Piano
della
sicurezza informatica

Introduzione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dalla Pubblica Amministrazione per lo snellimento, l'ottimizzazione e la maggiore efficienza nella gestione dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità, l'integrità e la disponibilità dei dati, dei documenti e dei servizi. Tali rischi sono imputabili
a due fattori caratteristici della tecnologia in questione: la non garanzia del corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo
da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause". Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei documenti e dei servizi erogati. Nel definire un "sistema" di sicurezza informatica particolare attenzione è riservata agli aspetti organizzativi, in quanto la disponibilità di una struttura accuratamente gestita, in cui ruoli, funzioni e mansioni siano ben assegnati, riconosciuti e svolti, offre all'ente lo strumento fondamentale per contrastare la sempre più rapida evoluzione tecnologica delle minacce dirette al sistema informativo.

Una strategia globale prevede anche un'articolata serie di interventi procedurali e organizzativi, più in dettaglio:

- definizione di compiti e responsabilità
- indicazione dei corretti comportamenti individuali
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo
- gestione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la business continuity attraverso meccanismi di superamento di situazioni anomale
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute.

L'Ente individua con il presente piano le misure fisiche, logiche e organizzative necessarie ad assicurare la riservatezza nel trattamento di informazioni, dati e documenti, anche ai fini della trasmissione, disciplinando il comportamento degli utenti e dei sistemi che accedono al sistema informativo.

Obiettivi

Gli obiettivi del presente Piano e le attività correlate sono finalizzati a garantire che:

- il sistema informativo della struttura soddisfi i requisiti di disponibilità, integrità, autenticità e riservatezza deidati e documenti trattati al proprio interno e per quelli affidati all'esterno;
- i dati personali, di qualsiasi natura, vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazionealle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche deltrattamento.

Il presente piano della sicurezza informatica si struttura secondo un percorso specifico dove vengono individuati egestiti gli elementi fondamentali per la sicurezza informatica dell'Ente:

- asset da proteggere;
- vulnerabilità, minacce e rischi a cui è esposto il sistema informatico;
- politiche e misure di sicurezza.

Il presente Piano è soggetto a revisione con cadenza almeno biennale, in funzione dell'ampliamento del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

Riferimenti normativi

Il presente piano è redatto ai sensi delle Linee guida sulla formazione, gestione e conservazione dei documentiinformatici nell'attuazione delle quali le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT in vigore emanate dall'ACN.

Soggetti e responsabilità

Il modello organizzativo prescelto per la gestione della sicurezza informatica prevede l'individuazione di compiti eresponsabilità assegnati a soggetti interni ed esterni.

I ruoli e le responsabilità per la gestione della sicurezza informatica dell'ente sono riportati nella tabella seguente:

Ruolo	Soggetto	Attività di competenza
Responsabile transizione digitale	Dott.sa Federica Zanoni	Coordinamento del processo di transizione dell'Ente alla modalità operativa digitale e conseguente riorganizzazione dei processi interni
Amministratore di sistema	Gruppo Se.Co.Ges	• Aggiornamento, installazione e configurazione dei dispositivi hardware informatici. • Aggiornamento, installazione e configurazione dei sistemi operativi. • Aggiornamento, installazione e configurazione dei software applicativi standard da ufficio. • Risoluzione dei problemi e supporto tecnico ai dipendenti. • Creazione e gestione delle autorizzazioni di sistema e degli account utente dei dispositivi hardware. • Creazione e gestione delle autorizzazioni di sistema e degli account utente di dominio Active Directory. • Esecuzione di test di sicurezza regolari e monitoraggio della sicurezza. • Manutenzione e configurazione di reti. • Manutenzione e configurazione dei file systems di rete. • Gestione backup. • Gestione disaster recovery. • Gestione servizi posta elettronica ordinaria • Gestione ed implementazione policy di sicurezza del sistema informatico
Responsabile della gestione documentale	Silvia Papa	• Predisposizione e aggiornamento del manuale di gestione documentale e allegati tecnici • Adozione di criteri uniformi per la gestione informatica dei documenti • Monitoraggio dei processi e delle attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici • Verifica dell'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e dei protocolli diversi dal protocollo informatico • Produttore del PdV
Responsabile della conservazione	Silvia Papa	• Definizione e attuazione delle politiche complessive del sistema di

		conservazione e gestione del sistema con piena responsabilità • Redazione del Manuale di conservazione

Nel contesto del sistema informativo ogni dipendente dell'Ente collabora, secondo le proprie specifiche funzioni, alla gestione dello stesso e alla gestione generale della sicurezza.
La scelta dei fornitori/gestori esterni è effettuata anche in funzione del grado di sicurezza del servizio prestato, nel rispetto delle normative di settore.
È compito del responsabile preposto verificare gli standard di sicurezza garantiti dal fornitore/gestore esterno di servizi tra cui la presenza nel Cloud Marketplace (catalogo dei servizi Cloud qualificati da ACN per la PA).

Il sistema informativo e gli asset

La puntuale conoscenza delle figure coinvolte nella gestione informatica e del patrimonio informativo dell'Ente, ossia dell'insieme dei beni (materiali e immateriali) che costituiscono gli asset e che vanno pertanto protetti, rappresentano in generale la premessa indispensabile per la corretta gestione della sicurezza. Tale assunto vale in particolare per la gestione del rischio informatico, che quindi prende l'avvio dall'individuazione delle figure coinvolte e dal riconoscimento dei beni coinvolti nei processi informatici.
Il sistema informativo dell'Ente è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico, sia dal punto di vista delle esigenze provenienti dai servizi interni all'amministrazione stessa, sia provenienti dall'utenza esterna all'amministrazione.

Nell'uno e nell'altro caso l'esigenza può essere soddisfatta da:

- sistemi fisicamente residenti presso la struttura gestita dall'ente;
- sistemi esternalizzati resi disponibile da altri soggetti;
- sistemi ibridi.

Indipendentemente dalla configurazione in essere, l'ente mantiene e aggiorna i necessari inventari relativi alle risorse ICT.

Sono stati quindi predisposti inventari per i seguenti elementi

- *Asset hardware e virtuali*
  - Utilizzo software Lansweeper
- Asset software
  - Utilizzo software Lansweeper
- *Utenze amministrative:*
  - Firewall Watchgurad Municipio:
    admin, status
  - Accesso Dominio "Comune.local":
    administrator, mario.tonolini, alessandro.paneroni, dimitri.scuri, andrea.vidaletti, gianliuca.cavaglieri, luca.bonomi, marco.altemani. riccardo.masiero
  - Posta Office 365
    admin@comunecastrezzato.onmicrosoft.com
  - NAS Municipio:
    secoges
  - Host vmware:
    root (accesso web e console)
  - Switch HP
    admin (accesso web e console), root
  - Log amministratore :
    logroot

Politiche della sicurezza

La definizione e l'applicazione delle politiche di sicurezza all'interno dell'Ente richiede l'individuazione di un insieme di regole (policy) che fanno riferimento alle tecnologie, alle metodologie, alle procedure di
implementazione utilizzate e ad altri elementi specifici dell'ambiente e sistema informativo. Un sistema di sicurezza per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici eorganizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integratifra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.
L'organizzazione della sicurezza del sistema informativo richiede tipicamente una serie di attività a diversi livelli,
che si possono ricondurre a:

- definizione delle policy in tema di sicurezza informatica;
- valutazione dei rischi associati ai trattamenti di dati;
- verifica e controllo della corretta attuazione e dell'efficienza delle misure di sicurezza adottate (audit sullasicurezza);
- programmi di formazione in ambito sicurezza informatica.

