Comune di Milano

Comune di Milano

Manuale di conservazione digitale

APPROVATO CON DELIBERAZIONE DELLA GIUNTA COMUNALE N° 909 DEL 24/07/2025

Indice

Capitolo 1
Disposizioni introduttive

1.1 Introduzione – 1.2 Scopo e ambito di applicazione – 1.3 Definizioni e norme di riferimento – 1.4 Forme di pubblicità legale e divulgazione

1.1 Introduzione

Il presente Manuale di conservazione digitale è stato redatto in attuazione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (in seguito Linee Guida) adottate dall'AgID in attuazione della delega prevista dall'art. 71 del D. Lgs 82/2005 (Codice dell'Amministrazione Digitale).

Tale Manuale si inserisce nei processi descritti dal Manuale di Gestione Documentale dell'Ente (Manuale GED).

1.2 Scopo e ambito di applicazione

Con il presente manuale si intende descrivere il sistema di conservazione dei documenti digitali del Comune di Milano.

In particolare, il Comune di Milano, in attuazione del CAD e delle Linee Guida AgID, è tenuto a dotarsi di un sistema di conservazione digitale al quale trasferire documenti e aggregazioni informatiche (anche relativi a procedimenti ancora non conclusi quando opportuno), nonché i relativi metadati.

1.3 Definizione e norme di riferimento

Per le definizioni e gli acronimi utilizzati all'interno del presente documento si fa riferimento al Glossario allegato al Manuale GED.

I principali riferimenti normativi presi in considerazione per la redazione del presente Manuale sono riportati nell'allegato Riferimenti normativi al Manuale GED.

Per le definizioni non riportate nel Glossario citato si deve fare riferimento alle definizioni previste negli atti normativi richiamati nell'allegato "Rifermenti normativi al Manuale GED".

1.4 Forme di pubblicità legale e divulgazione

Il Manuale di conservazione è reso pubblico mediante la diffusione sul sito web istituzionale nella sezione "Amministrazione Trasparente", come previsto dalle Linee Guida, quale allegato del Manuale GED.

La diffusione all'interno dell'Amministrazione Comunale segue le regole dettate per il Manuale GED.

Capitolo 2
Aspetti organizzativi

2.1 Modello organizzativo adottato – 2.2 Ruoli e responsabilità – 2.3 Struttura organizzativa

2.1 Modello organizzativo adottato

Alla data di approvazione del Manuale GED il Comune di Milano ha affidato a un soggetto esterno il sistema di conservazione digitale, di seguito indicato come Conservatore.

Nell'Allegato A al presente manuale (Conservatori) sono indicati in formato tabellare i conservatori di cui si è avvalso/si avvale l'Ente.

2.2 Ruoli e responsabilità

I ruoli individuati nelle Linee Guida AgID sono quelli riportati nella seguente tabella

Ruolo	Soggetto che ricopre il ruolo
Titolare dell'oggetto della conservazione	Comune di Milano organizzato con un'unica AOO
Produttore dei PdV*	Il soggetto individuato dall'Ente quale Responsabile della Gestione Documentale ai sensi del paragrafo 4.4. delle Linee Guida AgID
Utente abilitato	Sono utenti abilitati il Responsabile della Gestione Documentale e il suo Vicario, il Responsabile della Conservazione, il Responsabile della Transizione, il DPO, il Produttore dei PdV* e i Referenti Documentali descritti nel manuale GED. Sono, altresì, utenti abilitati i soggetti individuati dal Responsabile della Conservazione sino alla loro revoca.
Responsabile della Conservazione	Il soggetto nominato dal sindaco.
Conservatore	I soggetti individuati nell'allegato A al presente Manuale.

*Pacchetti di Versamento

Il Responsabile della Conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività, o parte di esse a uno o più soggetti interni alla struttura organizzativa o al Responsabile del Servizio di Conservazione del Conservatore. Tali deleghe sono riportate nell'allegato B del presente Manuale.

2.3 Struttura organizzativa

L'Ente produce i propri documenti e le aggregazioni documentali secondo il Manuale GED.

Il Responsabile della Gestione Documentale e Conservazione svolge i compiti affidati dalla normativa vigente, in particolare in ambito archivistico, delegando ai responsabili dei servizi IT gli aspetti tecnici.

Il sistema di conservazione è affidato a soggetti esterni nel rispetto delle normative vigenti e delle indicazioni di AgID.

Capitolo 3
Oggetti conservati e processo di conservazione

3.1 Oggetti conservati – 3.2 Processo di conservazione: rinvio al manuale del conservatore

3.1 Oggetti conservati

3.1.1 Registro giornaliero di protocollo

Il versamento riguarda elenco di tutti i protocolli del giorno esportati in un pdf inviato entro le 24 ore successive.

TIPO DOCUMENTO	DESCRIZIONE	DATA DI PRIMO VERSAMENTO	SISTEMA VERSANTE	PERIODICITÀ
REGISTRI DI PROTOCOLLO	Registri di giornalieri di protocollo	22/06/2017	EGRAMMATA (Engineering) - AURIGA	Giornaliera

Elenco metadati

DENOMINAZIONE	DESCRIZIONE
NumeroIniziale	OBBLIGATORIO. Numero della prima registrazione sul registro giornaliero
NumeroFinale	Numero dell'ultima registrazione sul registro giornaliero
DataInizioRegistrazioni	OBBLIGATORIO. Data della prima registrazione del registro giornaliero
DataFineRegistrazioni	OBBLIGATORIO. Data dell'ultima registrazione del registro giornaliero
Originatore	OBBLIGATORIO. Unità o settore responsabile della produzione del registro giornaliero
Responsabile	OBBLIGATORIO. Nome e cognome del Responsabile della tenuta del protocollo informatico
Operatore	Nome e cognome dell'operatore che ha creato il registro giornaliero
NumeroDocumentiRegistrati	Numero complessivo dei documenti registrati
NumeroDocumentiAnnullati	Numero complessivo dei documenti annullati

DenominazioneApplicativo	Denominazione commerciale dell'applicativo che produce il registro giornali ero
VersioneApplicativo	Versione dell'applicativo che produce il registro giornaliero
ProduttoreApplicativo	Denominazione del produttore dell'applicativo che produce il registro giornaliero
DenominazioneSistemaGestioneBase Dati	Denominazione del sistema di gestione della base di dati
VersioneSistemaGestioneBaseDati	Versione del sistema di gestione della base di dati
ProduttoreSistemaGestioneBaseDati	Denominazione del produttore del sistema di gestione della base di dati
DenominazioneSistemaOperativo	Denominazione del sistema operativo utilizzato
VersioneSistemaOperativo	Versione del sistema operativo utilizzato
ProduttoreSistemaOperativo	Denominazione del produttore del sistema operativo utilizzato
TempoConservazione	OBBLIGATORIO. Tempo di conservazione del registro: ILLIMITATO

3.1.2 Fatture attive

Il versamento riguarda elenco delle fatture attive emesse dall'Ente.

TIPO DOCUMENTO	DESCRIZIONE	DATA DI PRIMO VERSAMENTO	SISTEMA VERSANTE	PERIODICITÀ
FATTURA ATTIVA	Fattura attiva	13/04/2023	EGRAMMATA (Engineering) - AURIGA	Annuale tramite caricamento massivo

Tabella - Tipo struttura FATTURA ATTIVA_Dettaglio tipi documento

TIPO DOCUMENTO	ELEMENTO	OBBLIGATORIO	PERIODICITÀ DI VERSAMENTO	NOTE
FATTURA	PRINCIPALE	Si		
ACCONTO/ANTICIPO SU FATTURA	PRINCIPALE	Si		
GENERICO	ALLEGATO	No		
NOTA DI CREDITO	PRINCIPALE	Si		

NOTA DI DEBITO	PRINCIPALE	Si		
NOTIFICA DI SCARTO	ANNESSO	No		
NOTIFICA DI MANCATA CONSEGNA	ANNESSO	No		

Elenco Metadati

DENOMINAZIONE	DESCRIZIONE
CodiceRegistroSistemaContabile	CodiceRegistroSistemaContabile
NumeroRegistroSistemaContabile	NumeroRegistroSistemaContabile
DataRegistrazioneSistemaContabile	DataRegistrazioneSistemaContabile
DenominazioneDestinatario	DenominazioneDestinatario
TipoDenominazioneDestinatario	TipoDenominazioneDestinatario
IdentificativoDestinatario	IdentificativoDestinatario
TipoIdentificativoDestinatario	TipoIdentificativoDestinatario
ImportoTotale	ImportoTotale
ScadenzaFattura	ScadenzaFattura

3.1.3 Fatture passive

Il versamento riguarda elenco delle fatture passive ricevute dall'Ente.

TIPO DOCUMENTO	DESCRIZIONE	DATA DI PRIMO VERSAMENTO	SISTEMA VERSANTE	PERIODICITÀ
FATTURA PASSIVA	Fattura passiva	03/05/2017	EGRAMMATA (Engineering) - AURIGA	Annuale tramite caricamento massivo

Tabella - Tipo struttura FATTURA PASSIVA_Dettaglio tipi documento

TIPO DOCUMENTO	ELEMENTO	OBBLIGATORIO	PERIODICITÀ DI VERSAMENTO	NOTE
FATTURA	PRINCIPALE	Si		
ACCONTO/ANTICIPO SU FATTURA	PRINCIPALE	Si		

GENERICO	ALLEGATO	No		
NOTA DI CREDITO	PRINCIPALE	Si		
NOTA DI DEBITO	PRINCIPALE	Si		
SCARTO ESITO COMMITTENTE	ANNESSO	No		
NOTIFICA DI ESITO COMMITTENTE	ANNESSO	No		

Elenco Metadati

DENOMINAZIONE	DESCRIZIONE
NumeroProtocollo	NumeroProtocollo
DataProtocollo	DataProtocollo
NumeroRUF	NumeroRUF
DataRegistrazioneRUF	DataRegistrazioneRUF
CodiceRegistroIVA	CodiceRegistroIVA
NumeroRegistroIVA	NumeroRegistroIVA
DataRegistrazioneIVA	DataRegistrazioneIVA
NumeroEmissione	NumeroEmissione
DataEmissione	DataEmissione
DenominazioneMittente	DenominazioneMittente
TipoDenominazioneMittente	TipoDenominazioneMittente
IdentificativoMittente	IdentificativoMittente
TipoIdentificativoMittente	TipoIdentificativoMittente
OggettoFornitura	OggettoFornitura
ImportoTotale	ImportoTotale
Scadenza	Scadenza
RiferimentoContabile	RiferimentoContabile
TipoRifContabile	TipoRifContabile
RilevanzaIVA	RilevanzaIVA
CIG	CIG

3.1.4 Determinazioni Dirigenziali

Il versamento riguarda elenco delle fatture passive ricevute dall'Ente.

TIPO DOCUMENTO	DESCRIZIONE	DATA DI PRIMO VERSAMENTO	SISTEMA VERSANTE	PERIODICITÀ
DETERMINA	Fattura passiva	16/01/2020	EGRAMMATA (Engineering) - AURIGA	Dopo 90 giorni data chiusura atto, adozione ed esecutività

Tabella - Tipo struttura DETERMINA_Dettaglio tipi documento

TIPO DOCUMENTO	ELEMENTO	OBBLIGATORIO	PERIODICITÀ DI VERSAMENTO	NOTE
DETERMINA	PRINCIPALE	Si		
GENERICO	ALLEGATO	No		
RELATA DI PUBBLICAZIONE	ANNESSO	No		
VISTO REGOLARITA CONTABILE	ANNESSO	No		

Elenco Metadati

DENOMINAZIONE	DESCRIZIONE
PropostaIdentificativo	PropostaIdentificativo
PropostaData	PropostaData
StrutturaProponente	StrutturaProponente
Firmatario	Firmatario
RuoloFirmatario	RuoloFirmatario
VistoRegolaritaContabile	VistoRegolaritaContabile
VistoContabileResponsabile	VistoContabileResponsabile
VistoContabileData	VistoContabileData
VistoContabileEspresso	VistoContabileEspresso
VistoContabileNote	VistoContabileNote
CIG	CIG
ImpegnoSpesa	ImpegnoSpesa
EsecutivitaData	EsecutivitaData
Pubblicato	Pubblicato

Articolo	Articolo
ResponsabileTrasparenza	ResponsabileTrasparenza
FunzionarioPubblicazione	FunzionarioPubblicazione
PubblicazioneRegistro	PubblicazioneRegistro
PubblicazioneAnno	PubblicazioneAnno
PubblicazioneNumero	PubblicazioneNumero
PubblicazioneInizio	PubblicazioneInizio
PubblicazioneFine	PubblicazioneFine
IncaricatoPubblicazione	IncaricatoPubblicazione
ResponsabilePubblicazione	ResponsabilePubblicazione
Ripubblicazione	Ripubblicazione
Note	Note
AltraRegistrazioneRegistro	AltraRegistrazioneRegistro
AltraRegistrazioneAnno	AltraRegistrazioneAnno
AltraRegistrazioneNumero	AltraRegistrazioneNumero
AltraRegistrazioneData	AltraRegistrazioneData

3.1.5 Posta Elettronica Certificata (PEC)

Secondo il Codice Civile (art.2200 e 2214), **la corrispondenza rilevante deve essere conservata per 10 anni**,

TIPO DOCUMENTO	DESCRIZIONE	DATA DI PRIMO VERSAMENTO	SISTEMA VERSANTE	PERIODICITÀ
PEC	Posta elettronica certificata	24/01/2022	LegalDoc (TINEXTA INFOCERT)	Continua

3.2 Processo di conservazione: rinvio al manuale del conservatore

Si fa espresso rinvio al manuale di conservazione del Conservatore per quanto attiene:

- alla descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- alla descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- alla modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- alla descrizione delle procedure per la produzione di duplicati e il rilascio di copie;
- alle modalità con cui viene richiesta la presenza di un pubblico ufficiale.

Capitolo 4
Sistema di conservazione, monitoraggio, controlli e misure di sicurezza

4.1 Rinvio al manuale del conservatore – 4.2 Piano della sicurezza del sistema di gestione documentale

4.1 Rinvio al manuale del conservatore

Si fa espresso rinvio al manuale di conservazione del Conservatore per quanto attiene:

- alla descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- alla descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie.

4.2 Piano della sicurezza del sistema di gestione documentale

Il sistema di protocollo informatico del Comune di Milano è integrato nel sistema di gestione informatica dei documenti ed assicura il rispetto delle disposizioni in materia di sicurezza predisposte da AgID e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali. Pertanto, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017.

