gruppo di lavoro ex art. 29 ("WP29") ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "data breach") ai sensi del Regolamento UE n. 679/2016 (cd. "GDPR").

Con il termine "**Distruzione"** (*destruction*) si intende che non esistono più i dati ovvero i dati non esistono più in una forma che possa essere utilizzata dal Titolare. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro i sette giorni.

Con il termine "**Modifica"** (*alteration, damage*) si intende la possibilità che avvengano modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.

Con il termine "**Perdita"** (*loss*) si intende che i dati esistono ancora, ma il Titolare potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore a sette giorni. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati.

Per "**rivelazione**" si intende la trasmissione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.

Per "**accesso**" si intende l'accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

Un **trattamento non autorizzato o illecito** può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del GDPR.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione in base ai seguenti **tre principi di sicurezza delle informazioni**:

Violazione della riservatezza *(Confidentiality breach)*	**divulgazione** o accesso non autorizzato o accidentale ai dati personali come, ad esempio: • quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza; • quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento; • quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone prendono visione di informazioni; • quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato.
Violazione dell'integrità *(Integrity breach)*	**alterazione** non autorizzata o accidentale dei dati personali La "*alterazione*" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).
Violazione della disponibilità *(Availability breach)*	accidentale o non autorizzata **perdita di accesso** o **distruzione** di dati personali (Fattispecie non sempre di facile individuazione. La "*perdita di dati*" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi; la "*distruzione*" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal Titolare. Ci sarà sempre una violazione della Disponibilità del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione)

Ci si potrebbe chiedere se una **perdita temporanea della disponibilità** dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrà essere documentata in conformità all'articolo 33, paragrafo 5, mediante annotazione nell'apposito registro delle violazioni. Ciò aiuta il Titolare del trattamento a dimostrare l'assunzione di responsabilità all'Autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'Autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il Titolare del trattamento dovrà comunque valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il Titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato che, sebbene una perdita di disponibilità dei sistemi del Titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il medesimo Titolare consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sopra indicati o una combinazione di essi.

La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione o perdita di documenti con dati personali (furto, smarrimento, abbandono, etc.). La casistica è molto ampia.

A mero **titolo esemplificativo** e senza pretesa di esaustività, l'oggetto della segnalazione di un data breach può essere:

- l'accesso abusivo (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- dati cancellati accidentalmente o da soggetti non autorizzati;
- perdita della chiave di decriptazione;
- dati persi dall'ambiente di produzione che non possano essere ripristinati integralmente dalle copie di sicurezza e si debba provvedere manualmente alla loro ricostruzione;
- interruzione significativa di un servizio ("*black out*" elettrico o attacchi di tipo "*denial of service*");
- divulgazione di dati confidenziali a persone non autorizzate;
- errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi;
- divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato;
- pubblicazione erronea delle informazioni personali (non di dominio pubblico) sul portale web istituzionale del Titolare;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- perdita o il furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o il furto di documenti cartacei;
- pirateria informatica;
- virus o altri attacchi al sistema informatico o alla rete dell'Ente;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "*owner*";

- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- formattazione di dispositivi di memorizzazione;
- malfunzionamenti software quali esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.;
- Distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali;
- distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.;
- guasti alla rete aziendale: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

2. Rilevazione della violazione

La prima fase nella gestione del data breach è quella che conduce alla rilevazione della violazione o presunta violazione di sicurezza e della sua comunicazione al Titolare. Nell'ipotesi in cui ci si dovesse accorgere di essere stati vittima di un data breach la prima cosa da fare è quella di **non farsi prendere dal panico ed agire in modo scomposto** ma, anzi, applicare subito le procedure previste dalla presente policy.

2.1. Acquisizione della notizia

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia **affrontata immediatamente e correttamente** al fine di minimizzare l'impatto della violazione e prevenire che si ripeta. Ai fini di una corretta analisi della segnalazione, è necessario raccogliere fatti concreti prima di segnalare qualsiasi tipo di violazione, illecito ed irregolarità in ambito di tutela dei dati personali.

È importante che la raccolta della segnalazione o l'esecuzione della segnalazione da parte degli uffici avvenga **raccogliendo quante più informazioni possibili** (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc..). **Le segnalazioni, pertanto, devono essere fondate su elementi di fatto precisi, circostanziati e concordanti**.

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione dell'incidente al Dirigente o Titolare di P.O., competente in ragione del servizio o settore coinvolto, per una prima valutazione d'impatto, anche con **informazioni incomplete**. Laddove necessario, alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.

2.2. Fonte della notizia

La segnalazione di un data breach può essere **interna** (da personale dipendente, convenzionato, stagisti, tirocinanti, amministratori, DPO, …) o **esterna all'Ente** (Agid, Polizia, altre Forze dell'Ordine, giornalisti, utenti di servizi, RPD, Responsabili del trattamento, interessati, ecc.). Inoltre, ogni **interessato** può segnalare, anche solo in caso di sospetto, che i propri dati personali

siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'interessato può richiedere al Titolare la verifica dell'eventuale violazione.

Il pubblico e, in genere, i soggetti che non sono legati al Titolare del trattamento da rapporti contrattuali od altrimenti vincolanti, possono segnalare anomalie, disservizi o potenziali incidenti sulla sicurezza mediante comunicazione scritta inviata al protocollo. Il Titolare rende disponibili presso i propri uffici e sul **sito web istituzionale**, la **modulistica** e le **informazioni** utili allo scopo. Sebbene la segnalazione possa avvenire in forma libera, si ritiene opportuno suggerire al segnalante l'utilizzo di un apposito modello ALLEGATO A "Modulo di segnalazione di una potenziale violazione di dati personali", predisposto in modo tale da agevolare l'attività istruttoria e valutativa da parte del Titolare.

Nel caso in cui la segnalazione sia raccolta presso persone fisiche, senza l'utilizzo della modulistica e delle procedure di cui sopra, è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul segnalante (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica) che potranno, nel caso, essere utili durante la fase di gestione tecnica, per reperire maggiori informazioni circa la violazione segnalata. Ove possibile è sempre opportuno invitare il segnalante a rendere la propria dichiarazione per iscritto., anche in forma libera. In questa fase è opportuno non raccogliere dati personali appartenenti alle categorie particolari di cui all'art. 9 del GDPR, se non strettamente necessari.