Per garantire la sicurezza della struttura informatica dell'ente, i soggetti autorizzati possono monitorare gliapparati, i sistemi ed il traffico di rete in ogni momento. Per i motivi di cui sopra l'Ente si riserva il diritto di verificare l'attività dei dispositivi interessati per un determinato periodo anche al fine di assicurare la conformità alle politiche individuate.

Definizione delle policy in tema di sicurezza informatica

- Disattivazione esecuzione automatica strumenti removibili; (Group policy di dominio);
- Abilitato la scansione automatica dei dispositivi rimovibili con strumenti di sicurezza; Disattivato esecuzione di macro e script automatici; (Group policy di dominio);
- Disattivato anteprima dei file (Group policy di dominio);
- Abilitato screen saver;
- Abilitato blocco schermo con password temporizzato;
- Ogni postazione server e terminal server dispone di un antivirus locale gestito dalla console;
- Le postazioni inserite nel dominio dell'organizzazione, utilizzando credenziali di dominio non privilegiate;
- Su ogni postazione vengono installati tutti i software autorizzati necessari all'utente a cui verrà affidato, in base alle indicazioni del responsabile interessato;
- Su ogni postazione è attivo l'installazione di aggiornamenti automatici.
- Ad ogni nuovo dispositivo vengono applicate tutte le patch di sicurezza e aggiornamenti disponibili e dove possibile viene assegnato un indirizzo IP e un identificativo
- Le credenziali amministrative sono composte con password robuste, separate da quelle non amministrative e nominative per ogni apparato.

Al fine di garantire la sicurezza ed il corretto accesso ai sistemi informatici dell'Ente è necessario che ogni strumento
in uso, sia hardware che software, venga protetto da sistemi di autenticazione.
L'accesso ai sistemi informatici utilizzati dall'Ente è consentito agli incaricati dotati di credenziali di autenticazione, le quali permettono agli utenti di accedere alle risorse informatiche con differenti livelli di autorizzazione per consentirne la fruizione.
I profili di accesso sono definiti e gestiti dagli incaricati individuati interni e/o esterni in modo da garantire la sicurezza e l'ambito di accesso. L'accesso degli utenti, sia interni che esterni anche mediante portali, è realizzato con tecniche e procedure tali da garantire la sicurezza delle attività, dei documenti e del sistema informativo tramite:

- *Username e Password*
- *CNS*
- *SPID*
- *CIE*

L'organizzazione ha individuato le seguenti politiche che vengono implementate in ogni circostanza salvo diversa indicazione:

- *i sistemi di autenticazione composti da username e password possiedono le seguenti caratteristiche:*
  - *le credenziali sono nominative o comunque facilmente riconducibili all'utente utilizzatore;*
  - *le credenziali non sono condivise tra utenti diversi. In caso di comprovata necessità, la condivisione di credenziali deve essere autorizzata dalla figura individuata dall'organizzazione, notificata in forma scritta tramite mail nominativa dell'organizzazione al responsabile dei sistemi informativi e, se possibile, deve essere implementato un registro di utilizzo che renda imputabili eventuali accessi all'utente utilizzatore;*
  - *la password, se assegnata, viene modificata dall'utente al primo utilizzo;*
  - *la password è segreta e conosciuta solo dall'utente titolare delle credenziali;*
  - *la password è composta da almeno quattordici (14) caratteri;*
  - *la password contiene almeno 3 delle seguenti caratteristiche: una (1) lettera minuscola, una (1) maiuscola, un (1) numero ed un (1) carattere speciale;*
  - *la password non è facilmente riconducibile all'incaricato e non contiene informazioni personali facilmente individuabili da terzi (es. data di nascita, nome di familiari stretti ecc.);*
  - *la password non contiene porzioni dello username;*
  - *la password è sostituita periodicamente secondo congrue politiche in base ai dati accessibili: ogni sei (6) mesi se le credenziali permettono trattamento di dati di tipo comune, ogni tre (3) mesi se le credenziali permettono trattamento di dati di tipo particolare, giudiziari o comunque critici per l'organizzazione;*
  - *la medesima password non può essere riutilizzata per almeno dodici (12) sostituzioni;*
  - *la password non può essere sostituita dall'utente in maniera autonoma più di una (1) volta nell'arco di ventiquattro (24) ore.*

Datazione

L'ente utilizza un sistema data/ora standard che viene mantenuto sincronizzato sui client dai controller di dominio tramite protocollo NTP, gli stessi controller si aggiornano tramite server NTP esterni e pubblici al fine di gestire i riferimenti temporali per i sistemi informatici e documenti digitali.
Quale riferimento temporale opponibile a terzi utilizza prevalentemente quello contenuto nella segnatura di protocollo. Così come previsto dalla normativa di settore possono essere utilizzate laddove necessario anche le seguenti modalità:

- applicazione di marche temporali;
- riferimento temporale ottenuto attraverso la procedura di conservazione (invio nel sistema di conservazione).

Verifica e controllo attuazione, efficienza

L'adozione delle misure di sicurezza avviene mediante controlli periodici. Verranno valutate le policy definite e, se necessario, saranno implementate in modo specifico le relative misure di sicurezza in occasione di eventuali incidenti informatici, a fronte di cambiamenti derivanti da innovazioni per nuove procedure o funzionalità (aggiornamento software o hardware, ecc…).

I controlli vengono eseguiti localmente da un tecnico durante interventi fissati a non più di 6 mesi di distanza l'uno dall'altro.
Gli aggiornamenti dei sistemi sono, ove possibile, automatizzati e, in caso di necessità di aggiornamento critici di sistema o patch critiche dei vari software, tali aggiornamenti vengono svolti manualmente

Programmi di formazione in ambito sicurezza informatica

Sono pianificati interventi formativi e informativi al personale dipendente e, più in generale, agli utenti utilizzatori del sistema informativo dell'Ente al fine di garantire una maggiore consapevolezza delle tematiche in materia di sicurezza informatica.
La divulgazione della conoscenza dei rischi e delle correlative precauzioni per evitarli, definita come "cultura della sicurezza", è un elemento essenziale dello sviluppo dei servizi ICT. Man mano che i servizi diventano più complessi e pervasivi, man mano che le strutture informatiche surrogano quelle tradizionali, diventa sempre più necessario che tutti i soggetti interessati, adoperino le nuove tecniche con la stessa familiarità e cura con cui
utilizzano gli strumenti abituali. È bene sottolineare che quando si parla di "cultura della sicurezza" non si intende solo la coscienza del fatto che esistono problemi di sicurezza ma anche il possesso delle nozioni che consentono di prevenire, affrontare e risolvere questi problemi. Naturalmente queste nozioni dipendono dai contesti e dal ruolo delle parti interessate ma in ogni caso il bagaglio di conoscenze necessario per interagire con sistemi informatici deve comprendere i concetti essenziali della sicurezza. Per raggiungere questo obiettivo, è in generale necessaria una capillare azione di sensibilizzazione e responsabilizzazione. Tutto il personale concorre alla realizzazione della sicurezza, pertanto, dovrà proteggere le informazioni assegnate loro per lo svolgimento dell'attività lavorativa nel rispetto di quanto stabilito dalle politiche per la sicurezza.