Le modalità di accesso al sistema documentale sono disciplinate dalla Politica degli Accessi Logici approvata dalla Direzione Innovazione Tecnologica e Digitale 28 dicembre 2023 (allegato C).

La procedura da adottare in caso di data breach è disciplinata da apposita procedura approvata dall'Ente (allegato D).

Capitolo 5
Approvazione e modifiche al manuale

5.1 Approvazione del manuale – 5.2 Modifiche tecniche – 5.3 Ulteriori modifiche

5.1 Approvazione del manuale

Il manuale, e in sede di prima applicazione tutti i suoi allegati, viene approvato dalla Giunta Comunale su proposta di concerto del Responsabile della Gestione della Conservazione.

5.2 Modifiche tecniche

Gli allegati vengono aggiornati automaticamente in caso di approvazione di nuovi conservatori, rilascio di nuove deleghe, modifica delle procedure relative agli accessi logici e data breach.

5.3 Ulteriori modifiche

Ulteriori modifiche, oltre a quelle tecniche, sono approvate con le medesime modalità di approvazione del manuale.

Allegato A – Conservatori

Denominazione	Sede e codice fiscale	Nominato il	Revocato il	Estremi dell'atto di nomina, del contratto/accordo di servizio e di eventuali altri documenti integrativi
Regione Emilia-Romagna - ParER	Direzione Generale Risorse, Europa, Innovazione e Istituzioni Area Polo Archivistico e gestione documentale - Viale Aldo Moro 52, 40127 - Bologna - C.F. 80062590379	15 settembre 2024		DD 7993 del 15/09/2024
C.M. Trading S.r.l.	Via dei Prati Fiscali n° 201 - 00141 - Roma e c.f./p.i. 04077341008	05 Marzo 2025		DD n. 1544 del 05.03.2025
TINEXTA infocert	Tinexta Infocert S.p.A. Società Soggetta alla Direzione e al Coordinamento di Tinexta S.p.A. P.IVA 07945211006 - Sede legale: Piazzale Flaminio 1/B, 00196 - Roma	24 gennaio 2022		DD 11244 del 10/12/2021 DD 10493 del 22/11/2022 DD 658 del 5/2/2025

Allegato B – Deleghe

ATTIVITA' DELEGATE DEL RESPONSABILE DELLA CONSERVAZIONE

Soggetto delegato	Sede e codice fiscale	Funzioni e competenze delegate	Delegato il	Revocato il	Estremi dell'atto di delega
C.M. Trading S.r.l.	Via dei Prati Fiscali n° 201 - 00141 - Roma e c.f./p.i. 04077341008	Funzioni di cui al paragrafo 4.5 comma 6, lettere b, c, d, e, f, g, h, i, j e k delle Linee Guida Agid per la formazione, gestione e conservazione dei documenti informatici	05 marzo 2025		DD n. 1544 del 05.03.2025

Comune di Milano	**Allegato C - Politica degli accessi logici**		
PD-POL	Data	Versione	Stato
Protezione Dati Policy	**28/12/2023**	**1.0**	**Finale**

Versione del Documento

	Approvatori
Prima emissione	• *Direzione Innovazione Tecnologica e Digitale*

Indice dei contenuti

1 Introduzione

La presente policy nasce dalla necessità di garantire che la gestione degli accessi alle risorse informatiche di proprietà del Comune di Milano (di seguito il Comune), avvenga in modo tale che la riservatezza, l'integrità e la disponibilità dei dati sia garantita, evitando accessi non autorizzati, usi impropri e ogni altra possibile sorgente di rischio per il Comune, per i dati che tratta e per i servizi che eroga ai cittadini.

Lo scopo principale di tale policy è, pertanto, quello di prescrivere i comportamenti corretti da adottare nel contesto del controllo accessi, che i dipendenti e le terze parti dovranno attuare per non incorrere in condotte che, anche solo per negligenza o imprudenza, non risultino conformi alla normativa di settore o che siano fonte di danno effettivo o potenziale per il corretto svolgimento delle attività lavorative.

Quello del controllo accessi è un tema di rilevanza centrale per il Comune, soprattutto in un'ottica di conformità al Regolamento Europeo N. 2016/679 sulla Protezione dei Dati Personali (d'ora in avanti "il Regolamento") ed alla direttiva NIS2. In tale contesto, il Comune di Milano ritiene di cruciale importanza mettere in atto i tre processi di seguito descritti, aventi come focus principale i concetti di **identità digitale** e di **credenziale di autenticazione**.

- **Processo di identificazione**: risponde alla domanda "Chi sei tu?". L'utente che vuole accedere ad un sistema sia esso un computer, un server, un'applicazione, etc., deve "rispondere" a questa domanda per stabilire la propria identità. Nella maggior parte dei casi la risposta è il login, username, user-id o la chiave pubblica. Questa informazione può anche essere pubblica, non coperta cioè da nessun vincolo di segretezza.

- **Processo di autenticazione**: una volta stabilità l'identità di una persona, il sistema deve essere sicuro che l'utente sia quello che dice di essere. Per questo motivo, il sistema chiede "Come puoi dimostrare la tua identità?". In questi casi, la risposta è la credenziale di autenticazione (password) legata allo username con cui ci si è identificati, oppure il codice PIN, ma anche la chiave privata, la propria impronta digitale, l'iride dell'occhio. Questa informazione deve essere assolutamente tenuta segreta e conservata con la massima accuratezza.

- **Processo di autorizzazione**: una volta che il sistema ha acconsentito all'accesso, è necessario stabilire "cosa puoi fare?", ossia a quali risorse, a quali dati puoi accedere? Il tutto viene garantito con un controllo degli accessi in base alle autorizzazioni precedentemente date al profilo dell'utente. Il sistema è pertanto in grado di stabilire quali operazioni consentire e quali vietare all'utente (profilo autorizzativo).

Nel corso dei capitoli successivi i tre processi sopra indicati verranno declinati secondo un livello di maggior dettaglio.

2 Obiettivo

La presente Policy ha lo scopo di:

- Identificare i criteri per gestire e controllare gli accessi ai sistemi informativi del Comune. In tale contesto il Comune ha definito un modello di *access management*, strutturato come segue:

- **Utenza**: insieme di attributi che identificano e definiscono una persona - l'utente (ad esempio: il suo nome, il codice fiscale, il ruolo e le mansioni, etc.).
- **Identità Digitale**: associata all'utenza creata ed intesa come l'insieme delle informazioni e delle risorse concesse ad un utente utilizzatore di un sistema informatico attuando uno specifico processo di identificazione.
- **Profilo Autorizzativo**, categorizzato secondo le differenti tipologie di accesso (utente amministratore, utente standard, etc.).

- Individuare i criteri per la creazione, distribuzione, modifica, protezione, conservazione, recupero, validità e utilizzo delle credenziali di autenticazione con la relativa assunzione di responsabilità, nell'ambito di applicazione del documento.

L'applicazione dei criteri sopra indicati ha l'obiettivo di minimizzare il rischio di accessi non autorizzati ai sistemi e ai dati in essi custoditi (perdita di riservatezza), di alterazione e modifica dei dati che si stanno scambiando (perdita di integrità) e la possibilità che tali dati non siano fruibili da parte di chi ha necessità di accedervi (perdita di disponibilità).

3 Destinatari delle politiche

I principi contenuti nella presente policy si applicano a tutti i sistemi informativi, database e applicazioni di cui il Comune di Milano è direttamente responsabile[1] e che, a partire dalla definizione dell'identità dell'utente (identificazione), permettono o necessitano di un riconoscimento dello stesso (autenticazione) e assegnano all'utente dei parametri di configurazione (autorizzazione) per il loro utilizzo.

Destinatari della presente policy sono tutte le persone facenti parte dell'intera realtà organizzativa del Comune di Milano (incluse le terze parti) che, nell'espletamento delle proprie mansioni e/o in virtù di specifici accordi, accedono o gestiscono i sistemi informativi di responsabilità del Comune di Milano.

4 Normativa di riferimento

[1.]	*D.lgs. n. 196/2003, come modificato dal D.lgs. n. 101/2018*
[2.]	*Regolamento Europeo N. 2016/679 Sulla Protezione Dei Dati Personali*
[3.]	*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni – AGID*
[4.]	*Deliberazione Della Giunta Comunale N. _914_ del 25/05/2018 - Applicazione Del Regolamento Europeo N. 2016/679 Sulla Protezione Dei Dati Personali*
[5.]	*Policy "Amministratori di Sistema"*
[6.]	*Provvedimento del Garante Privacy "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008 modificato dal Provvedimento del 25 giugno 2009*
[7.]	*EA - Linee guida Identità e autenticazione Backoffice - ver. 1.3*
[8.]	*Direttiva (UE) 2022/2555 NIS2*

[1] La responsabilità si applica sia a tutti quei sistemi di cui il Comune di Milano è proprietario, che siano installati sulle proprie infrastrutture o presso le infrastrutture di terzi, sia ai sistemi di terzi installati sulle infrastrutture del Comune di Milano.

5 Definizioni

Termine o acronimo	Definizione
Amministratore di sistema	Secondo il provvedimento del Garante del 27 novembre 2008, si intende la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Autenticazione	È il processo che verifica l'identità di un utente in modo da poter correttamente permettere o negare l'accesso a risorse condivise e protette. Di fatto, tramite l'autenticazione, si associa un utente con la sua identità digitale presente nel sistema. Le tecniche di autenticazione possono spaziare dal semplice login con username e password a meccanismi più complessi e forti come token, certificati digitali a chiave pubblica o sistemi biometrici.
Autorizzazione	Segue l'autenticazione ed è il processo che consente l'accesso alle risorse solamente a coloro che hanno i diritti di usarle. Durante l'autorizzazione vengono quindi valutati i privilegi dell'identità digitale associata all'utente autenticato e viene consentito, limitato oppure impedito l'accesso alla risorsa, applicando opportune regole stabilite in precedenza.
BIOS	Sequenza di istruzioni di base per effettuare i controlli sulle periferiche e dare i primi comandi durante la fase di avvio che precede il caricamento del sistema operativo della macchina.
Chiave pubblica	Una chiave pubblica, nella crittografia, è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata. La caratteristica principale è che ogni coppia di chiavi è formata in modo tale che ciò che viene cifrato con la chiave pubblica, può essere decifrato solo con la chiave privata. Non è possibile derivare la chiave privata dalla chiave pubblica.
Credenziali di autenticazione	Dati e dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione ad un sistema informatico.
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 ad un identificativo come il nome o un numero, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Identificazione	Si parla di identificazione quando un utente che intende accedere ad un sistema informatico (server, applicativo, etc.) dà prova della propria identità per poterlo fare. Ciò può essere realizzato con l'individuazione di uno username, uno user-id, una smart card o qualsiasi altro elemento che possa far risalire in maniera univoca all'utente stesso.

Termine o acronimo	Definizione
Identità digitale	Insieme ben definito di: • informazioni di identificazione della persona fisica in un determinato contesto digitale (ad esempio ID, username, e-mail, nickname ecc.), • informazioni che ne caratterizzano i permessi
Log	Una registrazione cronologica degli eventi verificatisi in un sistema informatico, comprensiva dell'istante in cui essi sono avvenuti.
Log management	Un sistema di log management permette di aggregare e conservare i log prodotti da sistemi informativi eterogenei, con lo scopo di garantire la sicurezza dei sistemi stessi e consentendo di ridurre i tempi di rilevazione delle minacce informatiche.
Need to know	L'accesso logico a reti, sistemi e base dati deve essere concesso sulla base delle effettive esigenze operative dell'utente;
Non-Disclosure Agreement (NDA)	Atto tra enti pubblici o privati con il quale una parte garantisce all'altra di non rivelare a nessuno determinate informazioni confidenziali che lo riguardano e di cui sia giunto a conoscenza, in qualsiasi forma, sulla base di una relazione professionale, di un progetto, di uno 'scopo' specifico tra le parti coinvolte.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Privilegio minimo *(Least Privilege)*	Principio secondo cui ciascun utente o modulo computazionale (dispositivo, processo, programma, o sistema), abbia accesso alle sole risorse strettamente necessarie alla sua attività o funzionamento. L'obiettivo di questo principio è quello di ridurre la superficie di rischio in ogni istante, migliorando la protezione dei sistemi e dei dati in essi custoditi, sia per quanto riguarda la tolleranza ai guasti, che per la salvaguardia da condotte malevole.
Referente informatico	Dipendente del Comune di Milano che costituisce il punto di riferimento del soggetto esterno che svolge un'attività di collaborazione con la Direzione di assegnazione.
Responsabile per la gestione delle utenze	Soggetto che, in qualità di Amministratore di Sistema (compresi gli Amministratori Applicativi), dispone delle autorizzazioni necessarie per creare, modificare, disattivare o cancellare le utenze attribuite a dipendenti interni o soggetti esterni che collaborano con il Comune di Milano.
Rischio	Potenzialità di un evento indesiderabile.
Separazione dei ruoli *(Segregation of duties, in sigla SOD)*	Nella gestione degli accessi deve essere garantita la segregazione di attività incompatibili tra loro al fine di evitare la concentrazione di abilitazioni che potrebbero creare situazioni di rischio (ad es. uso improprio, modifiche non autorizzate o non intenzionali).
Sessione di lavoro	Insieme di dati, programmi e configurazioni presenti su un elaboratore e associati ad un utente dal sistema operativo. La sessione di lavoro personale è avviata dopo la fase di autenticazione, tipicamente digitando utenza e credenziale di autenticazione (login), e rimane operativa fino alla sua terminazione (logoff).