Qualora la segnalazione pervenisse per **posta elettronica** certificata od ordinaria su una casella qualsiasi (istituzionale o meno) non è sufficiente il solo inoltro del messaggio ma occorre, comunque, seguire le modalità di seguito riportate. Allo stesso modo, ove la segnalazione pervenisse su **supporto cartaceo** non è sufficiente la sua mera registrazione al protocollo, occorrendo comunque che si segua la procedura di cui *infra*. Questo per accertarsi che la segnalazione non passi inosservata.

Anche le **segnalazioni anonime e/o verbali** devono essere raccolte e trasmesse conformemente a quanto *infra*, al fine di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

La **segnalazione di una potenziale violazione di dati personali da parte del personale operante all'interno della struttura del Titolare** deve avvenire solamente utilizzando l'apposito modello ALLEGATO A "Modulo di segnalazione di una potenziale violazione di dati personali".

2.3. Il monitoraggio degli eventi di sicurezza con impatto sulla protezione dei dati personali

L'individuazione di potenziali violazioni dei dati personali può anche avvenire a seguito di **attività di monitoraggio** degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea. Il monitoraggio viene effettuato tramite il controllo delle attività di trattamento definite nel Registro dei trattamenti, in particolare per quei trattamenti che sono stati valutati con rischio non trascurabile in fase di valutazione d'impatto. Le attività di monitoraggio si possono suddividere in due tipologie:

A) **Il monitoraggio degli eventi generati dai sistemi ICT**: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dalle infrastrutture di sicurezza perimetrale che assumono carattere di rilevanza ai fini della sicurezza informatica. Tali eventi relativi ai sistemi ICT sono monitorati e gestiti dall'Amministratore di Sistema od altra figura equivalente, incaricata delle attività di gestione operativa della sicurezza ed alla quale siano assegnati i privilegi di accesso in lettura dei file di tracciamento.

B) Il monitoraggio dei luoghi fisici del trattamento e dell'archiviazione di dati personali. I luoghi fisici preposti al trattamento di informazioni personali riconducibili alle categorie di cui agli articoli 9 e 10 del GDPR, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati periodicamente dal personale preposto alla vigilanza, ove previsto, ed anche con l'ausilio di eventuali dispositivi di videosorveglianza. In ogni caso sia il personale di guardiania o di vigilanza, sia il personale operativo, autorizzato all'accesso ai locali o al trattamento dei dati personali, è tenuto a comunicare tempestivamente qualsiasi evento di presunta o palese violazione della privacy come ad esempio:

- smarrimento o furto di documenti cartacei contenenti informazioni personali;
- smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali;
- constatazione di effrazione o tentativi di effrazione alle porte di accesso od alle serrature di chiusura degli armadi che custodiscono documenti;
- presenza di personale non autorizzato nei locali preposti al trattamento di informazioni personali.

Qualunque constatazione di violazione o sospetta violazione, emersa in sede di monitoraggio, deve essere comunicata al Dirigente o Titolare di P.O. responsabile in ragione del servizio o settore coinvolto **entro e non oltre 4 ore** dalla sua verificazione.

2.4. Trasmissione della notizia

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza la medesima è immediatamente **trasmessa al Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto o, in caso di incertezza sulla sua individuazione, assenza o indisponibilità**, **al DPO**, compilando il documento di cui all'ALLEGATO B "Modulo di inoltro di segnalazione di una potenziale violazione di dati personali", senza ritardo e, comunque, entro 4 ore dalla sua ricezione. Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, ..) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Contestualmente alla **trasmissione documentale** della segnalazione è necessario **l'avvertimento** del destinatario anche in modo **verbale** allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Ricevuta la segnalazione, il Dirigente o Titolare di P.O. coinvolto, provvede ad **informarne prontamente e, comunque non oltre 12 ore dalla conoscenza della segnalazione, il DPO a mezzo PEC**, al seguente indirizzo: dpo@pec.gdpr.nelcomune.it

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, anche insieme ai soggetti coinvolti nell'incidente e sotto la supervisione del DPO, coordina la raccolta delle informazioni nel più breve tempo possibile ed **informa prontamente il Sindaco** o suo sostituto o delegato.

Nel caso la violazione coinvolga **più servizi o settori** del Titolare, il coordinamento dei Dirigenti o Titolari di P.O. avviene a cura del Dirigente o Titolare di P.O. competente in ragione del servizio o settore maggiormente coinvolto. In casi di incertezza o contrasto, spetta al DPO individuare la figura del coordinatore. Resta inteso che, l'utilizzo nel presente documento, della terminologia "Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto" sta ad indicare altresì la figura del coordinatore di cui sopra.

Nel caso in cui si tratti di violazione di dati contenuti in un **sistema informatico**, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Area IT o un suo delegato, in caso di assenza e/o l'Amministratore di sistema, ovvero, nei casi di dati gestiti in "cloud" da ditte esterne, il referente della ditta interessata.

3. Analisi e Valutazione della violazione

Questa fase si compone di tutte quelle operazioni, accertamenti e verifiche tese a supportare la valutazione dell'accaduto. Una volta stabilito che un data breach è avvenuto, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, insieme al DPO ed all'Amministratore di sistema od altra figura analoga, dovrà stabilire:

a) se esistono azioni che possano **limitare i danni** che la violazione potrebbe causare;
b) una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
c) se sia necessario **notificare** la violazione all'Autorità di controllo;
d) se sia necessario **comunicare** la violazione agli interessati.

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto e tutti i soggetti coinvolti nella gestione degli incidenti (a mero titolo esemplificativo, Amministratore di sistema od altra figura analoga, Responsabile IT, altri dirigenti o titolari di P.O., …) sono responsabili, sulla base delle rispettive competenze ed in base alla tipologia della violazione, dell'analisi tecnica dell'evento e delle azioni da mettere in atto tempestivamente per il contenimento del danno.