Procedure di archiviazione dati

Dati e documenti informatici di qualsiasi genere inerenti le attività lavorative sono conservati nelle aree di archiviazione dedicate su dispositivi appositamente predisposti. Tutti i file dell'organizzazione inerenti le attività lavorative devono essere conservati nelle aree di competenza definite dall'Ente.
Le aree di archiviazione disponibili sono correttamente suddivise e profilate in modo da garantire l'accesso esclusivamente a quelle necessarie per l'espletamento delle funzioni lavorative. Le medesime modalità di profilazione vengono contemplate ed implementate per ogni strumento informatico a disposizione del personale, sia hardware che software.

Per tutti gli strumenti utilizzati in modalità as a service le procedure sono definite in accordo con il rispettivo fornitore che dovrà garantire la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi.

Procedure di backup e disaster recovery

Al fine di garantire il recupero dei dati in caso di evento imprevisto, vengono eseguiti dei backup delle banche dati dell'organizzazione.

Nel dettaglio vengono eseguiti:

- *Modalità di Backup:*
  Il backup avviene con frequenza giornaliera, i dati vengono mantenuti per trenta (30) giorni.

- *Modalità di Disaster recovery:*
  NO

Per tutti gli strumenti utilizzati in modalità as a service le procedure sono definite in accordo con il rispettivo fornitore che dovrà garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai servizi e/o dati e documenti in caso di incidente fisico o tecnico.

Gestione dei Log

Il metodo principale per effettuare il monitoraggio dei sistemi fisici, operativi e applicativi è costituito dalla raccolta ed analisi dei file di "log" (log file), cioè file in cui i software/apparati installati, i sistemi operativi e le applicazioni scrivono tutte le principali operazioni svolte dagli utenti per loro tramite. Attraverso l'analisi dei log, effettuata tipicamente adottando strumenti automatici di reportistica e di sintesi, è possibile individuare, adesempio, i tentativi riusciti o meno di accesso al sistema e, più in generale, l'esecuzione di operazioni sospette o non appropriate.

Gli strumenti informatici dell'organizzazione sono dotati di un log eventi, accessibile solo al personale dotato di credenziali amministratore.

Log Amministratori, sistemi, server e applicativi

In relazione al Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre2008" e successive modifiche, con la definizione di "amministratore di sistema" si individuano generalmente,
in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento citato vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi didati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioniche implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni
e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecnichequali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quandol'amministratore non consulti "in chiaro" le informazioni medesime.

Gli strumenti in cui vengono archiviati dati di proprietà dell'organizzazione sono dotati di log amministratore inottemperanza alla normativa vigente.

Azioni di monitoraggio e audit

La verifica dell'efficacia e della validità nel tempo delle misure di sicurezza adottate è punto fondamentale di tutto il processo per la sicurezza dei Sistema Informativo Aziendale. In un contesto tecnologico in rapidissima evoluzione, è necessario avere le massime garanzie circa l'adeguatezza delle misure di sicurezza adottate nei confronti del sempre più vasto, articolato ed aggiornato panorama delle minacce possibili. Per quanto sopra le attività di verifica consistono in due attività distinte, sia per compiti, che per organizzazione. La prima, il monitoraggio, è l'attività di verifica continua della efficacia delle misure di sicurezza realizzate ed è effettuata, sotto la responsabilità della struttura che progetta e realizza le misure di sicurezza, durante la progettazione, implementazione ed esercizio delle misure stesse. La seconda, audit di sicurezza, è un'attività di verifica alla struttura che ha implementato le misure di sicurezza, e potrà avvenire in modo estemporaneo e non prevedibile. L'Ente si è posto l'obiettivo di potenziare il controllo continuo delle misure di sicurezza, per poter intercettare eventuali attacchi ai danni del sistema nel minor tempo possibile.

Il comune attualmente non ha implementato alcun sistema di audit o Vulnerability assessment.

Gestione delle anomalie e incidenti informatici

La gestione delle anomalie e degli incidenti hanno l'obiettivo di risolvere il più velocemente ed efficacemente possibile un evento che impatta, più o meno gravemente, sulla sicurezza, riservatezza, disponibilità e integrità di dati, documenti e servizi dell'Ente.
Si intende "anomalia" un qualsiasi evento non previsto che:

- abbia impatto limitato sui servizi e che non causi blocco di operatività e/o perdita o degrado di informazioni;
- si riferisca all'operatività di un singolo utente o di un gruppo esiguo di utenti;
- sia risolto in maniera automatica dai controlli tecnologici messi in campo e non richieda altri interventi manuali per il suo ripristino.

Sono esempi di anomalie segnalazioni di aggressioni da virus informatico rimosse automaticamente dal software antivirus; interruzioni temporanee di alimentazione coperte dall'UPS; guasti singoli ai PC degli utenti o qualsiasi segnalazione di malfunzionamento limitata al singolo utente; tracce di attacco rilevate dal firewall o dai proxy ma senza impatto sui servizi; comportamenti anomali di una stazione, di un utente o di un servizio ma senza impatti sull'infrastruttura.
Le anomalie sono considerate eventi comuni e inevitabili nella normale operatività del sistema.
L'anomalia o punto di debolezza può essere rilevata automaticamente dal sistema o segnalata dagli utenti al personale incaricato, che provvederà ad analizzarla e interverrà se necessario.
L'anomalia deve essere archiviata nel sistema di log automatico dello strumento tecnico impiegato per la sua gestione oppure mantenendone evidenza tramite ulteriori strumenti a disposizione.

Si intende "incidente" un qualsiasi evento non previsto che:

- incida sulla funzionalità completa di uno o più servizi;
- comporti superamento dei sistemi di sicurezza perimetrali o di protezione da virus informatici, con conseguente grave rischio di compromissione dei requisiti di sicurezza delle informazioni;
- richieda l'intervento delle forze dell'ordine;
- causi la permanenza dell'infrastruttura per periodi prolungati in condizioni di potenziale rischio.

Sono esempi di incidente la rilevazione di un accesso non autorizzato a locali tecnologici; l'attacco diffuso da virus informatici non rimosso dal sistema antivirus; il blocco prolungato di parte di un sistema ridondato, tale per cui ne resti in linea solo una delle due repliche; intrusioni nella rete interna o compromissione dei servizi informatici;
anomalie ripetute sistematicamente o che coinvolgano un ampio numero di utenti o che impattino potenzialmente su dati particolari, giudiziari o comunque critici per l'organizzazione.
Devono essere identificate le cause, definite le modalità di risoluzione tempestiva dell'incidente predisponendo un piano di intervento che preveda attività da porre in essere, incaricati, tempistiche e risorse. Devono inoltre essere individuati gli eventuali fattori che potrebbero causare il ripetersi dell'incidente.
L'incidente può essere considerato risolto solo trascorso un tempo ragionevole dal ripristino del servizio per la verifica dell'efficacia dell'intervento (il non ripetersi dell'incidente, l'analisi di eventuali ripercussioni non previste, la verifica del mantenimento dei parametri di normalità).