Termine o acronimo	Definizione
Sistema di autenticazione informatica	Insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità digitale.
Sistema di autorizzazione	Insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Strong Authentication	Metodo di autenticazione che si basa sull'utilizzo congiunto di due (*Two -factor authentication*) o più metodi di autenticazione individuale (*multi-factor authentication*). Per autenticarsi ad un sistema informatico (es. computer o bancomat) vengono distinti tre diversi metodi: • "Una cosa che conosci", per esempio una password o il PIN. • "Una cosa che hai", come un telefono cellulare, una carta di credito o un oggetto fisico come un token. • "Una cosa che sei", come l'impronta digitale, il timbro vocale, la retina o l'iride, o altre caratteristiche di riconoscimento attraverso caratteristiche uniche del corpo umano (biometria).
Risorse Informatiche	Qualsiasi tipo di hardware, software, dati, mezzi di comunicazione elettronica, reti di trasmissione. Nell'ambito della presente policy, ci si riferisce alle risorse fornite dal Comune di Milano ai propri dipendenti ed al personale esterno che li coadiuva per adempiere proprie attività lavorative in termini di produttività personale d'ufficio.
Unico Accesso	Principio secondo il quale tutte le utenze nominali devono essere uniche e personali, attribuite ad un individuo fisico. Tutti gli utenti utilizzatori di una risorsa informatica devono essere associati ad un'utenza singola, personale e non cedibile creata secondo un sistema di codifica previsto da standard definiti dal responsabile di sistema in accordo con l'Unità Cyber Security presso ITED. Dall'utenza deve essere possibile risalire al suo reale utilizzatore. Le utenze devono utilizzare livelli di autenticazione adeguati al rischio associato al valore del sistema informativo da proteggere. Gli standard del livello di autenticazione sono definiti dai responsabili di sistema in accordo con l'Unità Cyber Security presso ITED. Nel caso sia necessario utilizzare utenze di servizio non nominali deve essere implementato un metodo tecnico / organizzativo che permette di risalire al reale utilizzatore dell'utenza in un certo momento.
User name	È la componente pubblica ed univoca delle credenziali di autenticazione.
Utente	Nel contesto del presente documento, è la persona che fa utilizzo di una risorsa o sistema informatico.
Utenza	Viene creata prima della creazione dell'identità digitate ed è l'insieme di attributi che identificano e definiscono una persona (l'utente), come ad esempio il suo nome, il codice fiscale, il ruolo e le mansioni.
Utenza generica	Utenza non nominale utilizzato da più dipendenti tramite l'inserimento delle stesse User ID e credenziali
Utenza nominale	Utenza singola e personale utilizzata da un utente per l'accesso ad una o più risorse di un Sistema Informativo
Utenza tecnica	Utenza non nominale attivata tramite uno specifico processo per una connessione o interazione con un altro sistema.

Termine o acronimo	Definizione
Utenza privilegiata	Utenza che dispone di abilitazioni aggiuntive che possono modificare i diritti di accesso di altri utenti o risorse IT
VPN (Virtual Private Network)	È una rete di telecomunicazioni privata, instaurata come connessione tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico e condiviso, come ad esempio la suite di protocolli Internet.

6 Ruoli e responsabilità

Nel seguito la tabella riepilogativa dei ruoli e delle responsabilità relative al contenuto della presente policy.

Ruolo	Responsabilità funzionali
Amministratori di sistema, di server, di database, delle applicazioni e tutti gli utenti	• Assunzione di responsabilità nella gestione delle identità digitali e delle credenziali di autenticazione personale e nel rispetto dei contenuti della policy.
Direzione Innovazione Tecnologica e Digitale (ITED) e Responsabile della sicurezza informatica presso la direzione.	• Redazione della presente policy e revisione periodica della stessa. • Monitoraggio dell'applicazione delle regole dettate. • Redazione e approvazione di procedure tecniche correlate all'applicazione della presente policy su ambiti specifici. • Redazione dei modelli delle procedure specifiche di attuazione della policy. • Formazione e divulgazione tecnica e di responsabilità in relazione alla presente policy ed alle procedure correlate. • Individuazione dei sistemi informativi, applicazioni e database del Comune da proteggere attraverso l'immissione di credenziali di autenticazione sicure.
Direzione Organizzazione e Risorse Umane	• Approvazione della policy e delle sue revisioni. • Prima richiesta di creazione dell'identità digitale dei dipendenti neoassunti.
DPO (Data protection Officer)	• Collabora alla redazione della policy e delle sue revisioni.
Responsabili della progettazione e gestione di sistemi e applicazioni	• Valutazione, realizzazione e gestione delle scelte tecnologiche conformemente alle regole dettate e in condivisione con il responsabile della sicurezza informatica presso ITED. Adeguamento dei modelli di procedure alle specifiche esigenze. • Condivisione delle procedure con il responsabile della sicurezza informatica presso la Direzione ITED e con i responsabili della gestione delle identità digitali e delle credenziali di autenticazione secondo competenza. • Gestione dell'elenco e del ciclo di vita delle utenze, identità digitali e delle credenziali di autenticazione di propria competenza, secondo le indicazioni ricevute dai responsabili per la gestione delle stesse. • Gestione della tipologia di dati associati alle utenze e identità digitali.
Responsabili per la gestione delle Utenze	• Gestione del ciclo di vita delle utenze e delle identità digitali di propria competenza. • Propagazione delle modifiche recepite da Risorse Umane ai responsabili della gestione di sistemi, applicazioni e database.
Utenti	• Assunzione di responsabilità nella gestione delle identità digitali e delle credenziali di autenticazione loro assegnate e rispetto dei contenuti della policy.

La presente policy è strutturata in modo da evidenziare le regole da osservare e i conseguenti comportamenti da tenere nel rispetto delle disposizioni vigenti in materia di responsabilità penale, civile, amministrativa e disciplinare così come previsto dal CCNL e dallo Statuto dei Lavoratori.

7 Principi di carattere generale

Tutti gli accessi alle risorse e agli asset dei Sistemi Informativi del Comune di Milano devono essere gestiti in conformità con i principi e criteri di sicurezza di seguito riportati, inerenti alla gestione sicura delle identità digitali e delle credenziali di autenticazione.

Nello specifico, in ottica di conformità a quanto previsto dal Regolamento, il Comune ha definito i principi di seguito riportati:

- utilizzare un sistema centralizzato approvato dal Comune al fine di associare l'identità all'utenza creata per l'accesso ai sistemi informatici;
- gli identificativi (userID) utilizzati da parte di un soggetto (utente) per l'accesso alle applicazioni o ai sistemi informatici devono fare riferimento in maniera univoca all'identità fisica della persona stessa. Laddove per particolari esigenze operative o di business sia necessario l'utilizzo da parte di più utenti di una singola utenza non personale, è necessario prevedere controlli compensativi che assicurino di poter stabilire le singole responsabilità individuali e risalire univocamente al soggetto che ha eseguito una specifica operazione;
- disattivare o rimuovere gli ID utente al momento della cessazione del rapporto di lavoro di un dipendente o al termine di un contratto di fornitura;
- eliminare gli ID utente non più utilizzati. Non riutilizzare ID utente precedentemente assegnati ad altri utenti;
- prevedere una modalità per consentire la disabilitazione o rimozione immediata degli ID utente in caso di emergenza;
- i privilegi assegnati agli utenti devono permettere l'accesso ai dati, alle funzionalità applicative ed alle risorse informatiche, necessari allo svolgimento delle proprie funzioni, secondo il principio del Need-to-know e minimo privilegio;
- le attività considerate critiche devono essere separate a livello funzionale ed individuale per evitare quanto più possibile che lo stesso utente possa portare a compimento un intero processo critico in autonomia, secondo il principio della Separazione dei ruoli (Segregation Of Duty – SOD);
- devono essere registrati gli accessi ai sistemi informatici del Comune tramite un processo che consiste nella scrittura, su appositi archivi non modificabili, delle operazioni compiute per l'utilizzo di una risorsa (utente, tipo operazione, data/ora, etc.), come normato all'interno della Linea guida per la gestione e conservazione dei log;
- è necessario tracciare tutte le richieste di abilitazione e le relative approvazioni nonché le abilitazioni assegnate agli utenti in tutti i momenti della loro vita nell'Ente (storico delle abilitazioni);
- l'identificativo utente (account), la password od altri sistemi di autenticazione assegnati all'utente, devono essere gestiti da parte di ogni utilizzatore con la massima riservatezza, in modo tale da minimizzare il rischio di accessi ai dati non autorizzati.

Oltre ai punti sopra indicati, il Comune di Milano per la redazione del presente documento ha tenuto conto anche delle Misure Minime AgID (cfr. [3.]), con specifico riferimento alle "**regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi"** e del documento di EA **"***Linee guida Identità e autenticazione Backoffice"* in cui sono espressi tutti gli standard tecnologici ed i protocolli da utilizzare per gli ambiti di identificazione autenticazione e autorizzazione.

8 Classificazione delle utenze

Dal processo di gestione sicura delle identità digitali adottato dal Comune di Milano deriva la seguente classificazione delle utenze:

- **Utenze nominali:** utenze singole e personali utilizzate da dipendenti o da terze parti per l'accesso ad una o più risorse del Sistema Informativo. In questa categoria rientrano:
    - **le utenze privilegiate**: utenze nominali e riconducibili ad una sola persona, che dispongono di abilitazioni aggiuntive che possono modificare i diritti di accesso di altri utenti o risorse IT.

- **Utenze non nominali (generiche)**: utenze non nominali create ed utilizzate solo per casistiche straordinarie (eccezioni giustificate) da più dipendenti o terze parti tramite l'inserimento delle stesse User ID e credenziali di autenticazione. In tale categoria rientrano:
    - **utenze tecniche**: utenze non nominali attivate tramite uno specifico processo per una connessione o interazione con un altro sistema. Si potrebbe trattare ad esempio di utenze di "root" di UNIX o "Administrator" di Windows, che devono essere utilizzate solo per le situazioni di emergenza, o laddove non sia tecnicamente possibile l'utilizzo di utenza nominale e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.

9 Gestione dell'accesso logico

Il Comune di Milano per la gestione dell'accesso logico adotta i processi di seguito elencati, mettendo in atto i principi ed i criteri di sicurezza appartenenti agli stessi.

Il dettaglio tecnologico degli strumenti e piattaforme a disposizione per assolvere alle attività di identificazione autenticazione e autorizzazione per dipendenti e collaboratori sono presenti all'interno della Linea guida EA (cfr. [3.])

9.1 Identificazione

Secondo tale processo un'identità digitale risulta essere articolata in due parti:

- L'identità dell'utente (chi è l'utente).
- Le credenziali possedute dall'utente (gli attributi di tale identità).

L'identità consiste in un user-id o username e in una parola di identificazione segreta (password). In tale contesto, lo username può assumersi come identità digitale e la parola segreta come credenziale di autenticazione.

In tale contesto, il Comune identifica due diverse tipologie di utenze:

- **utente amministratore**, avente accesso alle risorse informatiche del sistema al quale si riferisce nonché il controllo di tutti gli altri profili;
- **utente base**, associato a identità digitali limitate unicamente alle risorse indispensabili all'espletamento delle proprie mansioni lavorative e al corretto funzionamento dei sistemi ai quali hanno accesso.

I sistemi informatici ivi comprese le applicazioni, devono verificare che l'identificativo utente sia un codice univoco al suo interno. L'identificativo deve essere assegnato e riconducibile ad una sola persona fisica e non ad utenze di gruppo.

9.2 Autenticazione

Il Comune prevede l'utilizzo di credenziali di autenticazione con un livello di sicurezza proporzionali al livello di criticità e di rischio del sistema informativo a cui si sta accedendo ed al tipo di dati trattati dallo stesso utilizzando le seguenti modalità per l'autenticazione:

- **Autenticazione semplice**: l'accesso al sistema informativo deve avvenire tramite l'immissione di credenziali di autenticazione sicure. Questa modalità di accesso deve essere utilizzata solo in ambienti protetti da ulteriori sistemi di sicurezza e considerati pertanto a rischio minore. Verrà progressivamente non più applicata.
- **Strong Authentication**: gli accessi ai sistemi informativi ritenuti critici in ottica riservatezza, disponibilità ed integrità dei dati trattati, devono essere gestiti tramite sistemi di autenticazione forte e devono avvenire mediante autenticazione multi-fattore. Tale metodo di autenticazione si basa sull'utilizzo congiunto di due o più metodi di autenticazione individuale. Qualsiasi accesso da remoto ai sistemi informativi del Comune deve essere gestito tramite autenticazione multi-fattore. Questo requisito deve essere formalmente espresso in ogni contratto per forniture di servizi su cui è applicabile. È previsto un periodo transitorio di sei mesi per permettere la transizione a questa modalità.
- **Autenticazione tramite certificato**: in cui si utilizza un certificato digitale per identificare un utente un sistema o dispositivo per l'accesso a una risorsa, una rete o un'applicazione, verificando che lo stesso sia autorizzato all'accesso.

Le regole per l'autenticazione tramite certificato prevedono che:

- il certificato digitale da utilizzare per l'autenticazione tra risorse interne ed esterne al perimetro del Comune di Milano, sia ottenuto da una Certification Authority di tipo trusted globalmente accreditata;
- l'utilizzo di certificati digitali di tipo self-signed sia previsto solo nei casi di autenticazione machine-to-machine come ad esempio tra appliance/dispositivi network, sistemi ed applicazioni interne al perimetro del Comune di Milano;
- sia effettuata l'encryption delle credenziali dei certificati digitali durante le fasi di generazione, distribuzione, conservazione e backup.

Oltre alle modalità sopracitate di autenticazione, sono presenti modalità di accesso non interattivo in cui non è direttamente coinvolto un utente nel processo di autenticazione e possono includere a titolo esemplificativo, l'autenticazione tra: applicazioni, script di automazione e applicazioni o tra applicazioni e servizi.

In questo ambito il Comune ha definito le regole di sicurezza di seguito riportate:

- le funzionalità dell'account utilizzato per il login non interattivo devono essere limitate allo specifico scopo previsto per tale account. (es. un account utilizzato per il monitoraggio non deve possedere i privilegi per accedere in modo interattivo al sistema, aggiungere utenti o modificare le configurazioni

del sistema e non deve essere riutilizzato per altri scopi, come l'esecuzione di backup del sistema o l'accesso regolare);

- l'account utilizzato per gli accessi non interattivi, ove tecnicamente possibile, non deve avere privilegi illimitati di amministratore o di superuser;
- i certificati, le chiavi SSH, le chiavi API, devono essere unici per ogni account e devono avere una complessità ed una robustezza significativamente superiori a quelle delle password o delle passphrase utilizzate per le utenze nominali o impersonali.
- le informazioni segrete di autenticazione utilizzate esclusivamente per gli account non interattivi devono essere sottoposte a rinnovo su base periodica, almeno annualmente;
- le informazioni segrete di autenticazione devono essere modificate tempestivamente e comunque entro le 24 ore se vi sono prove o sospetti di compromissione, o se chi a conoscenza di tali informazioni cambia mansione o non ha più un rapporto lavorativo con l'Ente;
- le informazioni segrete di autenticazione devono essere conservate in modo sicuro (Vault o cassaforte elettronica), ove tecnicamente possibile. Laddove non sia tecnicamente possibile, devono essere utilizzati controlli compensativi come, il monitoraggio rafforzato ed i controlli di accesso restrittivi (es. file ACL). Tutti gli accessi al Vault devono essere registrati e limitati alle persone autorizzate;
- monitorare l'uso dell'account non interattivo alla ricerca di prove di attività inappropriate o non autorizzate, ove tecnicamente possibile.