È importante che questa fase, nella sua prima esecuzione, **si concluda nel più breve tempo possibile, massimo 24 ore**, per consentire il primo processo decisionale di valutazione da parte del Titolare e permettergli di eseguire le eventuali notifiche e comunicazioni entro i termini previsti.

Si ricorda che l'art. 33 paragrafo n. 4 del GDPR recita "*Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni relative alla violazione di dati personali e, anche in caso queste non siano per il momento ritenute esaustive, effettuare comunque la notificazione all'Autorità di controllo.

3.1. Analisi tecnica dell'evento

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto (con il supporto dell'Amministratore di sistema od altra figura) effettua, anzitutto, un'analisi tecnica della segnalazione, all'interno della quale, **dovrà essere accertato se la violazione segnalata sia considerabile o meno un data breach**.

Questa fase dev'essere condotta con **estrema celerità**, anche se non si riescono ad individuare tutti gli elementi utili, ad eccezione della determinazione della sussistenza della violazione. Le verifiche potranno eventualmente proseguire anche dopo una prima valutazione. Inoltre l'Autorità di controllo o gli alti organi nazionali (polizia, magistratura, CERT-PA ecc, …) potrebbero richiedere o ritenere necessari approfondimenti. Dunque, l'incompletezza delle informazioni, così come la necessità di approfondimenti potrebbero rendere necessario ripetere la fase anche più volte.

Nessuna segnalazione deve concludersi in questa fase unicamente sulla base di un **giudizio di inaffidabilità del segnalante**: occorrerà comunque appurare se la violazione si è effettivamente verificata. Parimenti, nessuna segnalazione che sia relativa unicamente ad operazioni svolte con strumenti informatici potrà concludersi durante l'analisi tecnica per il solo fatto che non sussiste una violazione di dati personali, in quanto potrebbe in ogni caso rendersi necessario informare altre Autorità competenti (ad es., CERT-PA).

Si dovranno, ove possibile, rilevare:

• la causa e la natura del disservizio o della rottura;
• valutazione delle eventuali vulnerabilità collegate con l'incidente ed individuazione delle azioni di mitigazione delle vulnerabilità individuate;
• l'esistenza di misure adottate precedentemente all'evento per contrastare il rischio;
• valutazione dei tempi e modalità di riparazione e ripristino dei sistemi, dell'infrastruttura e delle configurazioni;
• verifica dei sistemi recuperati;
• l'eventualità di perdita di dati durante il ripristino, la loro tipologia, se i dati sono reperibili in altre aree dei sistemi o presso terzi e le tempistiche per il recupero.

3.2. Valutazione della violazione al fine del rispetto degli obblighi di notifica e comunicazione

Esaurita l'analisi tecnica, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, dovrà svolgere tutte le operazioni necessarie a raccogliere gli elementi per l'ulteriore valutazione dell'evento, ai fini dell'adempimento degli obblighi imposti dal GDPR. Più precisamente il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto (con il supporto dell'Amministratore di sistema od altra figura) dovrà **accertare che i dati oggetto di violazione siano dati personali nonché la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato**. Nello specifico verrà effettuato:

a) il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr. Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 Par. 1. punto 2);
b) l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
c) l'identificazione degli interessati;
d) il contenimento del danno;

Tutte le operazioni effettuate devono essere tracciate e riconducibili a specifiche persone.

3.2.1. valutazione dell'impatto sugli interessati

Nella fase di valutazione, sulla base delle informazioni rinvenute, occorre innanzitutto stabilire se nell'incidente sono coinvolti i **dati personali**. In caso di risposta positiva occorre valutare l'impatto sugli interessati:

a) ove si tratta di una *violazione di riservatezza* occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in uso rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note);
b) in caso di *perdita di integrità o disponibilità* di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

I fattori da considerare nella valutazione del rischio per i diritti e le libertà delle persone fisiche interessate dalla violazione possono così essere esemplificati (trattasi di elencazione non esaustiva né vincolante):

FATTORE	OSSERVAZIONI
Aspetti **generali**	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi. Se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore sarà anche il rischio
Tipo di **violazione**	distruzione, modifica, perdita, divulgazione (ad esempio, una violazione della riservatezza può avere conseguenze diverse rispetto ad una violazione in cui i dati siano stati persi e non più disponibili)
Natura, carattere sensibile e volume dei **dati** personali	Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato a malintenzionati. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate. Inoltre, di norma, una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale. Una violazione che interessi grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.
Facilità di **identificazione** delle persone fisiche	facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali
Gravità delle **conseguenze** per le persone fisiche	danno potenziale alle persone fisiche che potrebbe derivare dalla violazione comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni reputazionali). Il fatto che si sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Si dovrebbe altresì tener conto della permanenza delle

	conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.
Caratteristiche particolari del **Titolare**	La natura e il ruolo del Titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione
Caratteristiche particolari dell'**interessato**	Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili (minori, anziani, pazienti, …), queste ultime potrebbero essere esposte a un rischio maggiore di danni
Numero di persone fisiche interessate	Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.

Qualora il numero degli interessati dalla violazione, o potenziali interessati, sia ridotto e questi siano identificabili è opportuno stilare degli elenchi da utilizzare nel caso in cui il sia necessario inviare loro delle comunicazioni personalizzate.

3.2.2. valutazione della gravità del rischio

La gravità di una violazione di dati personali è definita come la **stima dell'entità del potenziale impatto sulle persone fisiche derivante dalla violazione medesima**. Tale valutazione di impatto permette di stabilire la necessità di notifica della violazione all'Autorità di controllo, in particolare se probabile un rischio per la libertà e diritti delle persone fisiche, e la comunicazione anche agli interessati, nel caso in cui tale rischio sia elevato.

La violazione dei dati può comportare elevati **rischi per i diritti e le libertà delle persone** fisiche. I rischi principali sono connessi alla possibilità che l'interessato subisca danni fisici, materiali o immateriali connessi perdita del controllo dei dati personali quali, ad esempio:

a) limitazione dei diritti;
b) discriminazione;
c) furto o usurpazione di identità;
d) perdite finanziarie;
e) decifratura non autorizzata della pseudonimizzazione;
f) pregiudizio alla reputazione;
g) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);
h) qualsiasi altro danno economico o sociale, significativo.