In caso si verifichi una violazione dei dati personali è necessario attivare la procedura di gestione data breach.

Procedure da adottarsi in caso di violazione di dati personali

Per data breach, ovvero nella versione italiana del GDPR "violazione dei dati personali", si intende 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.
Il Regolamento Europeo prevede che, in caso di violazione dei dati personali, il titolare del trattamento debba notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personalipresenti un rischio per i diritti e le libertà delle persone fisiche.

I casi in cui sarà necessario applicare la presente procedura sono, a titolo esemplificativo e non esaustivo i seguenti:

- sottrazione di credenziali di autenticazione;
- furto di PC, Notebook, Tablet, Smartphone contenente dati personali;
- erronea diffusione, pubblicazione, comunicazione di dati personali;
- intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali;
- furto di archivi cartacei e/o digitali;
- accesso non autorizzato nel sistema informativo;
- azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza logiche a protezione dellarete informatica;
- smarrimento di dati personali (archiviati su supporti cartacei e digitali);
- distruzione di dati personali (archiviati su supporti cartacei e digitali).

PROCEDURA IN MATERIA DI *DATA BREACH*

DEFINIZIONI

- GDPR o RGPD - Regolamento Europeo in materia di protezione dei dati personali nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia. Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, entrato in vigore il 24/05/2016 ed è diventato definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25/05/2018.
- Codice: Codice nazionale in materia di protezione dei dati personali (D.Lgs. n. 196/2003) modificato (con il D.Lgs. n. 101/2018) per essere conforme al GDPR.
- Garante: Garante per la protezione dei dati personali, quale autorità amministrativa pubblica di controllo indipendente, identificata dal GDPR come "Autorità di controllo" (vedasi artt. n.ri 51 e successivi del GDPR).
- Titolare: Titolare del trattamento, ossia il Comune di **Padenghe sul Garda**, che determina finalità e mezzi del trattamento di dati personali.
- Responsabile: Responsabile del trattamento, ossia il soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.
- *Data breach*: l'evento che cagiona una "violazione dei dati personali", ossia la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- *Accountability*: principio in forza del quale il Titolare è tenuto a dimostrare l'adozione di politiche privacy e misure tecniche e organizzative adeguate in conformità al GDPR.

- *Privacy by design*: principio in forza del quale le misure tecniche e organizzative adeguate devono essere adottate dal Titolare oppure dal Responsabile sin dal momento della progettazione dell'attività di trattamento, che deve risultare adeguata al GDPR in ogni suo aspetto.
- *Privacy by default*: principio in forza del quale si deve attuare il principio della minimizzazione, raccogliendo e successivamente trattando esclusivamente i dati personali strettamente necessari allo svolgimento dell'attività di trattamento.
- WP29: gruppo di lavoro istituito in virtù dell'art. n. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata), oggi sostituito dall'European Data Protection Board (EDPB).

IL *DATA BREACH* IN GENERALE

Ai sensi dell'art. 4, par. 1, n. 12 GDPR la violazione di dati personali è "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*". Per *Data breach*, perciò, sostanzialmente si intende un evento che causa un incidente di sicurezza in cui dati (siano essi personali, particolari, giudiziari, genetici, biometrici) vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato; altra ipotesi di *data breach* si verifica quanto i dati di cui sopra vengono danneggiati in tutto o in parte, bloccati e/o resi comunque inservibili oppure diffusi in un ambiente privo di misure di sicurezza in maniera involontaria o volontaria.

L'art. 33 del GDPR impone al Titolare del trattamento di **notificare all'Autorità di controllo** la violazione di dati personali **entro settantadue ore** dal momento in cui lo stesso ne viene a conoscenza. Tale termine non è perentorio: in caso di superamento, però, in sede di notifica è necessario **giustificare i motivi del ritardo** (art. 33, par. 1, GDPR).

La notifica al Garante, peraltro, non è necessaria qualora risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (paragrafo n. 1).

Il mancato rispetto dell'obbligo di notifica, invece, legittima il Garante ad applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la comminazione di sanzioni amministrative (secondo l'art. 83 GDPR, l'importo può arrivare a € 10.000.000 per un Ente pubblico).

La mancata notifica può inoltre dare luogo ad ulteriori accertamenti da parte del Garante, in quanto può rappresentare un indizio di carenze più profonde e strutturali che - se accertate - possono dar luogo ad ulteriore irrogazione di sanzioni.

D'altra parte, nel caso in cui la violazione dei dati sia suscettibile di cagionare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve **comunicare la violazione all'interessato** senza ingiustificato ritardo (art. 34, par. 1, GDPR).

Tutti i *data breach*, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati dal Titolare dando atto delle circostanze, delle conseguenze e dei provvedimenti adottati (art. 33 par. 5 del GDPR) su un registro tenuto, per estensione, secondo le indicazioni fornite dal Garante con il provvedimento n. 393 del 02/07/2015 (GU n. 179 del 04/08/2015 - doc. web n. 4129029). Quanto esposto anche in ossequio al

principio della *accountability*.

UNA DEFINIZIONE PIU' APPROFONDITA DI *DATA BREACH*

Ai sensi dell'art. 4, par. 12, GDPR il *data breach* (più correttamente indentificato con l'espressione "violazione di dati") viene definito come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

In particolare, si intende un evento in grado di provocare danni fisici, materiali o immateriali alle persone fisiche (perdita di controllo dei dati personali, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, danni economici o sociali, ecc.).

Per *data breach* si intende dunque il verificarsi di eventi quali: la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati.

Non è corretta quindi l'identificazione del *data breach* con l'attacco informatico, in quanto anche la distruzione o la perdita dell'accesso ai dati personali a seguito di eventi indipendenti dalla volontà del Titolare, del responsabile oppure di un terzo costituisce una violazione di dati. Si pensi al caso, tipico, di guasto che colpisca il sistema informatico del Titolare - in particolare i dispositivi di storage ove vengono salvati i dati trattati - in assenza di misure adeguate (come un sistema di backup) a permettere il loro recupero. Inoltre, il *data breach* può avere ad oggetto anche dati conservati in formato cartaceo: si pensi al furto di un archivio cartaceo oppure, ancora, ad un incendio che distrugga tale archivio senza che sia possibile ricostruirlo (ad es. perché si ha una seconda copia dei relativi documenti, in formato cartaceo o elettronico).

LE REGOLE DA OSSERVARE

Poiché un *data breach* può presentarsi in forme molto differenti, le regole di cui al presente documento non devono essere intese come tassative: esse, infatti, hanno la finalità di fornire al Titolare un esempio, o più propriamente un *modus operandi* corretto, per la gestione di una violazione di dati. Al contempo, invece, è necessario seguire in modo rigido le tempistiche e le ulteriori indicazioni procedurali che possono essere desunte dal GDPR.

LE SINGOLE FASI DEL PROCESSO DI GESTIONE DEI *DATA BREACH*

Di seguito una elencazione delle singole fasi che compongono una procedura corretta di gestione del *data breach*.