9.3 Autorizzazione

Il Comune garantisce che l'accesso alle risorse del sistema informatico sia limitato ai soli utenti che ne hanno diritto attribuendo specifici privilegi di accesso agli utenti denominati profili autorizzativi. I principi di sicurezza applicati sono riportati al par.7 ed in generale i profili autorizzativi devono:

- essere definiti in ragione del ruolo ricoperto;
- abilitare l'accesso alle risorse informatiche pertinenti alle mansioni svolte;
- essere configurati per limitare l'accesso ai soli dati necessari alle finalità dell'attività lavorativa secondo il principio del minimo privilegio e Need-to-know;
- rispettare la separazione dei ruoli secondo il principio di Segregation of Duties.

10 Gestione delle Utenze

10.1 Ciclo di vita delle utenze

Il ciclo di vita delle utenze adottato dal Comune di Milano è basato sugli stati di creazione, modifica, disattivazione e cancellazione**.**

Le attività ed i flussi riferiti ai vari stati sono descritti all'interno della Procedura degli accessi logici che costituisce il riferimento per le attività operative.

Tutte le attività relative al ciclo di vita delle utenze devono essere registrate su supporto elettronico non modificabile e protetto in modo sicuro per tenere traccia di tutte le attività associate alle stesse.

Le applicazioni che gestiscono dati associati alle utenze con il controllo esclusivo delle risorse informative necessarie all'amministrazione devono essere progettate e realizzate in modo tale che la disponibilità dei dati sia indipendente dal ciclo di vita delle singole utenze.

10.2 Gestione degli utenti con diritti di accesso privilegiato

Il ciclo di vita sopracitato è applicabile in tutte le sue quattro fasi anche alle utenze aventi diritto di accesso privilegiato (Amministratori di Sistema).

Sono identificati quindi come Amministratori di Sistema, le figure professionali che svolgono le seguenti funzioni, nella misura in cui esse consentono di intervenire sui dati personali:

- Amministratori di rete e/o di apparati di sicurezza (Network administrator);
- Amministratori di Unità elaborative (Server administrator);
- Amministratori di banche dati (Database administrator);
- Amministratori delle applicazioni.

Il Comune, in osservanza della normativa vigente, adotta delle regole di sicurezza specifiche, di seguito descritte:

- l'accesso privilegiato alle informazioni, ai dati ed ai sistemi informatici deve essere consentito unicamente previa identificazione, autenticazione e autorizzazione tramite apposite credenziali di accesso, appositamente definite e, se possibile, differenti dall'utenza istituzionale;
- deve essere verificato che l'utenza amministrativa sia stata designata come tale: in tal senso è necessario che venga predisposta una lettera di nomina e che questa venga conosciuta e firmata da parte dell'utente di riferimento. I criteri con cui il Comune sceglie di concedere privilegi da amministratore ad un utente, sono proporzionali al livello di criticità e di rischio di sicurezza delle informazioni relativi ai sistemi informativi di riferimento;
- i profili di accesso alle informazioni, ai dati ed ai sistemi devono essere mantenuti allineati al ruolo ed alle mansioni operative svolte, recependo eventuali cambiamenti, e devono essere monitorati periodicamente in osservanza dei requisiti previsti dalla normativa vigente.
- il Comune esegue un'attività di tracciatura e monitoraggio degli accessi degli amministratori di sistema sui propri sistemi informativi al fine di monitorare l'effettiva necessità di mantenerli attivi e di provvedere, in caso di inattività prolungata, al blocco degli stessi;

- qualora l'accesso non sia più necessario, l'utenza ed i relativi privilegi devono essere prontamente modificati o rimossi, assicurando comunque che sia possibile risalire al soggetto cui la stessa era associata;
- le utenze built-in devono essere utilizzate univocamente a scopo di configurazione e/o interventi che esulano dalla normale routine di un utente privilegiato;
- le utenze privilegiate nominali non devono essere condivise tra più utenti, per consentire sempre di risalire all'utente utilizzatore;
- le utenze privilegiate di servizio, necessarie allo svolgimento di task automatici/schedulati, possono essere condivise tra più utenti autorizzati (devono essere censite in correlazione alle persone a cui vi hanno accesso);
- l'utenza amministrativa deve utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi;
- qualora l'autenticazione a più fattori non sia supportata, è necessario utilizzare credenziali di autenticazione di elevata robustezza (es: password di lunghezza pari ad almeno 10 caratteri), al fine di impedire che per le utenze amministrative vengano utilizzate credenziali di autenticazione deboli;
- le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, devono essere utilizzate solo per le situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
- non si deve consentire l'accesso diretto ai sistemi con le utenze amministrative. Gli amministratori di sistema devono utilizzare un'utenza con privilegi standard per le normali attività lavorative ed utilizzare i privilegi amministrativi unicamente per le attività correlate allo scopo, avendo cura di recuperare le credenziali necessarie tramite i canali resi disponibili dall'Ente;
- si deve evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio);
- deve essere mantenuto un inventario in cui siano censite tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. Tale inventario delle utenze amministrative deve essere gestito attraverso uno strumento automatico che segnali ogni variazione.

Per ulteriori dettagli legati alla gestione delle utenze e dell'operatività degli Amministratori di Sistema si rimanda alla specifica normativa interna.

10.3 Riesame dei diritti di accesso

I diritti di accesso degli utenti devono essere riesaminati su base periodica e regolati attraverso la Procedura degli accessi logici.

Il Comune verifica periodicamente e comunque su base annuale, la sussistenza delle condizioni per il mantenimento dei profili autorizzativi, con particolare attenzione ai profili autorizzativi privilegiati (es. Amministratori di sistema).

I fattori che possono determinare un cambiamento nella definizione dei profili autorizzativi sono generalmente legati alle seguenti circostanze:

- cambio di ruolo o mutamento delle mansioni svolte dal titolare dell'utenza;
- mutamenti dello scenario tecnologico dell'infrastruttura informatica;
- evoluzione dello scenario normativo di riferimento.

10.4 Revoca o modifica dei diritti di accesso

Quando un dipendente od un collaboratore esterno cambia mansione, si dimette o termina il rapporto lavorativo con il Comune di Milano si adottano le regole espresse al par.7 avendo cura di bloccare o rimuovere gli accessi, o modificarne i diritti in funzione del nuovo ruolo ricoperto entro le 24h dalla notifica dell'evento.

È responsabilità del Responsabile diretto della risorsa la gestione della revoca dei diritti di accesso e la comunicazione tempestiva della cessazione del rapporto agli enti che gestiscono gli accessi.

11 Gestione delle credenziali di autenticazione

I sistemi di gestione delle credenziali di autenticazione all'interno del Comune di Milano devono essere interattivi e devono assicurare credenziali di qualità. In tale contesto, il sistema di gestione delle credenziali di autenticazione deve:

- forzare l'uso di identificativi di User ID e credenziali personali per mantenere la tracciabilità;
- permettere agli utenti di selezionare e cambiare le proprie credenziali e includere una procedura di conferma per errori di input;
- forzare la scelta di credenziali di autenticazione robuste composte da almeno dieci caratteri, che includano almeno un carattere maiuscolo, minuscolo, un numero ed un carattere speciale;
- forzare gli utenti a cambiare le credenziali di autenticazione al primo log-on;
- forzare un cambio periodico della credenziale di accesso ogni 120 giorni;
- se la password o la passphrase non può essere di almeno quindici caratteri, deve essere la più lunga tecnicamente consentita. Se tecnicamente possibile, privilegiare l'uso di passphrase, soprattutto se la password è destinata a essere memorizzata;
- impedire l'uso di password banali o facilmente individuabili o compromesse (es., impedire l'uso dell'id utente all'interno della password);
- impostare una validità minima delle password ad un giorno;
- mantenere una registrazione delle credenziali di autenticazione precedentemente usate per prevenire il loro riutilizzo;
- non mostrare le credenziali di accesso in chiaro quando queste vengono inserite;
- memorizzare i file delle credenziali di autenticazione in modalità criptata separatamente dai dati del sistema applicativo in una forma resistente agli attacchi offline;
- memorizzare e trasmettere le credenziali di autenticazione in modo protetto.

11.1 Ciclo di vita delle credenziali di autenticazione

Il ciclo di vita delle credenziali di autenticazione adottato dal Comune di Milano è basato sugli stati di:

- Creazione;
- Distribuzione;
- Modifica;
- Protezione, conservazione e ripristino;
- Validità e scadenza;
- Utilizzo.

Nei paragrafi che seguono, sono riportate in aggiunta alle regole generali presenti al punto 11, gli elementi specifici che caratterizzano ognuna delle singole fasi.

11.1.1 Creazione

- La creazione della password deve essere conforme allo standard definito dall'Ente; tale standard deve essere noto all'utente per facilitarlo nella scelta della composizione della credenziale;
- la scelta del formato di input è effettuata secondo criteri tali da garantire la maggior difficoltà di deducibilità e contemporaneamente la minor difficoltà di memorizzazione;
- la scelta della credenziale di accesso per applicazioni e database deve rispettare lo standard di complessità generale definito nella presente linea guida.

11.1.2 Distribuzione

- Le credenziali di autenticazione fornite all'utente sono strettamente personali e pertanto non devono essere comunicate a terzi o condivise;
- le credenziali di autenticazione devono essere consegnate all'utente proprietario separatamente dalla componente pubblica delle credenziali di accesso;
- le credenziali di autenticazione devono essere consegnate all'utente proprietario attraverso strumenti e canali sicuri che ne garantiscano la riservatezza come SMS, file criptato ecc., seguendo le procedure specifiche individuate per ogni sistema in base al livello di sicurezza stabilito dai responsabili.

11.1.3 Modifica

La modifica delle credenziali di autenticazione deve rispettare i criteri di creazione e distribuzione individuati dalla presente policy.

- Nel caso in cui il dipendente possa avere dubbi che la segretezza delle proprie credenziali di autenticazione sia stata compromessa:
    - qualora disponibile la funzione di cambio password, effettua un reset della password ed effettua la segnalazione al Responsabile della Sicurezza Informatica presso ITED;
    - in alternativa, effettua la segnalazione al Responsabile della Sicurezza Informatica presso ITED, il quale avvia il processo per richiedere immediatamente il cambio delle credenziali.
- Le credenziali modificate devono essere diverse dalle ultime 5 utilizzate.

11.1.4 Protezione, Conservazione e Ripristino

- Le credenziali di autenticazione sono personali e segrete; l'utente, responsabile della sua custodia, non deve cederle, divulgarle o lasciare che possano essere lette e/o conosciute da terzi;
- le credenziali registrate nel database di autenticazione devono essere crittografate. Il metodo crittografico selezionato deve rispondere ai criteri di sicurezza opportuni in relazione al contesto applicativo ed alto sviluppo tecnologico;
- è vietato utilizzare programmi in grado di decodificare le credenziali di autenticazione;
- le informazioni alternative alla credenziale di autenticazione che devono consentire l'identificazione dell'utente in caso di dimenticanza della stessa, devono essere crittografate secondo le medesime indicazioni;

- le credenziali devono essere conservate secondo i principi di segretezza, con lo scopo di poterle ripristinare, in caso di emergenza, da parte di personale autorizzato;
- le credenziali dimenticate non possono essere recuperate ma devono essere rigenerate secondo le modalità di creazione indicate nella presente policy;
- è compito della Direzione ITED individuare i sistemi informatici/informativi da proteggere attraverso credenziali di autenticazione;
- per ciascuna risorsa individuata, è necessario inoltre istituire il metodo di conservazione delle credenziali di autenticazione attraverso repository o database, comuni o dedicati, accessibili attraverso determinati livelli di sicurezza, in riferimento alle categorie:
    - credenziali associate ad utenze amministrative per le quali prevedere il ricalcolo periodico e il recupero esclusivamente da parte dei soggetti preventivamente identificati e autorizzati;
    - credenziali associate a dispositivi che regolano l'accesso a locali protetti;
    - credenziali di utenze di dominio;
    - credenziali di utenze per l'accesso ad applicativi e database;
    - password di BIOS.

- È compito del responsabile della gestione di ciascun sistema o applicazione, valutare e gestire le soluzioni tecnologiche più adeguate al contesto di sviluppo, rispetto al software di protezione, conservazione e ripristino delle password. Criteri di valutazione e scelte, devono essere condivise con il responsabile della sicurezza informatica dei dati presso ITED.

11.1.5 Validità e Scadenza

- Il periodo di validità delle credenziali è correlato al ciclo di vita delle identità disciplinato dalla presente policy;
- la scadenza delle credenziali di autenticazione è disciplinata dalle regole di modifica indicate nella presente policy.

11.1.6 Utilizzo

- Le credenziali di autenticazione devono essere utilizzate per accedere ad un sistema in modalità personale e riservata;
- l'utente è obbligato all'uso delle credenziali di autenticazione per impedire gli accessi da parte di terzi a sessioni da lui attivate;
- è vietato memorizzare in chiaro le credenziali di autenticazione nelle pagine dei servizi Internet o in quelle delle applicazioni;
- è compito dei responsabili dei sistemi di autenticazione o dei responsabili di applicativi, in accordo con il responsabile della sicurezza informatica presso ITED, definire tutte le procedure necessarie per la creazione, distribuzione, modifica, protezione, conservazione, recupero delle credenziali di autenticazione.

12 Autenticazione e autorizzazione – Migliori prassi

Al fine di rendere sicuri i meccanismi di autenticazione e autorizzazione nella linea guida di EA (cfr. [3.]), al par. 3 sono elencate le migliori prassi da seguire corredate da esempi pratici con le relative contromisure da applicare.

Si rimanda alla sezione specifica del sopracitato documento per i riferimenti puntuali.

13 Inosservanza della Policy

Qualora la condotta dell'utente non fosse conforme a quanto prescritto all'interno della policy, quest'ultimo potrebbe incorrere in responsabilità per inosservanza delle disposizioni di servizio o contrattuali.