Le linee guida elaborate dal Gruppo ex art. 29 suggeriscono di ritenere, il rischio elevato per i diritti e le libertà delle persone fisiche, quantomeno come "probabile" quando la violazione riguardi dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza.

I considerando 75 e 76 del GDPR suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la **probabilità** quanto la **gravità** del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva:
- **gravità**: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- **probabilità**: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

le **tabelle** che seguono rappresentano visivamente quanto deve essere oggetto di valutazione

GRAVITÀ	**Impatto della violazione sui diritti e le libertà delle persone coinvolte**
	BASSO: gli individui possono andare incontro a *disagi minori*, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);
	MEDIO: gli individui possono andare incontro a *significativi disagi*, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.);
	ALTO: gli individui possono andare incontro a *conseguenze significative*, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.);
	MOLTO ALTO: gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)
PROBABILITÀ	**Possibilità che si verifichino uno o più eventi temuti**
	BASSA: è improbabile che la minaccia si materializzi
	MEDIA: c'è una ragionevole possibilità che la minaccia si materializzi
	ALTA: la minaccia potrebbe materializzarsi
	MOLTO ALTA: l'evento temuto si è realizzato

PROBABILITA'	GRAVITA'				
		MA	A	M	B
	MA				
	A				
	M				
	B				

Tuttavia va considerato che nel caso di una violazione di dati personali effettiva, l'evento si è già verificato, quindi l'attenzione si concentra **esclusivamente sul rischio** risultante dell'impatto di tale violazione sulle persone fisiche.

	Descrizione	Notifica all'Autorità	Comunicazione agli interessati
Rischio	BASSO: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	MEDIO: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	ALTO e MOLTO ALTO: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Sulla base degli elementi di cui sopra, acquisito un ragionevole grado di certezza del fatto che sia avvenuto un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto:
a) stima la gravità e la probabilità della violazione e classifica il rischio;
b) documenta la decisione presa a seguito della valutazione del rischio nel Registro delle violazioni.
Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati utilizzando il modello ALLEGATO C - "Modulo di valutazione del rischio connesso al violazione di dati personali" e tale documentazione è conservata in apposito archivio.

Scenari al termine della fase valutativa

A) ove i **rischi per gli interessati siano trascurabili**, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. Una eventuale fase di miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

L'art. 33 paragrafo 1 chiarisce, infatti, che **non vi è obbligo di notifica della violazione quando è "*improbabile*" che questa comporti un rischio per i diritti e le libertà delle persone fisiche**: un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un

rischio probabile per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e **il rischio dovrebbe essere rivalutato**.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

B) nel caso che i **rischi per l'interessato non siano trascurabili** occorre procedere alla notificazione all'Autorità di controllo sulla scorta delle indicazioni di cui al successivo paragrafo 4. In questo caso, la procedura deve dare le giuste priorità agli sforzi di contenimento dell'incidente. In ogni caso va condotta una fase di miglioramento.

C) qualora i **rischi per l'interessato siano elevati** occorre procedere alla comunicazione della violazione alle persone fisiche interessate, di cui al successivo paragrafo 6, in aggiunta alla notificazione all'Autorità di controllo, salvo che quest'ultima richieda di omettere o ritardare la comunicazione stessa. In ogni caso va condotta una fase di miglioramento.

3.3. Valutazioni supplementari

Ulteriori analisi dell'accaduto possono rendersi necessarie qualora:

a) il Titolare ritenga necessario un approfondimento finalizzato ad es. all'integrazione di una precedente notifica all'Autorità di controllo;
b) l'Autorità di controllo, gli organi di polizia o la magistratura ritengano necessarie informazioni aggiuntive od approfondimenti di informazioni già fornite;
c) durante una delle fasi del processo di gestione del data breach siano emerse situazioni non approfondibili o non sia stato possibile coinvolgere pienamente responsabili esterni o questi non abbiano comunicato in tempo utile i risultati delle loro analisi.

L'analisi supplementare può essere attivata più volte per la stessa violazione, secondo necessità.

4. Notifica della violazione dei dati personali all'Autorità di controllo

4.1. Quando effettuare la notificazione

La normativa prevede che, **non appena si venga a conoscenza di una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone coinvolte**, sia obbligatorio effettuare la notifica all'Autorità. Pertanto, la notifica all'Autorità dell'avvenuta violazione non è un processo automatico, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Titolare.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, versione emendata e adottata il 6 febbraio 2018, chiariscono quando il Titolare del trattamento possa considerarsi "*a conoscenza*" di una violazione.

Il Gruppo di lavoro europeo ritiene che il Titolare del trattamento debba considerarsi "*a conoscenza*" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che abbia portato alla compromissione dei dati personali. Tuttavia, va considerato che il regolamento impone al Titolare del trattamento di attuare tutte le misure tecniche ed organizzative di protezione adeguate a stabilire immediatamente se si sia verificata una violazione ed informare tempestivamente l'Autorità di controllo e gli interessati. Il Gruppo ex art. 29 afferma inoltre che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato

ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato.

Il Titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva, in modo da poter adottare le misure appropriate.

Il momento esatto in cui il Titolare del trattamento può considerarsi "*a conoscenza*" di una particolare violazione dipenderà dalle circostanze della violazione.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva notificazione all'Autorità di controllo.

Vi sono casi, tuttavia, in cui è possibile definire se l'evento costituisca una violazione ai sensi del GDPR solo al termine della fase di valutazione. In questo caso la decorrenza della tempistica per la notificazione all'Autorità di controllo è, comunque, dal momento della constatazione.

Qualora i contorni della violazione non siano chiari si può attendere fino ad **un massimo di 72 ore** prima di effettuare una notifica (Non si tratta di un termine puramente indicativo ma **categorico**, il cui mancato rispetto se non adeguatamente motivato, integra una situazione sanzionabile). Alla scadenza delle 72 ore è comunque necessario fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Il GDPR consente infatti una notifica per fasi, a condizione che il Titolare indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1.