1. Acquisizione

La prima fase nella gestione del *data breach* è sicuramente quella che porta il Titolare a conoscenza della violazione (o presunta violazione) di sicurezza. Essa può comportare che il Titolare venga direttamente a conoscenza del *data breach* - attraverso la propria struttura o da terzi, come la Polizia Postale - oppure che tale soggetto venga informato da uno dei Responsabili esterni della violazione. Può accadere, inoltre, che il Titolare venga a conoscenza della violazione a seguito di una segnalazione da parte dell'interessato; ciò può verificarsi, ad es., nel caso in cui quest'ultimo sia stato contattato da truffatori informatici che abbiano previamente sottratto i suoi dati al Titolare. Per garantire che il Titolare possa

svolgere nel modo più completo le fasi successive di gestione del *data breach* è necessario che la segnalazione della violazione sia sufficientemente precisa e circostanziata: identificazione dei segnalatori, ricezione dei dati di contatto dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata, ecc..

Se la segnalazione proviene direttamente dall'interessato per la redazione dell'informativa dovrà essere osservato quanto disposto all'art n. 13 GDPR; al contrario, nel caso in cui i dati non siano ottenuti direttamente dall'interessato si dovrà seguire quanto previsto al successivo art. 14 GDPR. Si consideri, comunque, che nella fase dell'acquisizione è opportuno limitare la raccolta di eventuali categorie particolari di dati a quelli che risultino strettamente necessari per la gestione del *data breach*.

Se la segnalazione perviene a un Responsabile esterno (ossia il soggetto incaricato di eseguire un trattamento o parte di esso per conto del Titolare), quest'ultimo deve darne immediata comunicazione al Titolare.

Chi raccoglie la segnalazione dovrà inoltre fornire al segnalante un'informativa circa le modalità e finalità con cui i dati conferiti saranno trattati, ai sensi:

- dell'art. n. 13 GDPR se i dati sono forniti e raccolti direttamente dall'interessato (l'informativa deve essere resa al momento in cui sono ricevuti i dati personali);
- dell'art. n. 14 GDPR se i dati non sono raccolti direttamente dall'interessato (l'informativa deve essere resa entro un termine ragionevole, ma al più tardi entro un mese dall'ottenimento dei dati).

Nel caso in cui la segnalazione venga raccolta da un responsabile esterno, immediatamente dopo la ricezione della segnalazione è necessario che lo stesso provveda al suo inoltro al Titolare.

2. Gestione tecnica del *data breach*

Facendo riferimento al concetto di gestione tecnica si intende l'esecuzione di tutte le operazioni, gli accertamenti e le verifiche necessari ad acquisire gli elementi sui quali fondare la successiva fase di valutazione.

Il soggetto responsabile della fase di gestione tecnica è il Titolare: esso deve concludere nel più breve tempo possibile gli adempimenti di gestione tecnica, per dedicare il tempo necessario al primo processo decisionale, all'esito del quale deciderà se eseguire le eventuali notifiche e comunicazioni entro i termini previsti.

Come sopra esposto questa fase deve concludersi nel più breve tempo possibile, anche se il Titolare non è riuscito a determinare tutti gli elementi utili, pur avendo appurato l'esistenza della violazione: le ulteriori verifiche, infatti, potranno eventualmente proseguire dopo le valutazioni preliminari (che richiedono celerità, dati gli stringenti termini previsti dal GDPR) del Titolare.

La fase di valutazione tecnica potrebbe articolarsi nelle sotto-fasi seguenti:

a) Attivazione: una volta ricevuta la segnalazione della presunta violazione il Titolare incarica i soggetti competenti (ad es. nell'Ente l'amministratore di sistema oppure un esperto esterno) di eseguire la fase di valutazione tecnica.

b) Analisi preliminare: la sotto-fase basata sulle risultanze di quella indicata al precedente punto 1. E' finalizzata ad appurare se la violazione segnalata esiste e, in caso affermativo, se è qualificabile come *data breach*.

c) Analisi approfondita: una volta conclusa in senso affermativo l'analisi preliminare di cui al punto b) precedente, deve essere identificata puntualmente la tipologia di violazione

verificatasi, seguendo le categorie indicate del WP29:

i. violazione di riservatezza (quando si verifica una divulgazione o un accesso ai dati non autorizzato o accidentale);

ii. violazione di integrità (quando si verifica un'alterazione di dati personali non autorizzata o accidentale);

iii. violazione di disponibilità (ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate).

A seguito dell'analisi approfondita, nella successiva fase di valutazione, si dovrà decidere se la violazione determina o meno l'obbligo di notifica e/o comunicazione.

Il fac-simile del modello di notifica predisposto dal Garante (da non utilizzare, come si vedrà, in quanto dal 01.07.2021 deve essere seguita esclusivamente la procedura online) è allegato al presente documento, al pari di una bozza di comunicazione agli interessati.

d) Eventuale analisi approfondita supplementare: essa viene attivata se è necessario acquisire informazioni aggiuntive, ad esempio a fronte di richieste/indicazioni del Garante oppure delle Forze dell'Ordine.

3. Valutazione

Il Titolare in questa fase è chiamato a decidere se è necessario (oppure opportuno):

- notificare la violazione al garante;
- comunicare la violazione agli interessati (art. 34 GDPR);
- comunicare la violazione alle Forze dell'Ordine.

In ogni caso occorre registrare l'evento analizzato documentando la violazione dei dati personali, le circostanze ad essa relative, le sue conseguenze e le valutazioni eseguite: si può usare il modello di registro dei *data breach* allegato al presente documento.

4. L'eventuale notifica al Garante e la comunicazione agli interessati

Come sopra visto, la notifica di una violazione al Garante è resa obbligatoria dall'art. 33 GDPR nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti rischi per i diritti e le libertà delle persone fisiche.

A partire dal 01.07.2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.

Il paragrafo n. 3 dell'art. 33 sopracitato definisce il contenuto minimo della notifica, che deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nella presente fase, come sopra visto, il Titolare deve altresì operare la comunicazione della violazione di dati personali agli interessati, ove nella fase precedente sia stata rilevata la presenza dei relativi requisiti. Un modello di comunicazione è allegato al presente documento.

5. Registrazione delle violazioni

Come sopra visto, ai sensi dell'art. 33, par. 5, GDPR, il Titolare è tenuto a documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Ciò significa che le attività svolte nelle fasi precedenti (di scoperta dell'incidente, gestione tecnica, valutazione, notifica, comunicazione) come quelle successive, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Il WP29 nelle proprie linee guida ha perentoriamente sottolineato che il Titolare del trattamento è tenuto a documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, al fine di poter dimostrare la conformità al GDPR. Il Titolare del trattamento deve perciò registrare i dettagli relativi alla violazione, comprese le circostanze, le sue conseguenze e i provvedimenti adottati per porvi rimedio (art. 33, par. 5, GDPR).

Il GDPR non specifica un periodo di conservazione di tale documentazione. Qualora tali registrazioni contengano dati personali, spetta al Titolare del trattamento determinare il periodo appropriato di conservazione conformemente ai principi relativi al trattamento dei dati personali e indicare la relativa base giuridica per il trattamento. Nel caso di Ente pubblico, giova ricordare che i dati raccolti o comunque trattati per la gestione del *data breach* devono essere conservati sino all'esperimento, da parte dell'Ente, della procedura di scarto ai sensi degli artt. 61 e ss. del D.P.R. n. 445/2000 e dell'art. 21 co. I lett. d) del D.Lgs. n. 42/2004.