Comune di Milano	**Allegato D - Procedura di gestione dei Data Breach**		
PD-PRO	Data	Versione	Stato
Protezione dati Procedura	**30/12/2024**	**1.3**	**Definitiva**

Versione del Documento

	Data	**Approvazione**
Prima emissione	08/07/2020	*Direttore Operativo*
		Direzione Sistemi Informativi e Agenda Digitale

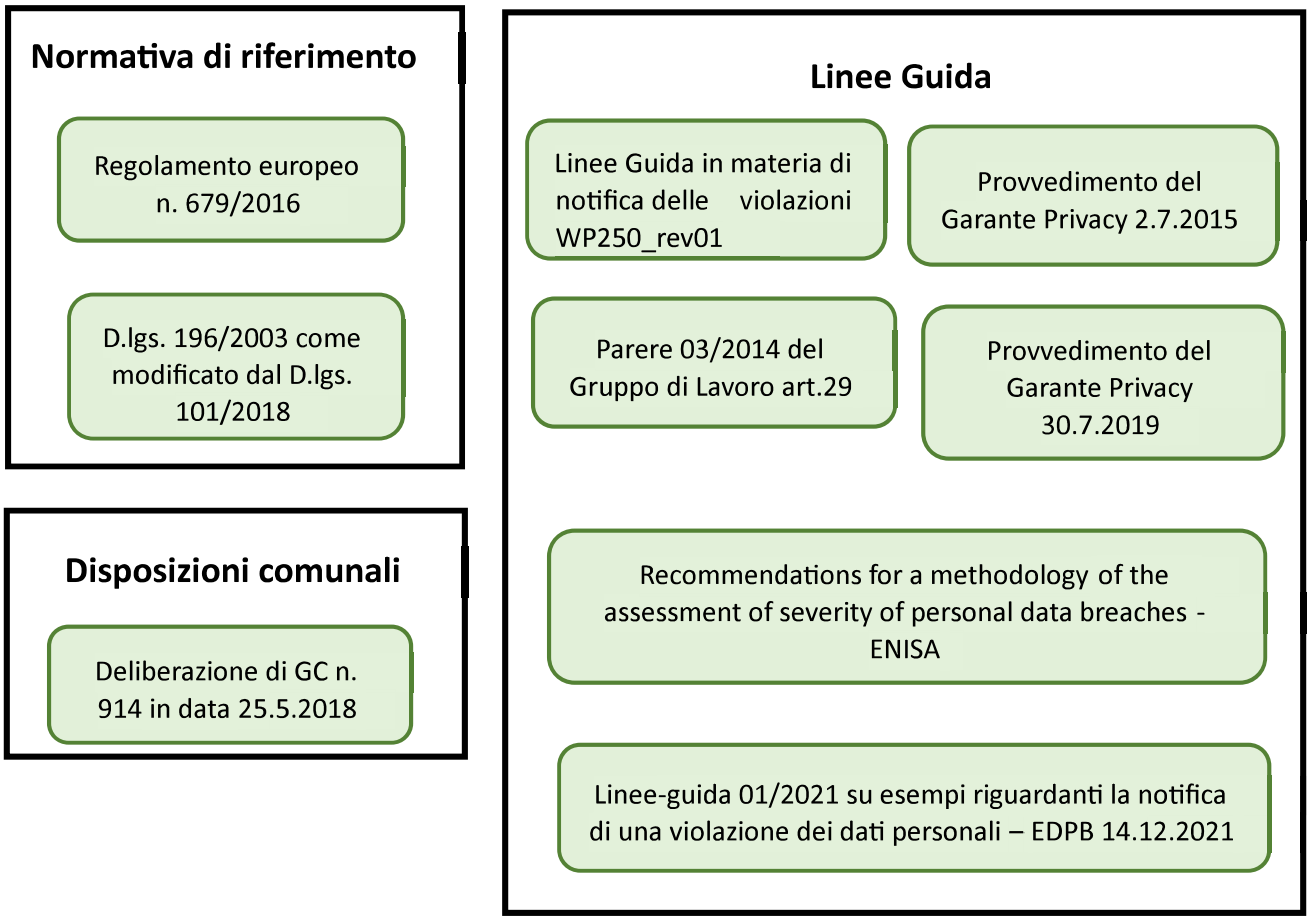
Revisioni

Versione	**Data**	**Motivo della revisione**	**Approvazione**	**Firma**
1.2	28/12/2022	Aggiornamento modalità notifica Autorità Garante	*Vice Direzione Generale*	
			Direzione Innovazione Tecnologica e Digitale	
1.3	30/12/2024	**Aggiornamento ruolo comitato di crisi, criteri individuazione punteggi e predisposizione modello verbale**	*Direzione specialistica Legalità e controlli*	
			Direzione Innovazione Tecnologica e Digitale	

CIACCI MARCO 30.12.2024 10:17:24 UTC

Guido Arnone Comune di Milano Direttore di Direzione 30.12.2024 14:14:48 GMT+01:00

Norme e linee guida di riferimento



I riquadri qui sopra indicati riportano le normative e le linee guida a cui ci si è ispirati al fine di definire il flusso da osservare nel caso si verifichi una violazione dei dati personali. Il documento individua le fasi da seguire per adempiere agli obblighi previsti in caso di data breach.

Per maggiore chiarezza su quanto previsto dalle Linee Guida WP250 – rev.01, dalle Raccomandazioni ENISA e dalle Linee Guida EDPB:

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

https://www.enisa.europa.eu/publications/dbn-severity

Guidelines 01/2021 on Examples regarding Personal Data Breach Notification | European Data Protection Board (europa.eu)

Indice dei contenuti

1 Normativa di riferimento

[1]	*Regolamento Europeo n. 2016/679*
[2]	*D.lgs. n. 196/2003, come modificato, da ultimo, dal D.lgs. n. 101/2018*
[3]	*"Linee-guida in materia di notifica delle violazioni di dati personali",* WP250_rev.01 del Gruppo di Lavoro ex Art. 29
[4]	*"Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach)"* – del Garante per la Protezione dei Dati Personali del 30 luglio 2019
[5]	*"Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche"* - del Garante per la Protezione dei Dati Personali del 2 luglio 2015
[6]	*"Parere 03/2014 sulla notifica delle violazioni dei dati personali",* del Gruppo di Lavoro ex Art. 29 del 25 Marzo 2014
[7]	*"Recommendations for a methodology of the assessment of severity of personal Data Breaches"* - ENISA
[8]	Deliberazione della Giunta Comunale n. 914 del 25 maggio 2018 recante "Modifica ed integrazione del Regolamento sull'Ordinamento degli Uffici e dei Servizi del Comune di Milano"[1]

2 Introduzione

Il Regolamento UE n. 2016/679 (d'ora in avanti, "il Regolamento") sulla protezione dei dai personali (artt. 33 e 34) ha introdotto per tutti i Titolari del trattamento l'obbligo di notificare all'Autorità di controllo, entro 72 ore dalla conoscenza dell'evento, i casi di violazione dei dati personali e di comunicare agli interessati l'accaduto quando ricorrono particolari situazioni (rischio elevato per i diritti e le libertà delle persone).

Le pubbliche amministrazioni in applicazione del provvedimento n. 393/2015 del Garante per la Protezione dei Dati Personali avevano già l'obbligo di notificare i casi di data breach, ma entro 48 ore dalla conoscenza dell'evento a differenza del Regolamento che estende i termini a 72 ore.

La notifica al Garante per la Protezione dei Dati Personali non è sempre obbligatoria ma è dovuta quando la probabilità del rischio di compromettere i diritti degli interessati è elevata. L'esonero della comunicazione, oltre che in tali casi, vale anche nei confronti degli interessati quando il Titolare del trattamento ha messo in atto misure di sicurezza adeguate come ad esempio quelle destinate a rendere i dati incomprensibili (es. crittografia).

Con il presente documento si intendono definire le procedure operative per la gestione delle violazioni dei dati personali tenendo conto del quadro giuridico attuale e del contesto organizzativo.

[1] La deliberazione definisce tramite l'Appendice n. 9 i criteri di applicazione del Regolamento, attribuendo alla Direzione Sistemi Informativi, Agenda Digitale la funzione di ridefinire o consolidare le procedure per reagire ai fenomeni classificabili come data breach, gestire l'emergenza e registrare comunque gli attacchi subiti, ancorché non abbiano determinato violazioni di dati personali.

Con il richiamo al quadro giuridico attuale si intende far riferimento, in particolare, al citato Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, al D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. n. 101/2018 e in via generale ai documenti prodotti dal Gruppo di Lavoro ex art. 29 Direttiva 95/46/CE (Working Party) la cui funzione è cessata ed è stato sostituito dal Comitato Europeo per la protezione dei dati (EDPB - European Data Protection Board).

3 Ambito di applicazione

La procedura si applica al Comune di Milano nel suo complesso in qualità di titolare del trattamento dati personali (di seguito anche solo "il Comune").

4 Principi generali

In base all'art. 6 del Regolamento i trattamenti effettuati dalle autorità pubbliche sono leciti se e nella misura in cui ricorrono particolari condizioni come *l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*.

Varie informazioni, seppur non rientrino tra le categorie di dati particolari come definite dal Regolamento, possono presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati stessi o alla modalità di trattamento o agli effetti che può determinare (es. condizioni economiche e/o disagio sociale). Tali informazioni se violate possono comportare, soprattutto se riguardano dati particolari, rischi per la dignità degli interessati.

Le attività disciplinate nel presente documento si pongono in continuità con le regole di comportamento definite in documenti interni (comunicati, circolari, linee guida) e in particolare con le linee operative del 31/7/2015 emanate in seguito al provvedimento del Garante n. 393/2015, nonché con la citata deliberazione n. 914/2018 che disciplina tra l'altro a livello generale la procedura per la gestione dei data breach (appendice 9 paragrafo 4.3).

Le strutture coinvolte nel presente documento assicurano, ciascuna nell'ambito della propria sfera di competenza, e anche mediante sistemi informativi idonei, la tracciabilità dei dati e delle informazioni, conservando la documentazione prodotta, sia cartacea che informatica, al fine di ricostruire ex post le fasi del processo. Le attività definite con questa procedura devono essere svolte assicurando la separazione dei ruoli e delle responsabilità al fine di evitare sovrapposizioni o concentrazione di potere svincolato da qualsiasi forma di controllo.

4.1 Principio di finalità

L'art. 5 del Regolamento prevede che i dati personali devono essere trattati in modo lecito e corretto, raccolti per finalità determinate, esplicite e legittime. In base a questa formulazione il Regolamento limita quindi il trattamento ad una finalità ben precisa, preventivamente individuata e resa esplicita.

4.2 Principio di proporzionalità e minimizzazione del trattamento

Devono essere definite preventivamente le modalità e il tipo di informazioni da trattare, in osservanza del principio di proporzionalità: i dati oggetto di trattamento devono essere pertinenti e non eccedenti rispetto alle finalità, nel senso che le operazioni da svolgere sui dati personali, qualitative e quantitative, non possono riguardare fatti o stati che esulano dal fine o che eccedano dalla reale esigenza di trattamento.

4.3 Principio di by design by default

Rappresenta un principio di "precauzione" nel senso che mira ad attenuare i rischi sviluppando e configurando i sistemi informativi e i programmi informatici in modo da escludere o ridurre al minimo l'eventuale utilizzo di dati personali qualora le finalità pubbliche possano essere perseguite anche senza dati personali o identificativi.

In base a tale principio gli strumenti e le modalità impiegati per il trattamento dei dati vanno progettati già all'origine (by design) in modo tale che siano garantite per impostazione predefinita (by default) la tutela della riservatezza e la protezione dei dati personali.

Il criterio della Privacy by design by default è strettamente connesso al principio di accountability, visto che al fine di dimostrare la conformità al Regolamento, il Titolare ha l'onere di adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default (considerando 78 e art. 25 Regolamento).

5 Contesto del Regolamento europeo

5.1 Definizione di data breach

Secondo quanto indicato dall'art. 4 punto 12 del Regolamento, il data breach è considerato una "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". Ai sensi del Regolamento si considera per:

- **Distruzione**, l'indisponibilità irreversibile dei dati personali con impossibilità di ripristino. La violazione è accompagnata dall'eliminazione logica e fisica (es. distruzione di supporti di memorizzazione) con l'impossibilità di ripristinare i dati.
- **Perdita**, l'assenza di controllo fisico dei dati conservati (anche temporanea) intesa come privazione, sottrazione, perdita di dispositivi contenenti dati o documenti cartacei.
- **Divulgazione**, la comunicazione non autorizzata di dati personali, non corrispondenti a informazioni pubbliche, a soggetti terzi non identificabili (persona fisica o giuridica, gruppi di soggetti).
- **Accesso**, si verifica quando terzi non autorizzati (es. dipendenti, fornitori esterni, hacker, etc.) accedono a dati personali non corrispondenti a informazioni pubbliche. L'accesso ai dati (anche in modalità di singola visualizzazione) comporta che gli accessi si sono effettivamente verificati al di fuori delle operazioni di trattamento previste e autorizzate.

Alla luce di quanto suindicato, si possono delineare 3 tipologie di data breach:

- **Violazione della riservatezza**: allorquando si è concretizzato l'accesso e quindi la disclosure accidentale o non autorizzata di dati personali;
- **Violazione della disponibilità**: laddove si è concretizzata la perdita di accesso o la distruzione accidentale o non autorizzata di dati personali;
- **Violazione dell'integrità**: allorquando si è verificata l'alterazione accidentale o non autorizzata dei dati personali.

Di seguito sono riportati alcuni esempi di violazione di dati, con la finalità di identificare con maggior dettaglio i rischi ai quali l'ente comunale può andare incontro.

Evento[2]
Furto di hardware contenente un archivio di dati personali.
Perdita di dati

[2] La lista costituisce un esempio e non può essere considerata esaustiva

Interruzione delle linee dati (o linee telefoniche) che impedisce agli interessati di contattare il Comune e avere accesso ai propri dati che perdura per un tempo eccessivo rispetto alle tempistiche normali di erogazione del servizio.
Attacco ransomware che provoca la crittografia dei dati. Non sono disponibili back-up e i dati non possono essere ripristinati.
Comunicazione di dati personali di interessati a destinatari errati (non incaricati del trattamento), ivi compresa la comunicazione a persone che non sono autorizzate ad avere accesso ai dati personali (e.g. parenti, amici o in ogni caso persone diverse dai destinatari o soggetti a cui i dati personali devono essere comunicati)
Violazione di caselle e-mail di dipendenti
Violazione dei siti web del Comune a causa di cyber attacco, con conseguente estrazione di dati personali degli interessati
Evento[2]
Qualsiasi installazione di software malevolo o virus scaricato sui dispositivi forniti dal Comune che può creare una perdita di disponibilità di dati personali, l'accesso abusivo a dati personali o la sottrazione di dati personali
Furto di identità segnalato dalle forze dell'ordine
Furto o intrusione nei locali del Titolare/Responsabile
Accesso non autorizzato ai dati
Distruzione di documenti cartacei o faldoni in cui vi erano dati personali
Perdita o sottrazione di documenti cartacei o elettronici contenenti dati personali, incluso materiale video fotografico.
Duplicazione non autorizzata di un volume significativo di documenti cartacei, incluso materiale fotografico.