In ogni caso, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, essa va corredata dei **motivi del ritardo**. Si suggerisce in ogni caso di procedere comunque all'effettuazione della notifica entro il termine, fatto salvo quanto *infra* con riferimento alla notifica per fasi.

Si ricorda che **l'obbligo di effettuare la notifica all'Autorità di controllo, ricorre solo quando:**

a) l'Ente è Titolare del trattamento di dati coinvolti nell'incidente;
b) l'Ente è Contitolare del trattamento con delega alla notifica;
c) l'Ente è Responsabile del trattamento con delega alla notifica. L'Ente non ha il dovere di notificare la violazione all'Autorità di controllo quando agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica. In questo caso l'Ente deve comunicare al Titolare del trattamento la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali, nei modi convenuti, con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

4.2. Come effettuare la notificazione

Per le violazioni identificate, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto redige il **documento di notifica della violazione, compilando l'apposito modello presente sul sito e secondo le istruzioni dell'Autorità di controllo**, **previa consultazione ed in collaborazione con il DPO**. Si allega al presente documento, a mero titolo

esemplificativo, il modello di notificazione approvato dall'Autorità di controllo italiana con provvedimento del 31 luglio 2019, fermo restando che è preciso onere del Dirigente o Titolare di P.O. competente ad effettuare la notifica, verificarne l'attualità, sia in termini di contenuto che di procedura (ALLEGATO D – "Violazione di dati personali – modello di notifica al Garante").

Si può valutare di effettuare una **notifica cumulativa** se una stessa compromissione abbia riguardato la stessa tipologia di dati con le stesse modalità e gli stessi siano stati violati in un lasso di tempo relativamente breve. Ove si verifichino diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale.

Si ricorda che è altresì ammessa una **notificazione "per fasi"** allorquando non si disponga di tutte le informazioni necessarie su una violazione, entro 72 ore dal momento in cui se ne è venuti a conoscenza. In tali casi, all'atto della prima notifica all'Autorità di controllo, il Titolare informa quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo.

4.3. Eventuali ulteriori notificazioni (o denunce)

Effettuata la notifica in favore dell'Autorità di controllo, è poi opportuno verificare se:
1) sia necessaria una *seconda notifica*, più approfondita, quale conseguenza di un'analisi tecnica supplementare ovvero di elementi ed informazioni successivamente acquisiti. È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostrasse che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il Titolare del trattamento può informarne l'Autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'Autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione;
2) sia necessario effettuare una comunicazione alle *forze dell'ordine* od all'*Autorità giudiziaria* competente.

5. Recepimento della eventuale risposta dell'Autorità di controllo

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto dispone con sollecitudine ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dall'Autorità di controllo. Parimenti provvede a seguito del ricevimento di indicazioni od ordini relativamente alla comunicazione da effettuare o non effettuare in favore degli interessati.

6. Comunicazione della violazione dei dati personali all'interessato

Contestualmente alla decisione di notificare all'Autorità di controllo, occorre valutare se sia il caso di informare anche gli interessati. Il modello di notificazione predisposto dall'Autorità di controllo richiede infatti specifica indicazione e descrizione delle circostanze e valutazioni che hanno condotto ad effettuare o non effettuare la comunicazione agli interessati.

A tale scopo va valutata la gravità del rischio per gli interessati ed i loro diritti.

Nel caso di accertamento di una **violazione di dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, come valutato secondo quanto indicato al precedente paragrafo 3, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio (**la soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica all'Autorità di controllo,**

pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica). In tale ipotesi occorre quindi valutare:

a) la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv);
b) le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi;
c) le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo ex art. 29 in materia di trasparenza (WP 260), aggiornate in base alle previsioni del Regolamento (UE) 2016/679.

Anche di questa fase deve essere prodotta e conservata appropriata documentazione.

6.1. Quando effettuare la comunicazione

Il GDPR afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "***senza ingiustificato ritardo***", il che significa il prima possibile. **L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi**. A seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Da notare inoltre che il Considerando 86 suggerisce che "T*ali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge*". Parallelamente, il Considerando 88 indica che la notifica di una violazione dovrebbe tenere "*conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*".

Conseguentemente si ritiene suggeribile, **nel contesto della notifica all'Autorità di controllo, formulare espressa richiesta di indicazioni in tal senso** (non soltanto se provvedere alla comunicazione o no, ma anche quale contenuto della comunicazione e quali canali suggeriti).

6.2. Come effettuare la comunicazione

Per la comunicazione, è possibile identificare **uno o più canali di comunicazione**, a seconda delle circostanze, quali email, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio. Caso per caso, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, dovrà **sempre privilegiare la modalità di comunicazione diretta** con i soggetti interessati (quali e- mail, SMS o messaggi diretti).

Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori.

Non deve essere utilizzato il canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il Titolare del trattamento.

Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Ove non si abbia la possibilità di comunicare una violazione all'interessato perché non si disponga di dati sufficienti per contattarlo, questi sarà informato non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce le informazioni necessarie per essere contattato).

6.3. Quali informazioni comunicare

Sebbene sia preferibile utilizzare il modello ALLEGATO E – "Comunicazione all'interessato della violazione dei dati personali", la comunicazione in altra forma deve comunque contenere, ai sensi dell'art. 34, le seguenti **informazioni**:

1) il nome ed i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
2) una descrizione della natura della violazione;
3) una descrizione delle probabili conseguenze della violazione dei dati personali;
4) una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
5) se l'Autorità di controllo abbia suggerito od ordinato misure di gestione della violazione e sull'attenuazione del suo impatto;
6) eventuali indicazioni al destinatario sul modo in cui proteggersi dalle possibili conseguenze negative della violazione

6.4. Quando non effettuare la comunicazione

Secondo quanto previsto dal paragrafo 3 dell'art. 34 del GDPR, **la comunicazione non è richiesta** se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il Titolare del trattamento ha, successivamente alla violazione, adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o ad una misura simile, ad esempio rendere disponibili le informazioni a richiesta, tramite la quale gli interessati siano informati con analoga efficacia.