Un modello di registro dei *data breach* (o più correttamente degli eventi) è allegato al presente documento.

Allegati:

1. fac-simle di procedura per la notifica al Garante (allegato in calce);
2. modello per la comunicazione agli Interessati;
3. registro dei *data breach*.

1. MODELLO DI COMUNICAZIONE DEL *DATA BREACH* AGLI INTERESSATI AI SENSI DELL'ART. 34 GDPR

Egregio Signore/Gentile Signora

Via _____

_____ - _____ (__)

A mezzo _____

_____, *Li* _____

OGGETTO: Comunicazione agli interessati di una violazione di dati ai sensi dell'art. 34 del Regolamento UE 2016/679

Egregio/Gentile _____

con la presente Le comunichiamo che, purtroppo, abbiamo accertato che presso il nostro Ente si è verificata una violazione di dati personali che ha riguardato, tra gli altri, anche i Suoi dati.

La violazione ha avuto ad oggetto i nostri archivi cartacei/i nostri sistemi informatici ed è stata causata da _____. La violazione ha comportato che soggetti esterni hanno potuto consultare/estrarre copia dei Suoi dati/che i Suoi dati non sono più nella nostra disponibilità, in quanto irrimediabilmente danneggiati/cancellati.

I suoi dati che sono stati oggetto della violazione sono i seguenti: _____.

La violazione di dati sopra descritta presenta i seguenti rischi per i Suoi diritti e le Sue libertà _____; i nostri tecnici informatici e i nostri esperti legali, oltre alle Forze dell'Ordine, sono infatti già al lavoro per minimizzare le conseguenze negative che Lei potrebbe patire a causa della citata violazione. Per contenere ulteriormente i rischi per i Suoi diritti e le Sue libertà Le suggeriamo di adottare le seguenti misure: _____.

Come previsto dall'art. 33 del Regolamento UE 2016/679 abbiamo già notificato la violazione al Garante per la protezione dei dati personali.

Per impedire che possa nuovamente verificarsi una violazione di dati personali i nostri tecnici informatici/i nostri esperti legali sono inoltre al lavoro per implementare le seguenti misure di sicurezza: _____. Esse vanno ad aggiungersi a quelle già in precedenza adottate, per elevare gli standard di sicurezza del nostro Ente.

Ci scusiamo enormemente con Lei per ogni disagio che dovesse derivarLe dalla violazione di cui alla presente, ma Le garantiamo che stiamo ponendo in essere ogni sforzo possibile per mitigare ogni conseguenza dannosa ed evitare, se possibile, qualsiasi problematica che potrebbe verificarsi per Lei.

Potrà fare riferimento ai nostri dati di contatto per ogni richiesta di chiarimento o spiegazioni ulteriori in merito all'accaduto.

In alternativa, potrà contattare il nostro Responsabile della Protezione dei Dati personali, per ottenere ogni chiarimento o spiegazione in merito a quanto verificatosi.

Responsabile della Protezione dei Dati: **dott. Gilberto Ambotta**

Contatti e recapiti:

Cellulare	3291215005
E-mail	privacy@gaservice.info
PEC	gilberto.ambotta@mailcertificata.it

Cordiali saluti.

Per il Comune di Padenghe sul Garda

Il Sindaco **dott. Albino Zuliani**

2. REGISTRO DEI DATA BREACH

EVENTO 1

(*) Tutti i campi sono obbligatori

DATA E ORA	
SEGNALANTE	
LUOGO VIOLAZIONE	
ENTE COINVOLTO	
MODALITA DELLA VIOLAZIONE	
TIPOLOGIA DI VIOLAZIONE	
SISTEMI IMPATTATI	
TIPOLOGIA DI DATI IMPATTATI	
NUMERO DI UTENTI INTERESSATI DALLA VIOLAZIONE	
TEMPO DI RIPRISTINO DEL SERVIZIO	
EFFETTI E LE CONSEGUENZE DELLA VIOLAZIONE	
ORGANI INFORMATI inserire DESTINATARIO DATA E ORA	
AZIONI EFFETTUATE/PIANO DI INTERVENTO	
DECISIONI ASSUNTE (SOLO SE TITOLARE) **Motivare SE:** **IL TITOLARE HA DECISO DI NON PROCEDERE ALLA NOTIFICA** **IL TITOLARE HA RITARDATO NELLA PROCEDURA DI NOTIFICA** **IL TITOLARE HA DECISO DI NON NOTIFICARE IL DATA BREACH AGLI INTERESSATI**	
RIFERIMENTI TRACCIATURA	
DATA DI CHIUSURA	

EVENTO 2

(*) Tutti i campi sono obbligatori

DATA E ORA	
SEGNALANTE	
LUOGO VIOLAZIONE	
ENTE COINVOLTO	
MODALITA DELLA VIOLAZIONE	
TIPOLOGIA DI VIOLAZIONE	
SISTEMI IMPATTATI	
TIPOLOGIA DI DATI IMPATTATI	
NUMERO DI UTENTI INTERESSATI DALLA VIOLAZIONE	
TEMPO DI RIPRISTINO DEL SERVIZIO	
EFFETTI E LE CONSEGUENZE DELLA VIOLAZIONE	
ORGANI INFORMATI inserire DESTINATARIO DATA E ORA	
AZIONI EFFETTUATE/PIANO DI INTERVENTO	
DECISIONI ASSUNTE (SOLO SE TITOLARE) **Motivare SE:** **IL TITOLARE HA DECISO DI NON PROCEDERE ALLA NOTIFICA** **IL TITOLARE HA RITARDATO NELLA PROCEDURA DI NOTIFICA** **IL TITOLARE HA DECISO DI NON NOTIFICARE IL DATA BREACH AGLI INTERESSATI**	
RIFERIMENTI TRACCIATURA	
DATA DI CHIUSURA	

EVENTO 3

(*) Tutti i campi sono obbligatori

DATA E ORA	
SEGNALANTE	
LUOGO VIOLAZIONE	
ENTE COINVOLTO	
MODALITA DELLA VIOLAZIONE	
TIPOLOGIA DI VIOLAZIONE	
SISTEMI IMPATTATI	
TIPOLOGIA DI DATI IMPATTATI	
NUMERO DI UTENTI INTERESSATI DALLA VIOLAZIONE	
TEMPO DI RIPRISTINO DEL SERVIZIO	
EFFETTI E LE CONSEGUENZE DELLA VIOLAZIONE	
ORGANI INFORMATI inserire DESTINATARIO DATA E ORA	
AZIONI EFFETTUATE/PIANO DI INTERVENTO	
DECISIONI ASSUNTE (SOLO SE TITOLARE) **Motivare SE:** **IL TITOLARE HA DECISO DI NON PROCEDERE ALLA NOTIFICA** **IL TITOLARE HA RITARDATO NELLA PROCEDURA DI NOTIFICA** **IL TITOLARE HA DECISO DI NON NOTIFICARE IL DATA BREACH AGLI INTERESSATI**	
RIFERIMENTI TRACCIATURA	
DATA DI CHIUSURA	

Sistema documentale

I documenti informatici, formati e ricevuti come descritto nel Manuale di gestione dell'Ente, sono acquisiti nel sistema di gestione informatica dei documenti al fine di garantirne la caratteristica di immodificabilità, ossia rendere non alterabile forma e contenuto durante le fasi di tenuta e accesso. Le funzionalità del protocollo informatico e dell'ambiente elaborativo dell'Ente garantiscono il rispetto dei requisiti di riservatezza, di integrità,di disponibilità e non ripudio, oltre a quelli sopra richiamati. Il sistema di gestione informatica del protocollo e dei documenti, è conforme alle specifiche previste dalla normativa vigente.