5.2 L'obbligo di notifica ai sensi del Regolamento Europeo

Il Regolamento ha introdotto l'obbligo di notificare i casi qualificabili come data breach al Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, e di darne comunicazione agli interessati, in presenza di un rischio elevato per i diritti e le libertà del singolo.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, deve essere corredata dei motivi del ritardo. L'eventuale responsabile del trattamento, inoltre, deve informare il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Tale notifica deve, secondo l'art. 33 del Regolamento, contenere almeno le seguenti informazioni:

- descrizione della 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;

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- 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.

Il titolare del trattamento è tenuto, inoltre, a documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

6 Definizioni

Comitato di Crisi	Gruppo di Lavoro deputato a supportare il titolare nella gestione degli incidenti informatici che coinvolgono dati personali di soggetti interessati. È costituito dal Responsabile dei Sistemi Informativi, dal Responsabile della Sicurezza Informatica, dal Dirigente della struttura che ha subito l'evento di sicurezza - probabile data breach - e dal Responsabile della Protezione Dati (Data Protection Officer - DPO).
Dirigente di riferimento	Il Dirigente della Funzione al quale è rimesso il presidio 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 o un numero, dati relativi all'ubicazione, un

	identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati biometrici	Dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati particolari	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, biometrici e i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona.
Dati relativi alla salute	Dati personali attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Dati relativi a condanne e reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

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.
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (es. in Italia: Garante per la Protezione dei 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. Il Responsabile del trattamento rileva la violazione che coinvolge i dati del Comune e che si è verificata presso i propri locali o sui propri sistemi e la comunica nelle modalità e nei termini previsti a livello contrattuale.
Soggetto esterno	Il soggetto esterno è identificabile con qualsiasi altro soggetto, diverso dal dipendente, che nella sua veste di collaboratore esterno opera nei locali del Comune di Milano e, di conseguenza, può trovarsi nelle condizioni di rilevare la violazione come qualsiasi altro dipendente del Comune.
Dipendente	Persona autorizzata al trattamento dei dati che opera sotto la diretta autorità del Titolare del trattamento e che, in relazione allo specifico ambito lavorativo coordinato e gestito, tratta dati personali.
Interessato	Qualsiasi persona fisica a cui si riferiscono i dati personali.
Violazione dei dati personali (o Data breach)	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.
Gravità della violazione (o severity)	Stima della portata dell'impatto potenziale sugli individui derivante da violazioni sui dati
Registro delle violazioni	Conserva traccia di ogni incidente con relative cause, eventuali notifiche al Garante per la Protezione dei Dati Personali e comunicazioni agli interessati, le conseguenze e le misure atte a contrastare il ritorno di incidenti dello stesso tipo in futuro (in linea con l'art. 33(5)).

Evento	Accadimento che può causare anomalie nella normale attività o prefigurare una possibile violazione di politiche e controlli o una compromissione di confidenzialità, integrità o disponibilità delle informazioni.
Incidente	Evento singolo o una serie di eventi che hanno una significativa probabilità di compromettere l'operatività aziendale, di minacciare la confidenzialità, l'integrità o la disponibilità dei dati e delle informazioni, di causare l'interruzione o il degrado dei servizi erogati.
Crisi	Situazione formalmente dichiarata di interruzione o deterioramento di uno o più processi critici in seguito a incidenti o catastrofi.

7 Oggetto e scopo

Il presente documento ha l'obiettivo di identificare un "Processo per la gestione dei Data Breach" relativo ai dati personali di cui è Titolare il Comune di Milano, prendendo in considerazione quanto previsto dal Regolamento Europeo n. 2016/679.

In particolare, la finalità di questo modello è quella di assicurare la corretta rilevazione e gestione delle violazioni registrate a garanzia:

- del rispetto degli obblighi di notifica verso il Garante per la Protezione dei Dati Personali, salvo il caso in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
- del rispetto degli obblighi di comunicazione verso gli interessati (es. cittadini, dipendenti, fornitori), allorquando la stessa violazione dei dati personali presenti un alto rischio per i diritti e le libertà delle persone fisiche;
- della minimizzazione di impatti sugli interessati in seguito a perdita di confidenzialità, integrità e disponibilità delle informazioni;
- dell'intercettazione di situazioni che configurano possibili scenari di violazione dei dati personali;
- del ripristino della normale operatività, temporaneamente anche ad un livello minimale di erogazione dei servizi eventualmente impattati;
- della minimizzazione dell'impatto sui servizi e sui processi interni;
- del corretto flusso di comunicazione e di escalation interno al fine di garantire la corretta gestione, prevedendo il sistematico coinvolgimento dei ruoli e delle strutture adeguate alla gestione di incidente configurato particolarmente grave e che possa esporre l'ente comunale a un rischio significativo di tipo finanziario o reputazionale.

8 Ambito di applicazione

La presente procedura si applica a tutte le Informazioni Personali che sono raccolte o gestite o comunque trattate dal Comune di Milano, siano esse dati contenuti su dispositivi elettronici, accessibili via rete o web, contenuti su dispositivi mobili o portatili ovvero su supporti cartacei.

9 Ruoli e responsabilità

Ruolo	Responsabilità funzionali
Comitato di crisi	• Si riunisce per definire nel dettaglio gli elementi della violazione; • Fornisce supporto al Titolare per: - l'attività di assessment preliminare dell'incidente e di valutazione della sua incidenza sulle libertà e diritti degli interessati; - la definizione di una strategia di contenimento della violazione; - l'individuazione delle misure correttive per ridurre il rischio della reiterazione dell'incident; - La valutazione della sussistenza dei presupposti per la notifica al Garante e la comunicazione agli interessati. • Informa il Titolare sulle evoluzioni circa l'analisi condotta sulla violazione e sulla strategia di contenimento da adottare.
Dipendente	• Rileva l'evento anomalo, potenziale violazione; • Comunica, senza ingiustificato ritardo, la potenziale violazione rilevata al proprio Dirigente di riferimento, anche se la potenziale violazione non è relativa alla propria struttura di riferimento[3].
Dirigente di riferimento	• Riceve la comunicazione circa l'evento anomalo, anche relativo a strutture diverse dalla propria; • Comunica l'evento alla DSIAD e in particolare al Referente della Sicurezza Informatica. • Comunica l'evento al DPO; • Viene informato dal soggetto terzo dell'evento anomalo verificatosi; • Comunica l'evento al Responsabile della struttura in cui si è verificato l'evento, se diversa dalla propria; • Partecipa al Comitato di Crisi se l'evento ha colpito la sua struttura, nel caso di violazione informatica; • Relaziona il DPO circa gli eventi oggetto della violazione; • Compie la notifica del data breach al Garante, con il supporto del DPO, per le violazioni non informatiche; • Comunica agli interessati la violazione che li ha coinvolti; • Compila il Registro delle Violazioni in caso di incidente non informatico.

[3] Ad es.: nel caso in cui il dipendente si accorge che è stato aperto un armadietto ed è stata sottratta la documentazione di una struttura diversa da quella di sua appartenenza; nel caso in cui il dipendente trova per strada dei faldoni appartenenti a una Struttura del Comune diversa da quella i n cui lavora.

Responsabile della Protezione dei dati (Data Protection officer DPO)	• Riceve le comunicazioni relative alle presunte violazioni; • Partecipa al Comitato di Crisi; • Riceve la relazione da parte del Responsabile della Sicurezza Informatica e del Dirigente in merito alla violazione; • Esprime al Titolare, in base alla relazione acquisita e agli esiti emersi dalla valutazione di gravità, il proprio parere circa la necessità e/o l'opportunità di procedere con la notifica all'Autorità Garante e/o con la comunicazione agli interessati; • Collabora con il Dirigente di riferimento per la redazione della notifica nel caso di incidente non informatico;
Ruolo	**Responsabilità funzionali**
	• Collabora con il Dirigente di riferimento per la redazione della comunicazione agli interessati nel caso di incidente non informatico; • Verifica la corretta compilazione del Registro delle Violazioni, al termine del processo di gestione dei data breach.
Responsabile dei Sistemi Informativi	• Partecipa al Comitato di Crisi, anche per il tramite di un delegato; • Compie congiuntamente al Responsabile della Sicurezza Informatica la Valutazione della Gravità della violazione; • Notifica il data breach al Garante, con il supporto del Responsabile della Sicurezza Informatica e del DPO; • Invia la comunicazione agli interessati nel caso di violazione informatica
Responsabile della Sicurezza Informatica	• Riceve le comunicazioni relative alle presunte violazioni; • Indìce, senza ingiustificato ritardo rispetto a quando ha notizia della potenziale violazione, la riunione del Comitato di Crisi; • Partecipa al Comitato di Crisi, anche per il tramite di un delegato; • Relaziona al DPO in merito agli eventi oggetto di valutazione; • Compie congiuntamente al Responsabile dei Sistemi Informativi la valutazione della Gravità della violazione; • Compila il Registro delle violazioni in caso di incidente informatico
Titolare del Trattamento	Costituisce il soggetto a cui fanno riferimento le responsabilità complessive nell'ambito generale del principio di accountability (artt. 5 e 24 del Regolamento UE 2016/679) in ordine all'adempimento della normativa sulla protezione dei dati personali, anche con riguardo alla policy in oggetto.
Soggetto esterno	Comunica, senza ingiustificato ritardo, la potenziale violazione rilevata al Dirigente della Funzione con cui collabora o di riferimento.
Responsabile del trattamento	Comunica la violazione senza ingiustificato ritardo e comunque entro i termini previsti, se fissati contrattualmente.

10 Procedura di gestione dei data breach

Il processo di gestione delle violazioni dei dati personali seguirà due flussi differenti a seconda che si tratti di violazioni non informatiche o di violazioni informatiche.

In ogni caso, entrambi i flussi di gestione dei data breach si esplicano nelle seguenti fasi:

1. *Rilevazione;*
2. *Gestione e verifica;*
3. *Contenimento;*
4. *Valutazione della gravità;*
5. *Notifica al Garante e/o comunicazione agli interessati*
6. *Monitoraggio e reporting*

10.1 Gestione delle violazioni di natura informatica

Nel momento in cui si verifica un evento anomalo di natura informatica sarà necessario seguire il seguente processo.

10.1.1 Rilevazione della violazione

Chiunque può rilevare una violazione di dati personali: i dipendenti, i collaboratori del Comune a qualsiasi titolo, autorità, media, forze di polizia ecc….. I dipendenti e i collaboratori devono riferire tempestivamente al Dirigente di riferimento (Delegato del Titolare) ogni violazione o presunta violazione della sicurezza che possa riguardare i **dati personali**, qualora vi sia un ragionevole grado di certezza che si sia verificato un incidente di questo tipo.

La segnalazione di una violazione può avvenire in diversi modi, ad esempio per le violazioni informatiche: a.

segnalazione del SOC esterno[4];

b. allarme derivante dall'analisi automatica o manuale dei log di rete o applicativi;
c. indagine interna a seguito di segnalazione di malfunzionamento;
d. segnalazione di violazione dei dati supposta o fattuale sia da dipendenti che da altre fonti; e. segnalazione del DPO.

Il processo di gestione dei data breach ha inizio con la rilevazione e la segnalazione di evento, di una anomalia o di un malfunzionamento che potrebbero potenzialmente impattare sui dati personali trattati dal Comune.

La rilevazione della violazione può avvenire sia internamente (da parte del personale del Comune) sia esternamente (da parte di fornitori, collaboratori esterni, autorità, media, forze di polizia, ecc.…)

[4] Security Operation Center – Centro di gestione delle funzionalità di sicurezza della rete. Per il Comune di Milano è il SOC esterno dell'AGID.

Il termine di 72 ore per la comunicazione al Garante non decorre dalla presente fase in quanto il Titolare deve avere la ragionevole certezza che si tratti di una violazione di dati personali. . Pertanto, solo successivamente a tale fase e all'esito dell'istruttoria (che deve essere svolta senza indugio) che può aversi contezza se l'evento anomalo costituisca una violazione o meno[5] .

10.1.2 Rilevazione interna

Il dipendente che rileva o viene a conoscenza di un fatto potenzialmente configurabile come violazione deve tempestivamente, e senza ingiustificato ritardo, darne comunicazione al proprio Dirigente di riferimento, anche se non si tratta del Dirigente della struttura in cui si è verificato l'evento.
Il Dirigente di riferimento, con la collaborazione del Dipendente, dovrà fornire le seguenti informazioni:

- la natura della potenziale violazione dei dati personali interessati;
- le categorie e il numero approssimativo di individui i cui dati sono stati oggetto del potenziale data breach;
- ogni altra informazione volta ad individuare i dati oggetto del potenziale data breach e a mitigarne le conseguenze negative.

Se il Dirigente a cui è stato comunicato l'evento anomalo è di una struttura diversa da quella in cui esso si è verificato, quest'ultimo ne dà comunicazione al Responsabile della struttura in cui si è verificato.

Inoltre, il Dirigente di riferimento della struttura che ha subito l'evento lo comunica al DPO ed al Responsabile della Sicurezza Informatica che, senza ingiustificato ritardo, dovrà indire una riunione del Comitato di Crisi al fine di valutare e gestire l'evento verificatosi.

Successivamente si procederà secondo quanto indicato al paragrafo 10.1.5.

10.1.3 Rilevazione da parte di un soggetto terzo

Qualora qualsiasi soggetto terzo (fornitore, collaboratore esterno…) dovesse rilevare un fatto potenzialmente configurabile come violazione dei dati personali, dovrà tempestivamente darne comunicazione al Dirigente di riferimento della Funzione con cui collabora o di riferimento dei dati interessati dalla sospetta violazione, inviando una mail all'indirizzo nominale del Dirigente di riferimento o alla casella e-mail condivisa della Funzione.

Il Dirigente di riferimento, con la collaborazione del soggetto terzo, dovrà fornire le seguenti informazioni:

- la natura della potenziale violazione dei dati personali interessati;
- le categorie e il numero approssimativo di individui i cui dati sono stati oggetto del potenziale data breach;
- ogni altra informazione volta ad individuare i dati oggetto del potenziale data breach e a mitigarne le conseguenze negative.

Il Dirigente di riferimento che ha ricevuto la comunicazione procederà secondo quanto indicato nel 10.1.2.

10.1.4 Rilevazione da parte di un Responsabile del Trattamento

Nel caso in cui l'evento anomalo sia rilevato presso un Responsabile del trattamento, quest'ultimo dovrà darne comunicazione al proprio Dirigente di riferimento del Comune senza ingiustificato ritardo e comunque entro 12 ore, salvo la previsione di diversi termini contrattuali.

---

[5] "*Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza" "*, WP250 del Gruppo di Lavoro ex Art. 29

Il Dirigente di riferimento che ha ricevuto la comunicazione procederà secondo quanto indicato nel paragrafo 10.1.2.

10.1.5 Gestione e verifica della presunta violazione

Il titolare del trattamento,, nel corso della riunione, dovrà avviare l'attività di gestione della violazione e unitamente al Responsabile per la sicurezza informatica e al Responsabile dei servizi informativi, compiendo una valutazione più approfondita della stessa cercando di identificare se si tratta di una violazione di dati personali, soggetta ad obbligo di notifica ex art. 33 del Regolamento.

Pertanto, nel corso della riunione dovrà essere effettuata una valutazione preliminare volta a valutare:

a. se la segnalazione ricevuta corrisponde effettivamente a una violazione di dati personali; b. in caso affermativo

a. le caratteristiche della violazione e la strategia da implementare per il suo contenimento;

b. la gravità della violazione sui diritti e libertà degli interessati.

c. in caso negativo

a. procede con il normale processo di gestione degli incidenti

d. al termine della gestione dell'incidente si aggiorna comunque il Registro delle violazioni come indicato al paragrafo 13.

IlDirigente di riferimento, unitamente al Responsabile per la sicurezza informatica e al Responsabile dei servizi informativi, nel caso in cui rilevi l'effettiva violazione dei dati personali, avvia tempestivamente la fase di contenimento della violazione e, da tale momento si avviano anche le operazioni per la notifica della violazione all'Autorità Garante entro le 72 ore dall'avvenuta conoscenza dell'evento secondo quanto previsto dall'art. 33 del Regolamento (cfr.11.1.8.1)

Si ritiene che il Titolare possa acquisire un grado di ragionevole certezza[6] dell'avvenuta violazione dei dati personali in presenza di:

- informazioni concrete relative alla violazione dei dati personali;
- evidenze della perdita di confidenzialità, integrità, disponibilità dei dati personali;
- conseguenze sicuramente derivanti dall'incidente di sicurezza sui diritti e le libertà dei soggetti interessati.

Per quanto riguarda l'area di analisi di cui al punto b.->a., Il Dirigente di riferimento, unitamente al Responsabile per la sicurezza informatica e al Responsabile dei servizi informativi e col supporto del comitato di crisi dovrà esaminare i seguenti aspetti:

- definire le cause, la natura e la portata del data breach, la quantità, la tipologia e il numero di interessati a cui si riferiscono i dati personali oggetto della violazione, raccogliendo le informazioni eventualmente da notificare al Garante;
- analizzare le azioni già intraprese e identificare eventuali ulteriori azioni da intraprendere al fine di porre rimedio alla violazione dei dati personali e per attenuare i possibili effetti negativi;
- valutare il livello di gravità della violazione, come descritto nel paragrafo 10.1.7;

[6] "*Il titolare del trattamento ha stabilito con ragionevole certezza che si è verificata una violazione, qualora siano soddisfatte le condizioni di cui all'articolo 33, paragrafo 1…",* WP250 del Gruppo di Lavoro ex Art. 29.

- valutare la necessità di notifica al Garante e comunicazione agli interessati.

Il Dirigente di riferimento, col supporto del Comitato di Crisi dovrà successivamente valutare la gravità della violazione determinando il suo impatto sui diritti e le libertà degli interessati esaminando i seguenti elementi:

- Tipo di violazione;
- Natura, carattere sensibile e volume dei dati personali;
- Facilità di identificazione delle persone fisiche;
- Gravità dell'impatto sui diritti e le libertà delle persone fisiche;
- Probabilità del verificarsi di tale impatto;
- Caratteristiche particolari dell'interessato[7] ;
- Caratteristiche particolari del Titolare del Trattamento[8] ;
- Numero di persone fisiche coinvolte.

10.1.6 Contenimento della violazione

Dopo aver accertato l'effettiva violazione dei dati personali, illl Titolare del trattamento, unitamente al Responsabile per la sicurezza informatica e al Responsabile dei servizi informativi e col supporto del comitato di crisi, nel corso della riunione, dovrà avviare l'attività di gestione della violazione, definire ed implementare la strategia di contenimento e contrasto più efficace, finalizzata a minimizzare ogni ulteriore conseguenza tramite l'adozione di specifiche contromisure, tese ad evitare un peggioramento della situazione, nonché provvedere a ripristinare tempestivamente la disponibilità e l'accesso ai dati personali.

Qui di seguito sono indicate a titolo esemplificativo alcune misure di riduzione del rischio [9]:

- Monitoraggio costante dei possibili punti deboli delle tecnologie utilizzate;
- Protezione dei dati con un idoneo prodotto per la crittografia dotato di una chiave sufficientemente forte e segreta;
- Attribuzione a ciascun utente delle autorizzazioni di accesso ai propri account e ai dati personali applicando i principi di necessità di sapere e di privilegio minimo;
- Memorizzazione sicura delle password utilizzando tecniche adeguate.

A seguito di tale fase, il il Titolare dovrà informare il comitato di crisi riguardo l'effettività delle contromisure applicate all'incidente e riguardo l'evolversi della situazione

10.1.7 Valutazione della gravità della violazione

Successivamente alla conclusione della fase precedente e, di conseguenza, della riunione, il Titolare del trattamento, col supporto del Responsabile della Sicurezza Informatica invia una relazione al DPO descrivendo gli eventi intercorsi, gli eventi accertati e le contromisure da adottare, e, congiuntamente al Responsabile dei Sistemi Informativi, compie la valutazione del livello di gravità della stessa secondo le modalità descritte al

---

[7] Per caratteristiche dell'interessato si intendono le caratteristiche in base alle quali è possibile desumere informazioni ulteriori sull'interessato (ad es. l'elenco dei bambini che hanno richiesto una dieta alimentare in relazione a principi religiosi)

[8] Per caratteristiche particolari del Titolare del Trattamento si intende il contesto in cui i dati vengono trattati, dal quale è possibile trarre informazioni ulteriori rispetto a quelle che vengono desunte dai dati oggetto del trattamento (ad es. è possibile desumere dati particolari). Costituisce, pertanto, un elemento aggravante rispetto alla natura del Titolare. (ad es. dall'anagrafica delle famiglie che abitano nelle case-famiglia è possibile desumere elementi ulteriori circa dati particolari riferibili agli stessi).

[9] Per maggiori dettagli vedi "*Parere 03/2014 sulla notifica delle violazioni dei dati personali*", del Gruppo di Lavoro ex Art. 29 del 25 Marzo 2014. Al fine di definire le misure da applicare al caso concreto è necessario fare riferimento alle procedure di Incident Response e di Privacy by Design.

paragrafo 10.3 per giungere alla stima della gravità dell'impatto potenziale sugli interessati derivante dalla violazione dei dati.

10.1.8 Notifica al Garante e comunicazione agli Interessati

10.1.8.1 Notifica al Garante

Non appena il Titolare ha avuto la ragionevole certezza che si sia verificata una violazione dei dati, tramite il Responsabile dei Sistemi Informativi, col supporto del DPO e del Responsabile della Sicurezza Informatica, notifica al Garante l'evento, utilizzando l'apposita procedura on line sul sito internet del Garante Nazionale: Home (gpdp.it).

Nella stessa pagina, il Garante ha messo a disposizione una serie di istruzioni da seguire per la compilazione della procedura telematica, la firma e l'invio della notifica.

è possibile procedere alla notifica sia come utente NON autenticato, utilizzando la firma digitale, sia accedendo tramite le credenziali SPID/CIE. Dopo l'accesso si avvia la procedura guidata in cui si devono compilare tutti i campi richiesti ove interessati dal Data Breach.

Nel caso in cui si sia scelta la procedura di notifica utilizzando la firma digitale, una volta terminata la compilazione, il Titolare riceverà una mail con le istruzioni per completare la procedura, firmando digitalmente il pdf della notifica e caricandolo sul sito dell'Autorità secondo le istruzioni ricevute. Al fine di agevolare la notifica il Garante ha messo a disposizione un fac-simile cartaceo delle varie fasi della piattaforma (Vedi Allegati).

La notifica dovrà avvenire possibilmente entro 72 ore dall'avvenuta conoscenza della violazione. Nel caso di notifica oltre il suddetto termine la stessa dovrà essere corredata dai motivi del ritardo.

Nel caso in cui dall'esame si rileva un livello di gravità trascurabile o basso sussistono i presupposti per non effettuare la notifica al Garante, salva ogni altra valutazione in ragione del contesto, delle caratteristiche del caso specifico della violazione.

La notifica deve contenere:

- Tipologia di notifica;
- Dati del soggetto che effettua la notifica, del Titolare del Trattamento, dati di contatto del DPO o altro punto di contatto;
- Indicazione su ulteriori soggetti coinvolti (Responsabili del Trattamento o contitolari);
- Informazioni di sintesi sulla violazione (data in cui questa è avvenuta, data/ora e modalità in cui il titolare del trattamento ne sia venuto a conoscenza, motivazioni in caso di ritardo nella notifica, natura e causa della violazione, descrizione della violazione, descrizione dei sistemi-software-IT coinvolti nella violazione e loro ubicazione, misure tecniche ed organizzative in essere al momento della violazione, categorie di interessati coinvolti, n. anche approssimativo di interessati coinvolti, categorie di dati personali oggetto della violazione, numero anche approssimativo di registrazioni coinvolte, dettaglio dei dati personali coinvolti);
- informazioni sulle possibili conseguenze della violazione sugli interessati, l'impatto per gli interessati e la stima della gravità dell'impatto della violazione per gli interessati;
- Misure tecniche organizzative adottate per porre rimedio alla violazione e che si intendono adottare per prevenire future violazioni;
- Valutazione del rischio per gli interessati e informazioni circa la comunicazione agli interessati (il contenuto della comunicazione qualora questa fosse stata inviata o da inviare, nonché le motivazioni

dell'eventuale mancata comunicazione, il numero di interessati a cui è stata/verrà comunicata, il canale utilizzato);

- informazioni circa ulteriori circostanze rilevanti come il coinvolgimento nella violazione di Paesi Terzi o l'aver provveduto alla notifica della violazione ad altre Autorità.
- Eventuali allegati che si vogliono trasmettere all'Autorità Garante a corredo della notifica

Qualora entro 72 ore non si abbiano a disposizione tutte le informazioni richieste, è possibile adempiere all'obbligo di notifica tramite la **notifica preliminare**. Essa si ha nel caso in cui, a causa della complessità della violazione o della necessità di compiere ulteriori indagini, il Titolare del Trattamento fornisce alcune informazioni di contesto della violazione entro 72 ore, riservandosi di comunicare le informazioni mancanti in fasi successive mediante una notifica integrativa; in caso di notifica preliminare è possibile, quindi, con successiva/e notifica/che procedere a:

a) Fornire ulteriori informazioni senza completare il processo di notifica che andrà, quindi, chiuso con ulteriore notifica;
b) Fornire ulteriori informazioni e completare il processo di notifica
c) Completare il processo di notifica senza fornire ulteriori informazioni
d) Annullare una precedente notifica fornendo le adeguate motivazioni

Nel caso in cui, al contrario, si abbiano a disposizione tutte le informazioni necessarie è possibile procedere direttamente alla **notifica completa:** con tale accezione si identificano i casi in cui la notifica comprende tutte le informazioni richieste e non necessita di successive integrazioni.

10.1.8.2 Comunicazione agli Interessati

Nel caso in cui dalla fase di valutazione della gravità della violazione emerga un livello di rischio "Alto" o "Molto Alto" e, quindi, un rischio elevato per i diritti e le libertà degli interessati sarà necessario informare anche quest'ultimi.

Il Titolare, col supporto del comitato di crisi, comunica ai soggetti interessati la violazione informatica che li ha coinvolti entro tempi ragionevoli e senza ingiustificato ritardo [10].

La comunicazione dovrà contenere le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione agli interessati non risulta obbligatoria in determinati casi:

- il Titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche;
- contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. In tale circostanza il

[10] Secondo il WP250 del Gruppo di Lavoro ex art. 29 "Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile." Vedi anche considerando 86 del Regolamento EU 2016/679.

titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

10.2 Gestione delle violazioni di natura non informatica

Nel momento in cui si verifica un evento anomalo di natura non informatica sarà necessario osservare il flusso previsto per le violazioni di natura informatica (paragrafo 10.1), ad eccezione delle seguenti previsioni:

- Il Dirigente di riferimento, dopo essere venuto a conoscenza del fatto potenzialmente configurabile come violazione, dovrà darne comunicazione al DPO;
- Il Dirigente di riferimento, con il supporto del DPO, avvia l'attività di gestione e di verifica della presunta violazione e di contenimento della stessa;
- Il Dirigente di riferimento invia al DPO la relazione in cui vengono descritti gli eventi intercorsi, gli eventi accertati e le contromisure da adottare e, successivamente, compie la valutazione del livello di gravità della violazione secondo le modalità previste dal paragrafo 10.3;
- Il Dirigente di riferimento, con il supporto del DPO, provvede a notificare il Data Breach al Garante e, eventualmente, a darne comunicazione ai soggetti interessati.

10.3 Valutazione della gravità della violazione

Successivamente alla conclusione della fase di Contenimento, le figure preposte, secondo il tipo di violazione (informatica o non informatica), ne compiono la valutazione del livello di gravità.

Mediante tale valutazione si giungerà alla stima della gravità dell'impatto potenziale sugli interessati derivante dalla violazione dei dati [11].

Nella valutazione del livello di rischio ci si basa su tre criteri[12]:

1. **Contesto del Trattamento (CT):** il criterio tiene in considerazione la tipologia di dati personali coinvolti nella violazione dei dati in correlazione a fattori specifici del trattamento che potrebbero aggravare o attenuare l'impatto sul soggetto interessato (volume dei dati violati, circostanze specifiche del Titolare, circostanze specifiche del soggetto interessato, disponibilità pubblica del dato, accuratezza del dato). Al fine della corretta individuazione del punteggio dovrà essere considerato per il calcolo finale il valore massimo attribuito, che è compreso tra 1 e 4.
2. **Facilità di Identificazione (FI):** il criterio considera la possibilità di identificare puntualmente un soggetto sulla base del dato oggetto di violazione, considerando anche i casi di violazione contemporanea di più di una tipologia di dati dello stesso soggetto, che possano essere correlati per pervenire all'identificazione. Il criterio è utilizzato come valore correttivo del primo criterio, in quanto minore è il livello di identificabilità dell'individuo sulla base degli identificatori comuni, minore risulterà la gravita della violazione. Al fine della corretta individuazione del punteggio dovrà essere

[11] In base WP250 del Gruppo di Lavoro ex art. 29 viene stabilito che "… non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione; in secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate." Vedi anche considerando 75 e 76 del Regolamento Europeo n. 679/2016.

[12] Metodo definito all'interno delle "Recommendations for a methodology of the assessment of severity of personal data breaches " di ENISA

considerato per il calcolo finale il massimo fra i valori attribuiti a ciascun criterio, che è compreso tra 0 e 1.

3. **Circostanze della violazione (CV):** specifiche circostanze della violazione in correlazione alla categoria della violazione (perdita di integrità, riservatezza, disponibilità). Quando è presente tale elemento, potrebbe determinare l'aumento del valore di gravità della violazione. Per ogni elemento il valore attribuibile è compreso tra 0 e 0,50. La somma degli elementi aggravanti può determinare, quindi, un valore compreso tra 0 e 2.

Il valore della gravità della violazione viene determinato mediante l'utilizzo della formula:

GR (gravità) = CT * FI + CV

Il risultato che scaturisce dalla suddetta formula corrisponderà ad un determinato livello di gravità su 4 valori[13] indicati nella seguente tabella:

LIVELLO DI GRAVITA' DELLA VIOLAZIONE		
GR ≤ 2	**Trascurabile**	Gli interessati non saranno impattati o potrebbero incontrare alcuni lievi inconvenienti, superabili senza particolari problemi (tempo trascorso a reinserire informazioni, fastidi, irritazioni, ecc.).
2 ≤ GR < 3	**Basso**	Gli interessati possono incontrare notevoli disagi, che saranno in grado di superare pur con alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
3 ≤ GR < 4	**Medio**	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
4 ≤ GR	**Alto**	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Al fine della definizione dei punteggi da attribuire ai criteri di calcolo è necessario fare riferimento alla "*Tabella di valutazione*" (vedi "16 Allegati").

Una volta definito il livello di gravità, le figure preposte comunicano i risultati della valutazione al DPO, che svolgerà un ruolo consultivo in relazione all'applicazione della metodologia e al risultato emerso.

11 Comitato di crisi – verbalizzazione riunioni

Ad esito di ciascuna riunione del Comitato di crisi dovrà essere redatto apposito verbale che indichi:

- I partecipanti con le relative qualifiche;
- Una breve descrizione dell'evento o dell'incident verificatosi (cause, dati personali e numero degli interessati coinvolti), con indicazione della data in cui il Titolare ha informato i componenti del comitato;
- le misure di contenimento già adottate dal titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;

[13] I valori presenti nelle line guida di ENISA sono stati rimappati sulla base dei valori considerati dal Garante Privacy al fine di garantire la corretta compilazione della notifica in caso di Data Breach.

- le misure di sicurezza che il Titolare del trattamento intende adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- la tabella di valutazione della gravità;
- le conclusioni del titolare sulla necessità o meno della notifica all'Autorità garante e/o della comunicazione agli interessati.

Il testo del verbale dovrà essere sottoscritto dal Titolare del trattamento e trasmesso, nel caso di violazioni informatiche, al Responsabile della sicurezza informatica che si occuperà della sua archiviazione; nel caso di violazioni non informatiche, al DPO per l'archiviazione.

12 Gestioni delle violazioni miste

Nel caso in cui si verifichino contemporaneamente sia un incidente di natura informatica sia un incidente di natura non informatica sarà necessario osservare il flusso previsto nell'ipotesi di incidente informatico.

A differenza del flusso previsto per l'incidente informatico, la fase della valutazione della gravità della violazione richiederà il compimento delle seguenti azioni:

- Il Responsabile della Sicurezza Informatica congiuntamente con il Responsabile dei Sistemi Informativi compiono la valutazione della gravità della violazione informatica;
- Il Dirigente di riferimento compie la valutazione della gravità della violazione non informatica separata rispetto a quella realizzata dai Responsabili di cui sopra;
- Il Responsabile della Sicurezza Informatica, il Responsabile dei Sistemi Informativi ed il Dirigente di riferimento si confrontano tra di loro al fine di definire il livello di gravità complessivo delle violazioni verificatesi.

13 Monitoraggio e reporting

In osservanza dell'obbligo di accountability, il Titolare del Trattamento è tenuto a conservare tutte le informazioni e le evidenze relative alle violazioni dei dati che si sono verificate.

Pertanto, a prescindere dalla notifica o meno al Garante della violazione, sarà necessario inserire nel "Registro delle Violazioni" (vedi "16 Allegati") le informazioni relative ai data breach intervenuti.

Nel caso di incidente informatico provvederà il Responsabile della Sicurezza Informatica alla registrazione del data breach nel Registro delle Violazioni, mentre nel caso di incidente non informatico sarà compito del Dirigente di riferimento della struttura che ha subito la violazione procedere alla registrazione.

14 Registro delle Violazioni

Il registro delle violazioni dovrà contenere le seguenti informazioni:

- le modalità di rilevazione;
- soggetto che ha comunicato la violazione;
- data in cui il Titolare ne ha avuto effettiva conoscenza;
- una breve descrizione dell'evento occorso;
- l'indicazione della data/periodo della violazione e del momento della sua attestazione;
- l'indicazione del luogo in cui è avvenuta la violazione dei dati;
- la tipologia di violazione occorsa e la tipologia del dispositivo oggetto della violazione;

- una sintetica descrizione degli eventuali sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- il numero delle persone colpite dalla violazione;
- categoria di interessati coinvolti;
- l'indicazione della tipologia dei dati coinvolti nella violazione;
- natura e causa della violazione;
- conseguenze della violazione;
- volume dei dati personali interessati;
- descrizione della categoria dei dati;
- il livello di criticità della violazione;
- le misure e i controlli di sicurezza in essere applicati ai dati colpiti da violazione;
- le misure tecnologiche ed organizzative assunte per contenere la violazione dei dati e prevenire eventi simili futuri;
- se effettuata, la comunicazione agli interessati e l'indicazione del canale utilizzato per tale comunicazione;
- se effettuata, la notifica al Garante, la data in cui è stata inviata e la tipologia di notifica;
- eventuali motivi del ritardo nell'effettuazione della notifica al Garante;
- se la notifica della violazione è stata effettuata anche ad altri Organismi di vigilanza o controllo e/o ad Autorità Giudiziaria o di polizia.

Sono previsti due distinti Registri delle Violazioni: un Registro in cui verranno registrate le violazioni di natura informatica, detenuto dal Responsabile della Sicurezza Informatica, ed un Registro in cui verranno registrate le violazioni di natura non informatica, detenuto dal DPO.

Le violazioni miste (di natura informatica e non) verranno registrate nel Registro delle violazioni di natura informatica.

Il Registri sono tenuti costantemente aggiornati ed il DPO, nel proprio ruolo di sorveglianza della corretta applicazione del Regolamento, verifica la completezza e l'integrità delle informazioni ivi contenute.

15 Matrice RACI

Il presente paragrafo contiene la matrice RACI che fornisce il dettaglio delle responsabilità per ciascuna delle attività descritte nel presente documento.

Viene identificato:

- ***R**esponsible, la figura che svolge l'attività (è colui che esegue ed assegna l'attività);*
- ***A**ccountable*, la figura responsabile della adeguata esecuzione delle attività e che ne ha in carico l'approvazione finale (è colui che ha la responsabilità sul risultato dell'attività). A differenza degli altri 3 ruoli, per ciascun processo deve essere univocamente identificato;
- ***C**onsulted*, la figura che collabora allo svolgimento delle attività e con il Responsible per l'esecuzione dell'attività;
- ***I**nformed*, la figura che è tenuta informata del risultato delle attività e, dove appropriato, del loro stato.

RACI – Violazione informatica

Ruoli Attività	Titolare	DPO	Responsabile Sistemi Informativi	Responsabile Sicurezza Informatica	Dirigente di Riferimento	Dipendente	Terzo	Responsabile Esterno	Comitato di crisi (1)
Rilevazione della violazione	A					R	R	R	
Comunicazione interna della violazione	A				R	R	R	R	
Ricezione della comunicazione	A	R	I	R	R				
Convocazione del Comitato di crisi	A	I	I	R	C/I				
Gestione e assessment della violazione	A	C	R	R	R				C
Contenimento della violazione	A	C	R	R	R				C
Redazione della relazione per il DPO	A	I	R	R					
Analisi del livello di gravità della violazione	A	C	R	R	C				C
Notifica al Garante per la protezione dei dati	A	C	R	C	I				C
Comunicazione agli interessati	A	C	R						C
Aggiornamento e gestione del registro delle violazioni	A	I	I	R					
Verifica del registro delle violazioni	A	R							

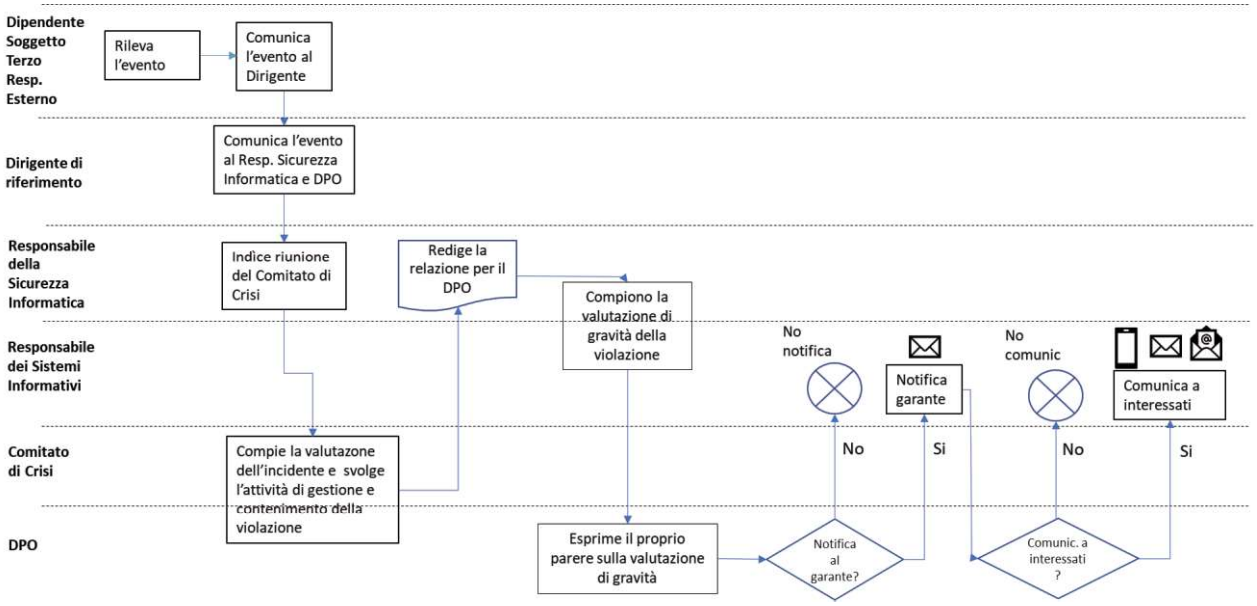
(*) Nella colonna relativa al Comitato di Crisi, per ogni attività, è riportato l'insieme dei ruoli assegnati per la stessa attività alle figure che siedono in Comitato.

RACI – Violazione non informatica

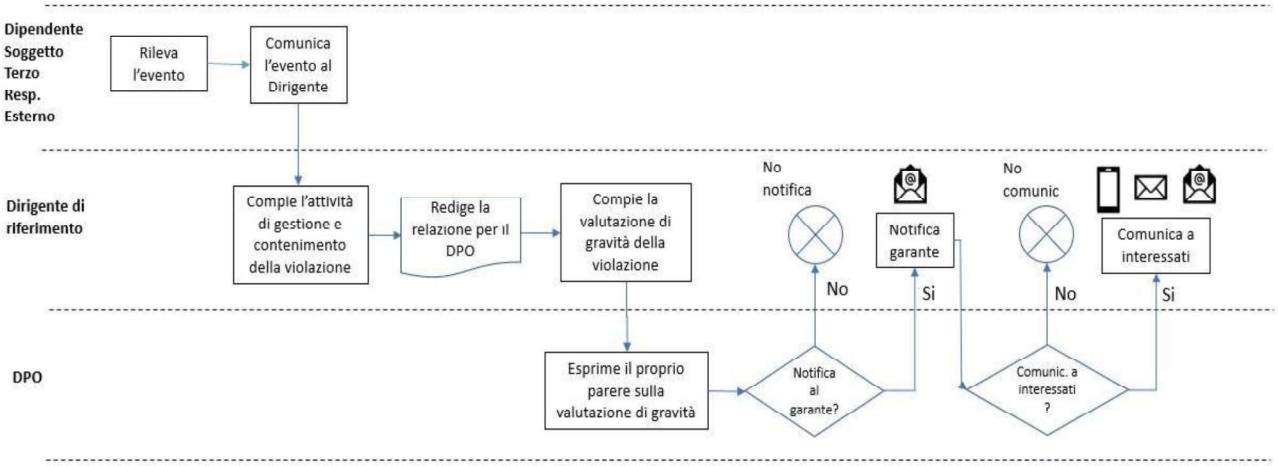
Ruoli / Attività	Titolare	DPO	Dirigente di riferimento	Dipendente	Soggetto terzo	Responsabile del Trattamento
Rilevazione della violazione	A			R	R	R
Comunicazione interna della violazione	A		R	R	R	R
Ricezione della comunicazione	A	R	R			
Gestione e assessment della violazione	A	C	R			
Contenimento della violazione	A	C	R			
Redazione della Relazione per il DPO	A	I	R			
Analisi del livello di gravità della violazione	A	C	R			
Notifica al Garante per la Protezione dei Dati Personali	A	C	R			
Comunicazione agli interessati	A	I	R			
Aggiornamento del registro delle violazioni	A	I	R			
Gestione del Registro delle Violazioni non informatiche	A	R				

16 Diagrammi di Flusso

16.1 Gestione delle violazioni informatiche



16.2 Gestione delle violazioni non informatiche



17 Allegati

ALLEGATO 1 – "TABELLA DI VALUTAZIONE"

ALLEGATO 2 – "FAC-SIMILE DEL MODELLO DI NOTIFICA DEL DATA BREACH"

ALLEGATO 3 – REGISTRO DELLE VIOLAZIONI

ALLEGATO 4 – MODELLO DI VERBALE