Ove si decida di non comunicare una violazione all'interessato, si ricordi che l'articolo 34, paragrafo 4, prevede che l'Autorità di controllo possa richiedere che lo si faccia ugualmente, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato, fatto naturalmente salvo l'esercizio dei poteri e delle sanzioni a propria disposizione.

7. Altre segnalazioni

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto dovrà verificare la necessità di informare altri organi quali, a mero titolo esemplificativo:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);

- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Al Gestore di Identità Digitale e Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

Ciascuna segnalazione dovrà avvenire nel rispetto delle procedure ed utilizzando la modulistica all'uopo eventualmente predisposta da ciascuna Autorità di vigilanza o controllo.

8. Documentazione della violazione

L'art. 33 paragrafo n. 5 del DGPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze ed i provvedimenti adottati al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Si ricorda che la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'Autorità di controllo dei suoi poteri ai sensi dell'articolo 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83.

Il Titolare ha, quindi, stabilito di documentare gli incidenti di sicurezza e le violazioni di dati personali come segue:

a) adozione, di un registro "interno" delle (sole) violazioni di dati personali, intendendosi per tale un inventario aggiornato delle violazioni contenente tutte le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate, le conseguenze che le stesse hanno avuto ed i provvedimenti adottati per porvi rimedio. Esso tiene traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione;
b) adozione di modulistica, anche a rilevanza esterna, idonea a documentare gli incidenti di sicurezza e le violazioni di dati personali.

Il GDPR non specifica un **periodo di conservazione** per tale documentazione. Essa sarà dunque conservata nel rispetto dei termini e delle norme di legge sulla conservazione della documentazione amministrativa, anche in considerazione del fatto che la conservazione è, in conformità dell'articolo 33, paragrafo 5, nella misura in cui il Titolare potrà essere chiamato a fornire prove all'Autorità di controllo in merito al rispetto di tale articolo oppure, più in generale, del principio di responsabilizzazione.

8.1. il Registro delle violazioni

Il DPO è responsabile della tenuta e dell'aggiornamento del Registro delle violazioni.

Poiché il GDPR non specifica quale debba essere il **contenuto** e la **forma** del Registro delle violazioni né il tipo di supporto sul quale debba essere redatto, per estensione delle disposizioni contenute nell'art. n. 30 del GDPR (relativamente al registro delle attività di trattamento e registro delle categorie di attività di trattamento) si presume che tale registro possa anche essere **di tipo elettronico**. Il Titolare ha quindi deciso di adottarlo in tale forma.

L'inventario dovrà essere accompagnato da idonee misure di sicurezza atte a garantire **l'integrità e l'immodificabilità dei dati in esso registrati** quali ad esempio la protocollazione, la stampa, …).

I dati presenti nel registro sono trattati nel rispetto del **principio di minimizzazione** e secondo le misure necessarie per mitigare i rischi di violazione dei dati personali.

Ogni segnalazione, comprese quelle **non veritiere**, deve essere soggetta a registrazione nel registro delle violazioni.

Per ogni violazione di cui sia accertata l'esistenza, anche se non notificata all'Autorità di controllo e non comunicata agli interessati, il registro riporterà:
(con riferimento alla segnalazione)
- numerazione progressiva;
- data ed ora della segnalazione;
- dati identificative del segnalante;
- unità organizzativa coinvolta;
- organi informati;
(con riferimento alla violazione)
- luogo violazione;
- modalità della violazione;
- descrizione dei sistemi, apparati, reti, banche dati oggetto di data breach;
- la natura della violazione dei dati personali;
- altri elementi utili alla descrizione della violazione;
(con riferimento agli interessati)
- indicazione delle categorie di interessati coinvolti;
- indicazione del numero approssimativo di interessati coinvolti;
(con riferimento ai dati personali coinvolti)
- indicazione delle categorie dei dati personali coinvolte;
- indicazione del numero approssimativo di dati personali coinvolti;
(con riferimento alle conseguenze)
- descrizione delle previste (o verificate) conseguenze;
(con riferimento ai rimedi)
- indicazione delle misure adottate per porre rimedio alla violazione;
- indicazione delle misure proposte per porre rimedio alla violazione;
(con riferimento all'attenuazione delle conseguenze)
- indicazione delle misure adottate per attenuare i possibili effetti negativi;
- indicazione delle misure proposte per attenuare i possibili effetti negativi;
(con riferimento ai tempi di ripristino)
- indicazione della tempistica stimata
(con riferimento alla notifica all'Autorità di controllo)
- indicazione se ricorre il rischio per i diritti e le libertà delle persone fisiche;
- effettuazione o meno della notificazione;
- ragioni della omessa notificazione all'Autorità di controllo;
(con riferimento alla comunicazione agli interessati)
- indicazione se ricorre rischio elevato per i diritti e le libertà delle persone fisiche e le relative ragioni;
- effettuazione o meno della comunicazione;
- ragioni della omessa comunicazione agli interessati;

8.2. Altri documenti ed informazioni

Ad integrazione di quanto riportato nel registro, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore competente raccoglie e **conserva tutti i documenti** relativi ad ogni

violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

9. Fase di miglioramento

Una volta contenuti i rischi o le conseguenze della violazione ed adempiuto agli obblighi di notificazione e comunicazione previsti dal GDPR occorre dedicare attenzione alla fase di miglioramento delle misure tecniche ed organizzative in uso presso il Titolare, al fine di evitare il ripetersi di incidenti analoghi.
Le azioni previste in questa fase sono:

- l'analisi della relazione dettagliata sull'incidente;
- la reiterazione del processo di Gestione del rischio informativo;
- l'eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza);
- l'individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- la revisione del sistema di gestione della protezione dei dati;
- la revisione con cadenza almeno annuale della procedura descritta nel presente documento.

10. Fattispecie di contitolarità e responsabilità del trattamento

Sulla scorta della previsione di cui all'articolo 26 del GDPR, laddove il Titolare si trovasse ad operare unitamente ad altri soggetti in fattispecie classificabili in termini di **contitolarità del trattamento** dei dati personali, il relativo accordo o convenzione dovrà contenere espressa determinazione di chi assumerà il comando o sarà responsabile del rispetto degli obblighi di cui agli articoli 33 e 34 del medesimo GDPR.