Esso assicura infatti:

- univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirel'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate;
- il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate. La conformità del sistema alle specifiche di cui soprasono attestate dal fornitore con idonea documentazione. Ad ogni documento informatico è associato l'insieme minimo dei metadati previsti dalla normativa vigente ed elencati nel Manuale di gestione dell'Ente, al fine di identificarne la provenienza e la natura e per garantirne la tenuta. Ad ogni documento registrato è associata in modo immodificabile l'impronta generata attraverso apposita funzione di HASH. Nella formazione dei documenti informatici effettuata nei diversi software applicativi, viene attuato un controllo delle versioni degli stessi, tenendotraccia dei loro passaggi e trasformazioni fino alla versione definitiva inviata alla registrazione.

Policy	**Caratteristiche**
1. Le credenziali di autenticazione sono nominative o comunque facilmente riconducibili all'utente utilizzatore	SI
2. Le credenziali di autenticazione non sono condivise tra utenti diversi	SI
3. Gli utenti sono configurati secondo il principio di minimizzazione	SI
4. La password per l'accesso al sistema documentale è segreta e conosciuta solo dall'utente titolare delle credenziali	SI
5. La password per l'accesso al sistema documentale viene modificata dall'utente al primo utilizzo	SI
6. La password per l'accesso al sistema documentale è composta da almeno 8 caratteri	SI
7. La password per l'accesso al sistema documentale prevede caratteristiche di complessità	NO
8. La password per l'accesso al sistema documentale non deve essere riconducibile all'incaricato e non contiene informazioni personali facilmente individuabili da terzi	NO
9. La password per l'accesso al sistema documentale non può contenere porzioni dello username	NO
10. La password per l'accesso al sistema documentale viene sostituita almeno ogni 3 mesi	SI se impostato (default 180 gg)
11. È attivo un sistema di password history per l'accesso al sistema documentale	SI
12. La password per l'accesso al sistema documentale non può essere sostituita dall'utente in maniera	NO

autonoma più di una (1) volta nell'arco di ventiquattro (24) ore	
13. È previsto un sistema di autenticazione per l'accesso al sistema documentale a fattore multiplo	NO
14. Il sistema di autenticazione per l'accesso al sistema documentale prevede policy di lockout	NO
15. Il sistema documentale prevede accesso tramite SPID	NO
16. Le utenze privilegiate e non privilegiate degli amministratori sono separate	SI
17. Le utenze privilegiate sono inventariate	SI
18. Le utenze amministrative anonime (root, administrator ecc.) sono utilizzate solo per situazioni di emergenza	SI
19. Le utenze amministrative anonime sono conservate in maniera sicura	SI
20. Viene mantenuta traccia dell'utilizzo di utenze amministrative anonime	SI
21. I dati contenuti nelle basi dati del sistema documentale sono cifrati	NO
22. Vengono eseguiti dei vulnerability assessment con cadenza semestrale dell'intero sistema documentale e sistemi correlati	NO – PER QUANTO RIGUARDA SICI VENGONO ESEGUITI VA CON CADENZA ANNUALE
23. Il sistema documentale è protetto da strumenti antimalware	SI
24. Il sistema documentale è protetto da firewall	SI
25. Il sistema documentale è protetto da sistemi anti-intrusione	SI
26. Il sistema documentale è protetto da strumenti di Data Loss Prevention	SI
27. La data e ora del sistema documentale è sincronizzata rispetto a una singola sorgente temporale, autorevole, di riferimento	SI
28. Le modifiche al sistema documentale e ai sistemi operativi interessati sono permesse solo agli utenti amministratori	SI
29. Il sistema documentale non è accessibile dall'esterno della rete dell'ente	SI (fatto salvo diversa configurazione sulla rete dell'ente)
30. Il sistema documentale e i dati in esso contenuti, compresi i sistemi operativi interessati, sono protetti da strumenti di backup	SI
31. Il sistema documentale e i dati in esso contenuti, compresi i sistemi operativi interessati, sono protetti da strumenti di backup con frequenza almeno giornaliera	SI
32. Il sistema documentale e i dati in esso contenuti, compresi i sistemi operativi interessati, sono protetti da strumenti di backup remoto	SI
33. Gli strumenti di backup remoto prevedono la cifratura dei dati prima dell'invio	SI
34. Le procedure di backup prevedono la conservazione di copie offline	NO
35. Le copie di backup offline sono cifrate	NO
36. Le copie di backup offline sono conservate in modo sicuro	NO
37. Vengono eseguiti dei test di ripristino dei backup	SI
38. I test di ripristino dei backup avvengono con frequenza almeno semestrale	SI
39. Gli accessi ai backup sono correttamente profilati seguendo il principio di minimizzazione	SI
40. Vengono registrati log eventi del sistema documentale	SI

41. I log eventi del sistema documentale comprendono la registrazione degli accessi utente	SI
42. I log eventi del sistema documentale comprendono la registrazione di attività di creazione di dati	NO
43. I log eventi del sistema documentale comprendono la registrazione di attività di modifica di dati	NO
44. I log eventi del sistema documentale comprendono la registrazione di attività di eliminazione di dati	NO
45. I log eventi del sistema documentale comprendono la registrazione di attività di oscuramento di dati	NO
46. I log eventi del sistema documentale vengono conservati per almeno 6 mesi	SI
47. Vengono registrati i log delle attività degli amministratori di sistema	SI
48. I log amministratori di sistema sono conservati per almeno 6 mesi	SI
49. I log amministratori di sistema presentano caratteristiche di immodificabilità	SI
50. Tutti i log vengono inviati ad un sistema centralizzato che ne permetta la consultazione e l'analisi	SI
51. Il sistema documentale prevede l'utilizzo della posta ordinaria come canale di comunicazione	SI
52. Il sistema documentale prevede l'utilizzo della PEC come canale di comunicazione	SI
53. I messaggi email sono filtrati prima di essere ricevuti dal sistema documentale da strumenti antispam	SI
54. I messaggi email sono filtrati prima di essere ricevuti dal sistema documentale da strumenti antimalware	SI
55. Gli allegati email non autorizzati vengono bloccati prima di essere ricevuti nel sistema documentale	SI
56. Il sistema documentale è costantemente aggiornato	SI
57. Le immagini di installazione del sistema documentale sono conservate offline	NO/LE IMMAGINI DI INSTALLAZIONE DI SICI IN CLOUD SONO CONSERVATE OFFLINE
58. Le immagini di installazione del sistema documentale offline sono conservate in maniera sicura	NO/PER SICI SI
59. Vengono eseguite verifiche periodiche del software installato	SI
60. I dispositivi critici al funzionamento del sistema sono posti in locali adeguati e ad accesso controllato	SI
61. I dispositivi removibili non autorizzati collegati al sistema documentale vengono automaticamente bloccati	SI
62. Il sistema documentale utilizza protocolli di comunicazione sicuri	SI
63. I dispositivi critici per il funzionamento del sistema documentale sono ridondati	SI
64. I dispositivi necessari al funzionamento del sistema documentale sono sottoposti a manutenzione periodica	SI
65. La validazione temporale avviene tramite sincronizzazione con ente certificato	NO

Canali di comunicazione gestiti

Il sistema prevede il download automatico, tramite protocolli standard, dei messaggi ricevuti agli indirizzi di posta ordinaria e certificata potenzialmente interessati dal processo di protocollazione.