Sulla scorta della previsione di cui all'articolo 28 del GDPR, laddove il Titolare necessiti che il trattamento di dati personali venga effettuato per suo conto ad opera di altri soggetti qualificabili come **responsabili del trattamento**, il contratto od altro atto giuridico che vincoli tale soggetto al Titolare dovrà contenere espressa previsione che il responsabile assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

In particolare è necessario prevedere che qualora il responsabile del trattamento venga a conoscenza di una violazione di dati personali che sta trattando per conto del Titolare, provveda a notificargliela senza ingiustificato ritardo e, comunque, entro e non oltre 24 ore dalla scoperta, senza effettuare alcuna valutazione circa la probabilità di rischio derivante dalla violazione stessa; spetta infatti soltanto al Titolare effettuare tale valutazione nel momento in cui ne verrà a conoscenza.

FONTI

Nella redazione del presente documento si è tenuto conto delle indicazioni e delle disposizioni:

1) del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - RGDP);
2) del Decreto legislativo 30 giugno 2003, numero 196, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal Decreto legislativo 10 agosto 2018, numero 101;
3) del Gruppo "Articolo 29" all'interno delle Linee-guida in materia di notifica delle violazioni di dati personali, approvate, in via definitiva, il 6 febbraio 2018;
4) del Garante per la protezione dei dati personali nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali";
5) del Garante per la protezione dei dati personali nel Provvedimento 30 luglio 2019 "sulla notifica delle violazioni dei dati personali" (doc. web n. 9126951);

Il presente documento è soggetto a integrazioni e modifiche alla luce dell'evoluzione normativa italiana e comunitaria, della riflessione che si svilupperà a livello nazionale ed europeo, nonché delle prassi che saranno, di volta in volta, riscontrate all'interno della struttura del Titolare.

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 27 aprile 2016
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
(regolamento generale sulla protezione dei dati)

Considerando (75)

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Considerando (76)

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Considerando (85)

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. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Considerando (86)

Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

Considerando (87)

È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

Considerando (88)

Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Articolo 4 - definizioni

Ai fini del presente regolamento s'intende per: (…)
12) «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

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

MANUALE DI GESTIONE
DEI FLUSSI DOCUMENTALI

Allegato n. 8

Manuale di conservazione
(schema)

1. Scopo del documento

Il presente Manuale della Conservazione è un documento interno della Provincia di Novara che descrive le responsabilità e l'organizzazione logica e fisica del sistema di conservazione dei documenti digitali in particolare i soggetti che nel tempo ne hanno assunto la responsabilità, i processi attuati nell'ambito della conservazione, gli oggetti e le tipologie documentarie da destinare a conservazione.

Quanto descritto nel Manuale rappresenta la struttura complessiva del processo di conservazione attivato dall'Ente in relazione al modello organizzativo, secondo quanto specificato nei paragrafi successivi.

La Provincia di Novara ha stabilito di realizzare i processi di conservazione digitale secondo il modello "in outsourcing", il quale prevede che il servizio di conservazione venga affidato dal Produttore ad uno o più Conservatori esterni, ossia a soggetti pubblici o privati accreditati ai sensi dell'art. 29 del D.Lgs. 82/2005 - Codice dell'amministrazione digitale.

Per il dettaglio delle tipologie documentarie degli oggetti sottoposti a conservazione l'Ente fa riferimento a quanto concordato e sottoscritto con i Conservatori accreditati, in forma di disciplinare tecnico.

2. Definizioni

Al fine di rendere esplicite le terminologie impiegate all'interno di questo manuale, si fa riferimento al glossario riportato nell'allegato 1 del D.P.C.M. 13 dicembre 2013 sulla conservazione.

accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico

autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
coordinatore della gestione documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del D.P.R. 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di *backup* degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
fascicolo informatico	aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice

formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione

pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche previste dalla normativa e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano della sicurezza del sistema di gestione informatica dei documenti	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici

	di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate al punto 4.5 delle Linee guida AGID del maggio 2021
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del CAD, richiamato al capitolo 4 delle linee guida AGID del maggio 2021
sistema di gestione informatica dei documenti	nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
staticità	caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal software utilizzato per la redazione
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
testo unico	decreto del Presidente della Repubblica 28 dicembre 2000, n.445, e successive modificazioni
ufficio utente	riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

3. Sistema di conservazione e tipologie documentarie

Il sistema di conservazione della Provincia di Novara prevede, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- i documenti informatici e i documenti amministrativi informatici prodotti e acquisiti dall'Ente, con i metadati ad essi associati e descritti nella documentazione sottoscritta tra Ente e Conservatore;
- i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati e descritti nella documentazione sottoscritta tra Ente e Conservatore, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Essi sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

- **pacchetti di versamento;**
- **pacchetti di archiviazione;**
- **pacchetti di distribuzione.**

Le tipologie documentali oggetto di conservazione sono individuate dal Responsabile della Gestione Documentale e dal Responsabile della Conservazione.
Per ogni tipologia documentale sono definite le caratteristiche necessarie e qualificanti all'identificazione e al trattamento dei singoli documenti durante il loro intero ciclo di vita.

4. Struttura organizzativa dell'Ente per i processi di conservazione

L'iter procedurale del processo di conservazione viene descritto nel presente capitolo e nei successivi in forma schematica, individuando i ruoli coinvolti, le competenze e le responsabilità necessarie a garantirne il regolare svolgimento.
I ruoli previsti nel processo di conservazione sono i seguenti:

Ruolo	Descrizione
Produttore	E' la persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Tale figura si identifica con il Responsabile della Gestione Documentale.
Responsabile della Gestione Documentale	È il soggetto responsabile del servizio della gestione dei flussi documentali, per la tenuta del protocollo informatico e degli archivi (art. 61 D.P.R. 28 Dicembre 2000 n. 445). È anche responsabile della produzione del pacchetto di versamento (art. 6 comma 3 - D.P.C.M. 3 Dicembre 2013 sulla conservazione).
Responsabile della Conservazione	Il Responsabile della Conservazione è il soggetto cui fa capo la responsabilità di verifica del corretto svolgimento del processo di conservazione.
Utente	Ai sensi dell'art. 6 delle regole tecniche sulla conservazione, è la persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

5. Responsabile della Conservazione

Il Responsabile della Conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il Responsabile della Conservazione:

- 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;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, qualora previsto;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- 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;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il Responsabile della Conservazione può delegare in tutto o in parte lo svolgimento del processo di conservazione ad uno o più soggetti esterni. La delega è formalizzata esplicitando chiaramente il contenuto della stessa ed in particolare le specifiche funzioni e competenze affidate al delegato. La delega prevede per il soggetto esterno anche la nomina del responsabile del trattamento dei dati personali ai sensi della normativa vigente.

6. Il sistema di conservazione

Il sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Produttore, fino all'eventuale scarto indipendentemente dall'evolversi del contesto tecnologico e organizzativo. La Provincia di Novara intende avvalersi di conservatori accreditati esterni per la conservazione delle tipologie documentarie descritte nell'allegato 1.

7. Il processo di preparazione dei pacchetti di versamento (PdV)

La produzione dei pacchetti di versamento riguardanti le singole tipologie documentali viene effettuata con l'ausilio dei corrispondenti applicativi gestionali in uso presso l'Ente.

Il Produttore e il Responsabile della Conservazione definiscono le modalità di trasmissione dei documenti ai sistemi di conservazione dei conservatori affidatari.

I conservatori svolgono le funzioni di archiviazione e conservazione digitale, nella logica di sviluppo integrato della conservazione digitale dei documenti informatici nel rispetto dei principi di efficacia, efficienza ed economicità.

Gli affidamenti del servizio di conservazione per le singole tipologie documentali vengono gestiti periodicamente con appositi provvedimenti sotto la supervisione del Responsabile del Servizio di Conservazione.

8. Il processo di conservazione

I documenti informatici trattati dall'Ente devono, secondo necessità, essere memorizzati in un sistema di gestione informatica dei documenti idoneo a garantire le caratteristiche di immodificabilità e integrità degli stessi.

L'iter procedurale del processo di conservazione viene di seguito descritto in forma schematica, individuando i ruoli coinvolti, le competenze, le responsabilità necessarie a garantirne il regolare svolgimento.

Si rimanda agli allegati per i dettagli organizzativi e tecnologici relativi ai processi di conservazione specifici per le varie categorie documentali.

9. Procedure di monitoraggio e verifica dei sistemi informativi interni all'Ente

La Provincia di Novara, nell'ambito della conservazione, gestisce e regolamenta come segue gli aspetti inerenti alla sicurezza dei sistemi informativi dell'Ente, all'interno dei quali vengono prodotti e gestiti i documenti informatici.

I documenti appartenenti alle tipologie documentali Registro giornaliero di protocollo, Atti amministrativi, Flussi OPI, Fatture elettroniche e Ricevute telematiche degli avvisi di PagoPA vengono gestiti con applicativi gestionali in cloud qualificati Agid/ACN che garantiscono le necessarie misure di sicurezza.

Il monitoraggio dei processi di conservazione viene effettuato secondo le modalità previste dai conservatori affidatari sia tramite interrogazione diretta del sistema di conservazione sia attraverso la ricezione di report periodici.

10. Misure di Sicurezza

La Provincia di Novara verifica che il conservatore scelto sia tra i soggetti accreditati da AGID, secondo le specifiche norme e circolari di riferimento (all'art. 44-bis del D.Lgs. 7 Marzo 2005 n. 82, D.P.C.M. 3 Dicembre 2013, Circolare AGID n. 65 10 Aprile 2014, Circolare AGID Maggio 2021), e che possieda quindi i requisiti previsti per la conservazione dei documenti informatici.

Seguono allegati

ALLEGATO 1

Elenco delle tipologie documentarie sottoposte a conservazione (Fase di attuazione operativa)

Tipologia documentale	Conservatore	Periodicità di invio in conservazione	Note
Registro giornaliero di protocollo	INFOCERT (Fino al 31.12.2023) poi ParER/Regione Emilia Romagna	giornaliera	
Fattura elettronica	• INFOCERT fino al 31.12.2023 • poi ParER/Regione Emilia Romagna (a seguito di protocollazione) • Dal 2026 attraverso il produttore del software di gestione dell'iter delle fatture (Maggioli)	Mediamente mensile Dal 2026: • versamento dopo 15 giorni dal fine iter di formazione ed eventuale notifica ed entro	

		un anno dalla chiusura della serie a cui appartengono • conservazione entro 15 giorni dal versamento	
Contratti	ParER/Regione Emilia Romagna		
Atto amministrativo	ParER/Regione Emilia Romagna	Mediamente mensile	Delibere Consiglio Delibere Assemblea Sindaci Decreti del Presidente Atti dirigenziali
Ordinativo di pagamento e incasso (Mandati di pagamento e Reversali d'incasso-c.d. flussi OPI)	Fornitore del software di contabilità (attualmente Maggioli)	mensile	
Pec	ParER/Regione Emilia Romagna		
Ricevute telematiche degli Avvisi di PagoPA	Top Consult	mensile	Servizio Conserva RT attraverso Plug&Pay di E-Fil S.r.l.

ALLEGATO 2
Fascicolo informatico o aggregazione documentale informatica, informazioni minime (da implementare)

Informazione	Definizione
Identificativo	Identificativo univoco e persistente è una sequenza di caratteri alfanumerici associata in modo univoco e permanente al fascicolo o aggregazione documentale informatica in modo da consentire l'identificazione
Amministrazione Titolare	Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo
Amministrazioni partecipanti	Amministrazioni che partecipano all'iter del procedimento
Responsabile del procedimento	Responsabile del procedimento
Oggetto	Metadato funzionale a riassumere brevemente il contenuto del documento o comunque a chiarirne la natura
Documento	Elenco degli identificativi dei documenti contenuti nel fascicolo che ne consentono la reperibilità

ALLEGATO 3
Responsabile della Conservazione interno all'Ente

Soggetto	Qualifica	Estremi atto di nomina
Ing. Alberto Ravarelli	Dirigente	Decreto 236 del 29.12.2022