Dopo l'esecuzione del download, il sistema prevede la cancellazione automatica dei messaggi di posta contenuti nelle caselle email collegate (quindi archivi esterni al sistema) dopo 7 giorni.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

V.2021-03

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codice in materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questa procedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legale del titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] …… Nome[1*] ……
E-mail[2*] ……
nella sua qualità[3] di

- ○ rappresentante legale
- ○ delegato del rappresentante legale

  Cognome[4*] …… Nome[4*] ……

notifica la seguente violazione di dati personali e ☐ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

———————————

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamente dovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

- ***Prima notifica***
  - a) Completa
  - b) Preliminare[1]

  La notifica viene effettuata
  - ai sensi dell'art. 33 del RGPD
  - ai sensi dell'art. 26 d.lgs. 51/2018
- ***Notifica integrativa***[2]
  - c) fascicolo n. [3*] …… PIN [3*] ……

———————————

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi a) o b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- ○ a) Fornire ulteriori informazioni senza completare il processo di 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 per le seguenti motivazioni:

C) Titolare del trattamento

1. Il titolare del trattamento è:

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento che effettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

- ○ Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti *(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)*
- ○ Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)* (*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)
- ○ Non censito in nessuno dei due precedenti indici

2. Dati del Titolare del trattamento

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione* ……
Codice Fiscale [1]* …… Soggetto privo di C.F./P.IVA italiana ☐
Stato* ……
Provincia* …… Comune* …… CAP* ……
Indirizzo* ……
Telefono* ……
E-mail[2]* ……
PEC[2]* ……

---

[1] In relazione all'indicazione del Codice Fiscale IVA si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

C1) Rappresentante del titolare del trattamento non stabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fatti salvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

- ○ a) Compila la sezione
- ○ b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] ……

Codice Fiscale/P.IVA* …… Soggetto privo di C.F./P.IVA italiana ☐

Stato* ……

Provincia* …… Comune* …… CAP* ……

Indirizzo* ……

Telefono* ……

E-mail[2*] ……

PEC[2*] ……

———————

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni (cfr. art. 33, par. 3, lett. b), del Regolamento).

- ***1) Responsabile della protezione dei dati***
  - i cui dati di contatto sono stati già comunicati con la comunicazione prot.[1*] n.....
  - i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone[2] del numero di protocollo della relativa comunicazione

    Cognome* ..... Nome* .....
    E-mail* .....
    Recapito telefonico per eventuali comunicazioni* .....

- ***2) Altro soggetto***

  Cognome* ..... Nome* .....
  E-mail* .....
  Recapito telefonico per eventuali comunicazioni* .....
  Funzione rivestita* .....

---

[1] Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numero di protocollo assegnato alla comunicazione dei dati di contatto.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile[1])

Denominazione[2*] .....
Codice Fiscale[3*] .....Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

Denominazione[2*] .....
Codice Fiscale[3*] .....Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

Denominazione[2*] .....
Codice Fiscale[3*] .....Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

---

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par. 2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;

  Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

F) Informazioni sulla violazione

1. *Momento in cui è avvenuta la violazione*

- a) Il ___ /___ /_____
- b) Dal ___/___ /_____ (la violazione è ancora in corso)
- c) Dal ___/___ /_____ al ___ /___ /_____
- d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- a) Rilevazione da parte del titolare[1]
- b) Comunicazione da parte del responsabile del trattamento
- c) Segnalazione da parte di un interessato
- d) Segnalazione da parte di un soggetto esterno
- e) Notizie stampa
- f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data …… **Ora** ……

~~4.~~ *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2]
[ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna
[ ] b) Azione accidentale interna
[ ] c) Azione intenzionale esterna
[ ] d) Azione accidentale esterna
[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

8. *Descrizione dei sistemi, software, servizi e delle infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione*

9. *Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti*

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- a) N. …… interessati
- b) Circa n. …… interessati
- c) Non determinabile
- d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati di localizzazione
[ ] l) Dati che rivelino l'origine razziale o etnici
[ ] m) Dati relativi a opinioni politiche
[ ] n) Dati relativi a convinzioni religiose o filosofiche
[ ] o) Dati che rivelino l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

13. Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione

- a) N. ……
- b) Circa n. ……
- c) Non determinabile
- d) Non ancora determinato

14. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati

15. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative, che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni.

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

[ ] a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
[ ] d) Altro

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali
[ ] b) Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità
[ ] e) Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione
[ ] h) Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale
[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

- a) Trascurabile
- b) Bassa
- c) Media
- d) Alta
- e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

1. ***Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati***

2. ***Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future***

3. ***Allegati***

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. Il titolare del trattamento ritiene[1] che:

- a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citato articolo.

1. La violazione è stata comunicata direttamente agli interessati?

- a) Sì, è stata comunicata il ___/___/_____
- b) No, sarà comunicata entro il ___/___/_____
- c) No, sono tuttora in corso le dovute valutazioni
- d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- e) No e non sarà comunicata perché:

[ ] e1) il titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);

Descrivere le misure applicate

[ ] e2) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Descrivere le misure adottate

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.

Descrivere la modalità tramite la quale gli interessati sono stati informati

2. Numero di interessati a cui è stata comunicata la violazione

N. …….. interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica
[ ] d) Altro

4. Contenuto della comunicazione agli interessati

5. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[1]?

O SI O NO

Indicare a quale organismo e in virtù di quale norma

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

O SI O NO

Note

---

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessati in più di un Paese dello Spazio Economico Europeo.

1. ***La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?***

   - a) Sì
   - b) No
   - c) Sono tuttora in corso le dovute valutazioni

2. ***Indicare l'autorità di controllo capofila[1]***

   - a) Garante per la protezione dei dati personali
   - b) Altra autorità di controllo: [Selezionare]
   - c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. ***Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione***

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

---

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dello stabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. ***La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?***

   - ○ a) Sì
   - ○ b) No

2. ***Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione***

[ ] Austria
[ ] Belgio
[ ] Bulgaria
[ ] Cipro
[ ] Croazia
[ ] Danimarca
[ ] Estonia
[ ] Finlandia
[ ] Francia
[ ] Germania
[ ] Grecia
[ ] Irlanda
[ ] Islanda
[ ] Lettonia
[ ] Liechtenstein
[ ] Lituania
[ ] Lussemburgo
[ ] Malta
[ ] Norvegia
[ ] Paesi Bassi
[ ] Polonia
[ ] Portogallo
[ ] Rep. Ceca
[ ] Romania
[ ] Slovacchia
[ ] Slovenia
[ ] Spagna

[ ] Svezia
[ ] Ungheria

3. Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)
[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata