Procedura "Protezione dati personali e tutela della riservatezza riferibili al Residente e al personale dipendente – Gestione Data Breach"

Sommario

REV.	DATA	ELABORATA DA	VERIFICATA DA	APPROVATA DA
04	22/7/22	Ass. Amministrativo Daniela Debertolis Consulente Serv. DPO Avv. Grazioli	Upipa Serv. Dpo	Direttore Dott. ssa Federica Taufer
		Responsabile Qualità: Daniela Debertolis		Firma:

DISTRIBUZIONE

La presente procedura viene distribuita in copia alle seguenti figure professionali:

- **Coordinatore/Infermiere/i/Fisioterapista/O.S.S./Animatrice/ Personale Amministrativo**
- **Originale presso ufficio responsabile Qualità. Una copia rimane a disposizione del personale presso :**
  - sala del personale/riunioni

LISTA DELLE REVISIONI

REVISIONE N.	DATA	DESCRIZIONE DELLE MODIFICHE
00	28.05.2013	Prima emissione approvata dalla Direzione
01	09.05.2014	Aggiornamento contenuti
02	30.04.2019	Adeguamento al GDPR e al d.lgs 101/18
03	12/12/2019	Inserimento alleg. proc. data breach – revisione allegati (ambito e incarico unico doc.)
04	22/07/2022	Modifica punto 4) dell' istruzione del data breach Allegato nr. 4 "notifica della violazione al Garante"

1 - SCOPO e CAMPO DI APPLICAZIONE

La presente procedura definisce le responsabilità in merito al trattamento dei dati personali trattati dall'ente nell'esercizio dei propri compiti istituzionali affinché questo si svolga nel rispetto della normativa vigente nonché dei diritti e delle libertà fondamentali, della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

La presente procedura è stata elaborata tenuto conto del concetto di "acccountability" derivante dal Regolamento UE 16/679.

Scopo della presente procedura è quello di garantire che il trattamento dei dati personali acquisiti dell'ente sia disciplinato in modo tale da assicurare un elevato livello di tutela dei diritti e delle libertà di cui sopra nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per favorire l'adempimento degli obblighi di legge da parte del titolare del trattamento, A.P.S.P. "San Giuseppe" di Primiero e dei suoi preposti.

La presente procedura è applicata per la gestione del trattamento dei dati riferibili a:

- ✓ Utenti
- ✓ Dipendenti

2 - RESPONSABILITA'

La responsabilità legata alla presente procedura è affidata al Direttore dell'Ente e al Coordinatore Sanitario designati in ragione delle rispettive competenze quali soggetti delegati a talune operazioni di trattamento secondo le indicazioni del primo comma dell'art. 2 - quaterdecies del Codice in materia di protezione dei dati personali (si rimanda alla documentazione agli atti per l'evidenza di quali siano le rispettive funzioni e competenze).

Nell'ottica di implementare un modello organizzativo che tiene conto del concetto di "responsabilizzazione", al Direttore dell'Ente sono state assegnate le seguenti competenze:

- operare attivamente affinché nel contesto delle attività di trattamento svolte nell'area amministrativa dell'Ente siano rispettate da parte del personale coinvolto le regole e le disposizioni previste dal Regolamento UE 16/679 e dal Codice in materia di protezione dei dati personali;

- fornire supporto al titolare affinché sia data applicazione al principio di "minimizzazione" favorendo la riduzione dell'utilizzo di dati personali e identificativi in modo da escludere il loro trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi o modalità che consentano di identificare l'interessato solo se necessario;

- individuare le persone autorizzate a trattare i dati personali degli interessati con i quali l'ente si rapporta verificando che ognuna di esse abbia ricevuto appropriate istruzioni su come proteggere i dati e un'idonea autorizzazione a poter compiere specifiche attività di trattamento. In caso negativo, provvedere affinché ciò venga portato a compimento. Si ricorda che tutte le persone coinvolte in operazioni di trattamento dovranno attenersi con

scrupolo alle seguenti prescrizioni: sono consentite unicamente operazioni di accesso ai dati per finalità connesse all'adempimento delle prestazioni di competenza del singolo incaricato così come indicato nel documento di autorizzazione elaborato dal titolare. Eventuali diverse operazioni di trattamento sono tassativamente vietate. Nel dettaglio sono assolutamente vietate la comunicazione a terzi non legittimati o la diffusione, tramite qualsiasi mezzo, di dati personali di qualsiasi natura provenienti dai data base del titolare;

- verificare periodicamente che il processo di trattamento, diffusione ed archiviazione dei dati personali svolto nell'ambito di competenza sia coerente con il fine della loro protezione in modo tale da ridurre al minimo il rischio che i dati trattati possano andare persi, distrutti o entrare in possesso di terzi non autorizzati;

- verificare che il trattamento dei dati acquisiti sia sempre rispettoso delle finalità della raccolta;

- verificare che agli interessati sia stata somministrata l'informativa prevista dall'art. 13 del Regolamento UE e, laddove necessario, sia stato acquisito il loro consenso al trattamento;

- provvedere all'individuazione dei soggetti delegati a compiere determinate operazioni, segnalandone gli estremi al titolare in modo tale che nei loro confronti si possa procedere con la designazione quali responsabili del trattamento;

- coordinarsi con il responsabile della protezione dei dati segnalando a tale figura ogni ipotesi di criticità, vulnerabilità e violazione per consentire gli adempimenti di conseguenza;

- coadiuvare il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato), 35 (Valutazione d'impatto sulla protezione dei dati) e 36 (Consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

- verificare la conformità del trattamento svolto mediante videosorveglianza.

Al Coordinatore Sanitario sono state affidate le seguenti attività:

- operare attivamente affinché nel contesto delle attività di trattamento svolte nell'area socio sanitaria e assistenziale dell'Ente siano rispettate da parte del personale coinvolto le regole e le disposizioni previste dal Regolamento UE 16/679 e dal Codice in materia di protezione dei dati personali;

- sia data applicazione al principio di "minimizzazione" favorendo in ambito socio assistenziale e sanitario la riduzione dell'utilizzo di dati personali e identificativi in modo da escludere il loro trattamento quando le finalità perseguite possono essere realizzate mediante dati anonimi o modalità che consentano di identificare l'interessato solo se necessario;

- individuare le persone autorizzate a trattare i dati personali degli interessati con i quali l'ente si rapporta verificando che ognuna di esse abbia ricevuto appropriate istruzioni su come proteggere i dati e un'idonea autorizzazione a poter compiere specifiche attività di

trattamento. In caso negativo, provvedere affinché ciò venga portato a compimento. Si ricorda che tutte le persone coinvolte in operazioni di trattamento in ambito socio sanitario e assistenziale dovranno attenersi con scrupolo alle seguenti prescrizioni: sono consentite unicamente operazioni di accesso ai dati per finalità connesse all'adempimento delle prestazioni di competenza del singolo incaricato così come indicato nel documento di autorizzazione elaborato dal titolare. Eventuali diverse operazioni di trattamento sono tassativamente vietate. Nel dettaglio sono assolutamente vietate la comunicazione a terzi non legittimati o la diffusione, tramite qualsiasi mezzo, di dati personali di qualsiasi natura provenienti dai data base del titolare;

- verificare periodicamente che il processo di trattamento, diffusione ed archiviazione dei dati personali svolto nell'ambito socio assistenziale e sanitario sia coerente con il fine della loro protezione in modo tale da ridurre al minimo il rischio che i dati trattati possano andare persi, distrutti o entrare in possesso di terzi non autorizzati;

- verificare che il trattamento dei dati acquisiti, con particolare attenzione quando questi possano afferire informazioni sullo stato di salute, sia sempre rispettoso delle finalità della raccolta;

- verificare che agli interessati sia stata somministrata l'informativa prevista dall'art. 13 del Regolamento UE e, laddove necessario, sia stato acquisito il loro consenso al trattamento;

- provvedere all'individuazione dei soggetti delegati a compiere determinate operazioni, segnalandone gli estremi al titolare in modo tale che nei loro confronti si possa procedere con la designazione quali responsabili del trattamento;

- coordinarsi con il responsabile della protezione dei dati segnalando a tale figura ogni ipotesi di criticità, vulnerabilità e violazione per consentire gli adempimenti di conseguenza;

- operare affinché siano rispettate le indicazioni prescritte nelle Linee guida in materia di Dossier sanitario del 4 giugno 2015 del Garante per la protezione dei dati personali verificando che i trattamenti realizzati presso l'Ente mediante lo strumento del "dossier sanitario" o del "fascicolo sanitario elettronico" siano conformi alle predette indicazioni supportando attivamente il Titolare in ogni eventuale implementazione;

- adottare nel contesto dell'erogazione dei servizi assistenziali e sanitari le misure volte ad eliminare o, comunque, a ridurre al minimo qualsiasi rischio di distruzione o perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio anche attraverso idonee procedure di valutazione di impatto;

- predisporre e verificare periodicamente lo stato di applicazione nel contesto dell'erogazione dei servizi assistenziali e sanitari del titolare di un idoneo sistema di sicurezza relativamente ai trattamenti svolti da parte di tutte le persone autorizzate tale da rispettare le prescrizioni di legge e le indicazione dell'Autorità garante;

- coadiuvare il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 (Sicurezza del trattamento), 33 (Notifica di una violazione dei dati personali all'autorità di

controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato), 35 (Valutazione d'impatto sulla protezione dei dati) e 36 (Consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

3 - RIFERIMENTI NORMATIVI

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205);
- Provvedimento del Garante privacy "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018). provvedimento Garante Privacy in materia di amministratore di sistema;
- provvedimento Garante in materia di videosorveglianza;
- provvedimento Garante in materia di fascicolo sanitario elettronico/dossier sanitario elettronico.

4- ABBREVIAZIONI, TERMINI E DEFINIZIONI

Ai fini della presente procedura si intende per:
a) **"trattamento",** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
b) **"dato personale",** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
c)"**categoria particolare di dati personali",** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
d) "**titolare del trattamento",** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici

applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
e) **"responsabile del trattamento",** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
f) "**destinatario",** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
g) **"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
h) **"interessato",** la persona fisica cui si riferiscono i dati personali;
i) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acqui- site di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
l) **«dati biometrici»: i** dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
m) **«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
n) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
o) **"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
p) "**autorità di controllo**", l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

5- MODALITA' OPERATIVE

TRATTAMENTO DATI DIPENDENTI

- Il Collaboratore Amministrativo referente del personale, su incarico del Direttore consegna l'incarico al trattamento ove è definito l'ambito del trattamento con le relative istruzioni operative sviluppato per categorie omogenee per mezzo della quale si autorizzano del trattamento i dipendenti e collaboratori dell'ente nonché gli altri soggetti che, in ragione dell'attività svolta, potrebbero avere la necessità di trattare dati personali, secondo le categorie uniformi (secondo comma art. 2- quaterdecies Codice privacy, comma 4 art. 32 RegUe 16/6769). L'incarico dovrà essere firmato per accettazione dal dipendente/addetto.

- Ai dati personali possono avere accesso solo soggetti incaricati in ragione di specifiche necessità derivanti dalla funzione svolta. L'elenco dei soggetti coinvolti viene ad essere descritto nel Registro dei trattamenti (agli atti). Ciascun incaricato è autorizzato a compiere le operazioni di trattamento necessarie ed indispensabili per adempiere ai compiti cui affidatario entro i limiti definiti nel proprio profilo autorizzativo.
- Il responsabile del sistema informatico provvede a definire i profili di autorizzazione e quindi l'accesso ai dati personali in base al ruolo ricoperto da ciascun soggetto autorizzato.
- Nell'adempimento dell'incarico conferito tutti i soggetti coinvolti sono tenuti ad attenersi ai principi di necessità indispensabilità. Ciascun incaricato è stato istruito sul fatto di dover trattare i dati ai quali ha accesso esclusivamente per lo svolgimento dei compiti e delle funzioni cui affidatario senza poter porre in essere alcuna nuova o diversa operazione di trattamento senza la preventiva autorizzazione del titolare nel pieno rispetto delle prescrizioni del Regolamento UE 16/679.
- Ogni attività deve essere svolta riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, con particolare attenzione quando questi possano rientrare nella "categoria particolare di dati personali", in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
- Agli incaricati si consegna il materiale formativo e le istruzioni operative allegate all'ambito; viene inoltre condiviso un disciplinare aziendale alleg. nr. 3 riferito al corretto utilizzo degli strumenti informatici.
- Periodicamente si organizzano sessioni formative in materia di protezione dati personali coinvolgendo se del caso il DPO e l'amministratore di sistema.
- Il rispetto da parte dei soggetti autorizzati delle indicazioni operative e delle istruzioni loro conferite viene ad essere verificato costantemente da parte del Direttore e del Coordinatore.
- Il collaboratore amministrativo distribuisce l'informativa al trattamento dei dati ai dipendenti (allegato nr. 1), ai liberi professionisti dell'ente e ai tirocinanti con attestazione della ricevuta di avvenuta consegna.
- Il trattamento dei dati personali relativi al personale dell'ente, gestiti dal Collaboratore Amministrativo addetto all'Ufficio gestione del personale, viene eseguito sia in modalità elettronica mediante utilizzo di strumenti informatici che in modalità cartacea (raccolta, registrazione, conservazione, utilizzo dei documenti mediante fascicoli, schede raccoglitori e archivi) e consiste nella trascrizione su cartaceo e nella conservazione nei locali dell'ente. In esecuzione ad obblighi di legge o di regolamento i dati personali dell'interessato potranno essere diffusi tramite sul sito internet dell'ente secondo la normativa vigente in materia; non è prevista diffusione dei dati riferiti allo stato di salute. I dati comunicati non saranno trasferiti verso Paesi Terzi o organizzazioni internazionali extra UE.
- Il trattamento a cui sono e saranno sottoposti i dati personali acquisiti nell'ambito della gestione del rapporto di lavoro (dati anagrafici, dati di contatto, dati identificativi, ecc.) ha le seguenti finalità: instaurazione e gestione del rapporto con il personale dipendente; adempimento di obblighi fiscali e contabili; applicazione della legislazione previdenziale e assistenziale; trattamento giuridico ed economico del personale; adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali; igiene e sicurezza del lavoro.

- I dati acquisiti vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. Tali misure sono oggetto di una costante attività di verifica e implementazione anche mediante il coinvolgimento dell'amministratore di sistema e la supervisione del DPO.
- Il trattamento dei predetti dati è indispensabile per consentire il perseguimento di finalità istituzionali proprie della APSP e dare adempimento agli obblighi previsti dalla normativa vigente.
- Il titolare del trattamento è impegnato nell'applicazione dei principi di indispensabilità e necessità nel trattamento. La raccolta e le operazioni di trattamento si limitano a quelle strettamente indispensabili per il perseguimento dei fini di cui legittimato. I dati personali sono:
  - ✓ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
  - ✓ raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
  - ✓ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
  - ✓ esatti e, se necessario, aggiornati;
  - ✓ conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
  - ✓ trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Nel trattamento, nella archiviazione e nella distruzione vengono rispettati i seguenti criteri:
- i dati personali dei dipendenti sono archiviati in cartelle chiuse e non trasparenti, contenute in armadi presso l'ufficio personale;
- i documenti contenenti dati personali sono utilizzati in modo tale da evitare che possano essere visionati da personale esterno;
- eventuali stampati contenenti dati personali vengono strappati prima di essere smaltiti;
- l'accesso ai computer è protetto da password personale e riservata soggetta a periodico aggiornamento;
- i locali in cui sono presenti dati personali sono in ogni caso presidiati da personale dell'Ente durante l'eventuale presenza di soggetti esterni.

Nei confronti di tale attività di trattamento l'ente ritiene di dover eseguire una valutazione di impatto tenuto conto dell'art. 35 del Reg. Ue 16/679 e delle indicazioni fornite dall'autorità Garante nel provvedimento "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018). Tale valutazione di impatto è attualmente oggetto di definizione con il coinvolgimento del DPO e verrà costantemente monitorata.

I dati acquisiti non saranno trasferiti in Paesi extra UE e saranno conservati nel rispetto dei termini di legge.

- In caso di ipotesi di violazione della sicurezza, l'ente provvede alla gestione del "data breach", come indicato negli artt. 33 e 34 del Reg. Ue 16/679 mediante una idonea

procedura elaborata con la condivisione e la supervisione del DPO (procedura agli atti allegato nr. 4).

- Relativamente ai dati conferiti, l'interessato o un suo rappresentante può esercitare, senza particolari formalità, i diritti previsti dagli artt. 15 e segg. del Regolamento UE 16/679 rivolgendosi al titolare o al responsabile per la protezione dei dati.
- La base giuridica del trattamento tiene conto di quanto indicato dall'art. 2-ter del codice in materia di protezione dati personali (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

TRATTAMENTO DATI RESIDENTI

- L'impiegato amministrativo che si occupa della gestione degli utenti è tenuto a consegnare l'informativa (allegato nr. 2) al momento della raccolta delle informazioni di pre ingresso.
- Al momento del colloquio di pre ingresso l'impiegato amministrativo dovrà acquisire il consenso al trattamento dati (parte finale informativa Allegato nr. 2) nel quale quali verranno indicati i nominativi dei soggetti ai quali l'ente è autorizzato a fornire informazioni. In caso di impedimento da parte del residente il modulo di consenso va firmato da parte di una figura esercitante legalmente la potestà, famigliare, prossimo congiunto, convivente o responsabile della struttura. Originale dello stesso rimarrà nel fascicolo dell'ospite presso l'ambulatorio infermieristico in apposito armadio e una copia presso il fascicolo amministrativo in deposito presso l'ufficio ospiti.
- I dati acquisiti vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. Tali misure sono oggetto di una costante attività di verifica e implementazione anche mediante il coinvolgimento dell'amministratore di sistema e la supervisione del DPO.
- Il trattamento dei predetti dati è indispensabile per consentire il perseguimento di funzioni istituzionali proprie della APSP e, nello specifico, per le seguenti finalità: permettere l'instaurazione, gestione e amministrazione del rapporto; dare esecuzione di obblighi contrattuali e di legge; consentire la programmazione e pianificazione delle attività; favorire la gestione del contenzioso; organizzare servizi di controllo interni (della sicurezza, della qualità dei servizi, dell'integrità del patrimonio, degli ingressi e delle uscite anche mediante predisposizione e attivazione di pertinenti sistemi di contenzione personale); svolgere analisi statistiche o attività di ricerca (mediante dati anonimi); permettere l'erogazione di servizi infermieristici, fisioterapici, medici e sanitari e prestazioni di prevenzione, diagnosi, cura, riabilitazione a tutela dell'incolumità fisica e della salute dell'interessato e di terzi; favorire la comunicazione delle informazioni dello stato di salute dell'interessato a soggetti terzi legittimati; permettere l'erogazione dei servizi a favore degli interessati in condivisione o in contitolarità con altri soggetti (medici, farmacisti, liberi professionisti, operatori servizi sociali, enti territoriali, ecc.) per esigenze di cura e amministrative strettamente correlate alla attività sopra indicata; garantire la fornitura di servizi assistenziali, infermieristici o sanitari su delega o in convenzione con la APSS.
- Il titolare del trattamento è impegnato nell'applicazione dei principi di indispensabilità e necessità nel trattamento. La raccolta e le operazioni di trattamento si limitano a quelle strettamente indispensabili per il perseguimento dei fini di cui legittimato. I dati personali sono:
  - trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

❖ I dati non saranno trattati mediante processi decisionali automatizzati. Tutti i dati conferiti sono trattati secondo i principi di correttezza, liceità e trasparenza sia in forma cartacea che elettronica e protetti mediante misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR.

❖ Il trattamento dei dati personali relativi ai residenti dell'ente in ambito sanitario viene eseguito sia in modalità elettronica mediante utilizzo di strumenti informatici che in modalità cartacea (raccolta, registrazione, conservazione, utilizzo dei documenti mediante fascicoli, schede raccoglitori e archivi) e consiste nella trascrizione su cartaceo e nella conservazione nei locali dell'ente. Non si effettua alcuna diffusione dei dati stessi. Nel trattamento, nella archiviazione e nella distruzione vengono rispettati i seguenti criteri:

- i dati personali dei residenti sono archiviati in cartelle chiuse e non trasparenti, contenute in armadi presso l'ambulatorio infermieristico e utilizzati in modo tale da evitare che possano essere visionati da personale esterno;
- eventuali stampati contenenti dati personali vengono strappati prima di essere smaltiti;
- l'accesso ai computer è protetto da password personale e riservata soggetta a periodico aggiornamento;
- le informazioni relative ai residenti sono registrate e archiviate nel software denominato Cba, il quale consente l'accesso tramite password nonché l'autorizzazione degli accessi e delle visualizzazioni/inserimenti consentiti tramite diversi profili a seconda della figura professionale;
- il trattamento di dati personali, comuni e riferiti allo stato di salute, potrà essere effettuato, previo specifico consenso, attraverso procedure volte a informatizzare la gestione della cartella sanitaria. Tale modalità prevede l'elaborazione in formato elettronico delle informazioni inerenti lo stato di salute dell'interessato relativamente ad eventi clinici presenti e trascorsi (p.es.: referti, documentazione relativa a ricoveri, dati clinici, immagini di indagini diagnostiche, ecc.) al fine di permettere e documentare la storia clinica e migliorare le prestazioni di prevenzione, diagnosi e cura. Tale sistema prevede che dati comuni e riferiti allo stato di salute siano elaborati con modalità informatiche e allocati su banche dati idonee a rendere accessibile la consultazione, differenziata per ambiti specifici e profili di autorizzazione, da parte di personale incaricato al loro trattamento del rispetto dei principi di necessità, indispensabilità e pertinenza.
- Nello specifico, alle banche dati potrà avere accesso personale incaricato da parte dell'A.P.S.P. nonché, alla luce dell'attivazione del sistema TreC, da parte di eventuali soggetti incaricati al trattamento da parte della Azienda Provinciale per i Servizi Sanitari della Provincia Autonoma di Trento in riferimento alle distinte competenze e nel rispetto dei principi di pertinenza e necessità per le seguenti finalità: gestione

delle schede U.V.M., gestione anagrafica ospiti e predisposizione di piano assistenziale sintetico (software ATLANTE); refertazione esami di laboratorio e radiologici (sistema SIO); anagrafe provinciale esami laboratorio (sistema IPPOCRATE), prenotazione servizi CUP, gestione servizi decentrati (centro prelievi, fisioterapia, ecc.). Gestione sistema TreC (cartella clinica del cittadino). Il dossier o il fascicolo potrà essere consultato, anche senza il consenso dell'interessato, ma nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività.

- i locali in cui sono presenti dati sensibili dei residenti sono in ogni caso presidiati da personale dell'Ente durante l'eventuale presenza di soggetti esterni.
- Anche nei confronti di tale attività di trattamento l'ente ritiene di dover eseguire una valutazione di impatto tenuto conto dell'art. 35 del Reg. Ue 16/679 e delle indicazioni fornite dall'autorità Garante nel provvedimento "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018). Tale valutazione di impatto è attualmente oggetto di definizione con il coinvolgimento del DPO e verrà costantemente monitorata.
- I dati acquisiti non saranno trasferiti in Paesi extra UE e saranno conservati nel rispetto dei termini di legge.
- In caso di ipotesi di violazione della sicurezza, l'ente provvede alla gestione del "data breach", come indicato negli artt. 33 e 34 del Reg. Ue 16/679 mediante una idonea procedura elaborata con la condivisione e la supervisione del DPO (procedura agli atti).
- Relativamente ai dati conferiti, l'interessato o un suo rappresentante può esercitare, senza particolari formalità, i diritti previsti dagli artt. 15 e segg. del Regolamento UE 16/679 rivolgendosi al titolare o al responsabile per la protezione dei dati.
- La base giuridica del trattamento tiene conto di quanto indicato dall'art. 2-ter del codice in materia di protezione dati personali (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

5 – MAPPA SISTEMA INFORMATIVO

FASI	*ELEMENTI DEL SISTEMA INFORMATIVO*			
RACCOLTA E TRASFORMAZIONE DEI DATI IN INFORMAZIONI	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
INGRESSO UTENTE	dati anagrafici dell'utente dati bancari dell'utente raccolta consenso trattamento dati	creazione fascicolo utente	personale ufficio amministrativo	sistema informatico - SofwtwareC.S.S. programma CBA
	dati assistenziali dell'utente	creazione cartella sanitaria assistenziale dell'utente	personale addetto all'assistenza sociosanitaria dell'utente	sistema informatico - SofwtwareC.S.S. programma CBA
	dati sanitari dell'utente	raccolta ordine temporale dei referti di tipo diagnostico e terapeutico dell'utente divisi per tipologia		faldone cartaceo
ASSUNZIONE DI PERSONALE	dati anagrafici del neo assunto curriculum vitae dati bancari del neo assunto raccolta consenso informato e incarico trattamento dei dati	creazione fascicolo dipendente	personale ufficio amministrativo responsabile formazione	fascicolo cartaceo inserimento in anagrafica del personale programma informatico CBA e sito ECM Trento
ATTIVITA' AMMINISTRATIVA	raccolta dati dei fornitori	creazione elenco dei fornitori	personale ufficio amministrativo	sistema informatico
	raccolta dati beni acquistati	inventario beni	personale ufficio amministrativo	sistema informatico - Software Sipcar plus Programma C.B.A.
ATTIVITA' DI MONITORAGGIO DELLA SODDISFAZIONE ESTERNA	raccolta dati soddisfazione utenti	creazione fascicolo soddisfazione utenza	responsabile di servizio	sistema informatico
GESTIONE DATI E INFORMAZIONI:	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
ATTIVITA' EROGATA AGLI UTENTI	consultaizone quotidiana della cartella clinico assistenziale dell'utente registrazione quotidiana in cartella clinico assistenziale dell'utente	acquisizione delle nuove informazioni creazione di valutazioni multiprofessionali dell'utente	personale addetto all'assistenza sociosanitaria dell'utente	Software Sipcar plus Software Atlante
	consultazione referti inerenti il residente	acquisizione di nuove informazionei sanitarie diagnostico - terapeutiche	personale medico	Programma S.I.O.
ATTIVITA' CONTABILE	fatture emesse e ricevute, ordini a fornitori, dati bancari	bilancio d'esercizio, relazioni di gestione	personale ufficio amministrativo	sistema informatico - Software CBA Sipcar plus
	timbrature del personale	database mensile	personale ufficio amministrativo	sistema informatico - Programma C.B.A.
ATTIVITA' DI COMUNICAZIONE	comunicazioni in entrata / uscita (cartacee , elettroniche)	registrazione di lettere ed e-mail in entrata e uscita nel protocollo	personale ufficio amministrativo	programma CBA, archivio cartaceo delle comunicazioni
PRODUZIONE, EROGAZIONE, DIFFUSIONE, MESSA A DISPOSIZIONE DI INFORMAZIONI	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
INFORMAZIONI ALL'UTENZA	informazioni rispetto allo stato di salute e alla quotidiantià dell'utente	colloquio con utenti - famigliari - ammministratori di sostegno - tutori	medico, coordinatore, responsabili di servizio, infermieri, operatori	registrazione comunicazioni in CBA CSS
ATTIVITA' DI PUBBLICITA'	informazioni inerenti l'attività offerta e la regolamentazione della stessa	carta servizi, regolamenti, statuto, brochure, avvisi	personale dell'azienda ed esterni - potenziali utenti / fruitori dei servizi	pubblicazioini cartacee - pubblicazione sito internet aziendale
ATTIVITA' DI MONITORAGGIO	dati relativi l'andamento delle attività	report di monitoraggio dell'attività e relazioni	direzione - C.d.A. - referenti dei servizi	file di gestione dati in excel; estrapolazione dati dal SofwareCBA Programma C.S.S.; stampa di report cartacei
ATTIVITA' ORGANIZZATIVA	informazioni al personale delle modalità operative da adottare nelle varie fasi dell'attività	protocolli, procedure, istruzioni operative	tutto il personale coivolto da ogni documento	faldone cartaceo
	compiti ed orari del personale	piano delle attività	tutto il personale del settore socio - sanitario e assistenziale	documento cartaceo
ARCHIVIAZIONE DATI	**DATI**	**INFORMAZIONI**	**PERSONE**	**STRUMENTI**
USCITA DELL'UTENTE	dati anagrafici, sanitari, assistenziali e sociali dell'utente	fascicolo dell'utente e cartella sanitaria	personale ufficio amministrativo personale addetto all'assistenza sociosanitaria	faldoni cartacei; cartelle informatizzate CSS
RELAZIONI ATTIVITA' SVOLTA	dati inerenti l'attività	report, relazioni,	direzione	faldoni cartacei; cartelle informatizzate.
USCITA DEL PERSONALE	dati anagrafici, sanitari, assistenziali e sociali del dipendente	fascicolo del dipendente	personale d'ufficio	faldoni cartacei; cartelle informatizzate.

6 - ALLEGATI E DOCUMENTI DI REGISTRAZIONE

1. Informativa al trattamento dei dati ai dipendenti (allegato nr. 1)
2. Informativa utenti (allegato nr. 2) Consenso al trattamento dati (Allegato nr.2)
3. Disciplinare aziendale (alleg. nr. 3)
4. Istruzione Data breach (allegato nr. 4)

AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA"SAN GIUSEPPE" DI PRIMIERO
Viale Marconi, 19 - Pieve
38054 PRIMIERO SAN MARTINO DI CASTROZZA (TN)
Segreteria ☎ (0439) 62371 - fax 🖷 (0439) 765399
Infermeria ☎ (0439) 64620 - fax 🖷 (0439) 765406
Cod. Fiscale e P.iva 00374850220
E-mail: segreteria@apsp-primiero.net
Posta Elettronica Certificata: segreteria@pec.apsp-primiero.net
Sito Internet: https://www.apsp-primiero.net/

INFORMATIVA TRATTAMENTO DATI DEL PERSONALE DIPENDENTE

Ai sensi dell'articolo 13 del Regolamento EU 16/679 La informiamo che i Suoi dati sono trattati dalla APSP "San Giuseppe" di Primiero, titolare del trattamento e in particolare che:

Finalità del trattamento

Il trattamento a cui sono e saranno sottoposti i dati personali acquisiti nell'ambito della gestione del rapporto di lavoro (dati anagrafici, dati di contatto, dati identificativi, ecc.) ha le seguenti finalità:

- instaurazione e gestione del rapporto con il personale dipendente;
- adempimento di obblighi fiscali e contabili;
- applicazione della legislazione previdenziale e assistenziale;
- trattamento giuridico ed economico del personale;
- adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali;
- igiene e sicurezza del lavoro.

Trattamento di categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati

Il trattamento riguarda anche le seguenti categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati: contributi sindacali; permessi, congedo straordinario ed aspettative sindacali; condanne e procedimenti giudiziari pendenti contenuti in dichiarazioni sostitutive ai sensi del D.P.R. n. 445/2000.

Conferimento dei dati

I dati sono di norma raccolti presso l'interessato. Per l'instaurazione e la prosecuzione del rapporto di lavoro, nonché per la corretta quantificazione della retribuzione, è necessario il conferimento dei Suoi dati anagrafici e quelli di eventuali familiari a carico o componenti del nucleo familiare. L'eventuale non comunicazione di tali dati, comporta l'impossibilità da parte del titolare di garantire la congruità del trattamento stesso ai patti contrattuali, nonché l'impossibilità di adempiere agli obblighi imposti dalla normativa fiscale, amministrativa o del lavoro. In caso di richiesta di accredito dello stipendio presso istituti bancari, è necessario il conferimento degli estremi del c/c bancario. Per adempiere a richieste specifiche del dipendente o per obbligo di legge o contrattuale,

il trattamento potrebbe riguardare anche dati idonei a rivelare lo stato di salute (assenza per malattia, maternità, infortunio, inidoneità a determinate mansioni, categorie protette), l'adesione a sindacato (assunzione di cariche sindacali, richiesta di trattenute per quote di associazione), l'adesione a partito politico (richiesta di permessi o aspettativa per cariche pubbliche elettive), convinzioni religiose (richiesta di fruizione di festività religiose), opinioni filosofiche (assolvimento di obbligo di leva quale obiettore di coscienza), origini razziali ed etniche ecc.

Il trattamento dei dati personali conferiti si basa sulla vigente normativa in materia di rapporto di lavoro, tra cui si indica: Legge n. 104/92 "legge quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate"; Legge n. 68/99 "norme per il diritto al lavoro dei disabili"; Decreto Legislativo 81/2008 "Testo Unico delle disposizioni legislative in materia di tutela della salute e della sicurezza nei luoghi di lavoro"; Decreto legislativo 38/00 "Disposizioni in materia di assicurazione contro gli infortuni sul lavoro e le malattie professionali"; Decreto Legislativo 151/01 " Testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità"; Decreto Legislativo 215/03 "Attuazione della Direttiva 2000/43 CE per la parità di trattamento delle persone indipendentemente dalla razza e dalla origine etnica"; Decreto Legislativo 216/03 "Attuazione della Direttiva 2000/78 CE per la parità di trattamento in materia di occupazione e condizioni di lavoro"; Legge 300/70 "Statuto dei lavoratori"; Decreto Legislativo 165/01 "Norme Generali sull'ordinamento del lavoro alle dipendenze delle Amministrazioni Pubbliche"; TU 81/2008; C.C.P.L; L.R. 21/09/2005 n. 7; Regolamento organico del personale dipendente; L.P. n.14/91; L.P. n.6/98; Statuto dell'Ente.

Altre disposizioni normative possono essere richiamate nella documentazione consegnata all'interessato in sede di assunzione o, se del caso, in momenti successivi. Eventuali variazioni di dati dovranno essere tempestivamente comunicate al titolare del trattamento.

Base giuridica del trattamento
La base giuridica del trattamento dei dati raccolti è rappresentata dalla necessità di dare esecuzione ad un obbligo di legge e/o eseguire un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Modalità del trattamento
I dati vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. I dati non saranno trattati mediante processi decisionali automatizzati. Tutti i dati conferiti sono trattati secondo i principi di correttezza, liceità e trasparenza sia in forma cartacea che elettronica e protetti mediante misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR.

Obbligatorietà del conferimento
Il conferimento dei dati ha natura obbligatoria. Non fornire i dati comporta non osservare obblighi di legge e/o impedire che l'amministrazione possa rispondere alle richieste presentate dagli interessati.

Comunicazione dei dati e responsabili del trattamento
I dati possono essere conosciuti dal titolare, dai responsabili del trattamento, dagli incaricati del trattamento appositamente istruiti. I dati raccolti possono essere comunicati, in tutto o in parte ove necessario e comunque per le finalità del trattamento in oggetto, a: società di consulenza nominata responsabile del trattamento per finalità di elaborazione degli stipendi e di tutti gli emolumenti dovuti (a tale soggetto possono venire comunicati anche i dati rientranti nella "categoria particolare

di dati personali" strettamente necessari); medico competente, nominato responsabile del trattamento, per gli adempimenti connessi alla normativa sull'igiene e sicurezza sul lavoro; società informatiche, nominate responsabili del trattamento, per la gestione e manutenzione dei sistemi informativi e dei programmi installati; altri soggetti nominati responsabili la cui precisa specificazione può essere oggetto di verifica presso gli uffici dell'Azienda; enti e/o uffici pubblici in obbligo di legge (a tali soggetti possono essere comunicati anche i dati rientranti nella "categoria particolare di dati personali" strettamente necessari agli obblighi di legge); banche e istituti di credito per l'accredito sul conto corrente personale dello stipendio e di tutte le spettanze dovute (a tali soggetti non sono comunicati i dati rientranti nella "categoria particolare di dati personali"; assicurazioni per stipula polizze; enti pubblici (PAT e A.P.S.S.); UPIPA per finalità connesse alla gestione e alla organizzazione di percorsi o adempimenti formativi. Ai dati potrebbero avere accesso anche organi ispettivi e di controllo.

Durata del trattamento e periodo di conservazione
I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto in essere tra le parti e saranno conservati per il tempo di legge.

Ambito di diffusione dei dati
In esecuzione ad obblighi di legge o di regolamento i dati personali dell'interessato potranno essere diffusi tramite sul sito internet dell'ente secondo la normativa vigente in materia; i dati relativi a nome, cognome ed indirizzo e-mail attribuito potranno essere pubblicati in Internet e/o sul notiziario dell'ente; non è prevista diffusione dei dati riferiti allo stato di salute. I dati comunicati non saranno trasferiti verso Paesi Terzi o organizzazioni internazionali extra UE.

Responsabile per la protezione dei dati:

La nostra Azienda, titolare del trattamento, ha designato il proprio responsabile per la protezione dei dati raggiungibile all'indirizzo: serviziodpo@upipa.tn.it

Diritti dell'interessato
Relativamente ai dati conferiti, l'interessato o un suo rappresentante può esercitare, senza particolari formalità, i diritti previsti dagli artt. 15 e segg. del Regolamento UE 16/679 rivolgendosi al titolare o al predetto responsabile per la protezione dei dati. In particolare, potrà chiedere la rettifica, la cancellazione, la limitazione del trattamento dei dati stessi nei casi previsti dall'art. 18 del GDPR, la portabilità dei dati che La riguardano nei casi previsti dall'art. 20 del GDPR, nonché proporre reclamo all'autorità di controllo competente ex articolo 77 del GDPR (Garante per la Protezione dei Dati Personali).

AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA
"SAN GIUSEPPE" DI PRIMIERO
Viale Marconi, 19 - Pieve
38054 PRIMIERO SAN MARTINO DI CASTROZZA (TN)
Segreteria ☎ (0439) 62371 - fax 🖷 (0439) 765399
Infermeria ☎ (0439) 64620 - fax 🖷 (0439) 765406
Cod. Fiscale e P.iva 00374850220
E-mail: segreteria@apsp-primiero.net
Posta Elettronica Certificata: segreteria@pec.apsp-primiero.net
Sito Internet: https://www.apsp-primiero.net/

Primiero San Martino di Castrozza, 05/11/19

Informativa all'interessato in relazione al trattamento dei dati personali
art. 13 Regolamento europeo 16/679

L' AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA "SAN GIUSEPPE" DI PRIMIERO con sede in Primiero San Martino di Castrozza, titolare del trattamento, Le fornisce le seguenti informazioni nel merito del trattamento svolto sui Suoi dati personali.

Finalità del trattamento dei dati
Il trattamento a cui sono e saranno sottoposti i dati personali acquisiti nell'ambito della gestione del rapporto instaurato con l'interessato risponde alle seguenti finalità:

- instaurazione, gestione e amministrazione del rapporto con l'interessato;
- esecuzione di obblighi contrattuali e di legge;
- programmazione e pianificazione delle attività;
- gestione del contenzioso;
- servizi di controllo interni (della sicurezza, della qualità dei servizi, dell'integrità del patrimonio, degli ingressi e delle uscite anche mediante predisposizione e attivazione di sistemi di videosorveglianza e contenzione personale);
- analisi statistiche o attività di ricerca (mediante dati anonimi);
- finalità di tutela della salute (prevenzione, diagnosi, cura e riabilitazione, fornitura di beni o servizi all'utente per la salvaguardia della salute) mediante erogazione di servizi infermieristici, fisioterapici, medici e sanitari;
- tutela socio assistenziale e interventi di rilievo sanitario a favore di soggetti bisognosi, non autosufficienti o incapaci;
- fornitura di servizi assistenziali, infermieristici o sanitari su delega o in convenzione con la APSS PAT.

Categorie di dati trattati
Per tutte le predette finalità devono essere trattati dati personali "comuni" (ad.es. dati anagrafici e identificativi dell'interessato). Il conferimento di tali dati ha natura obbligatoria per accedere alle prestazioni richieste alla nostra APSP. Il mancato conferimento comporta per l'Amministrazione l'impossibilità di rispondere in tutto o in parte alle richieste presentate dagli interessati e dare esecuzione a quanto di propria spettanza.

Per le finalità di tutela della salute è necessario trattare dati riferiti allo stato di salute dell'interessato. Il conferimento di tali informazioni è indispensabile per consentire al titolare di adempiere agli obblighi contrattuali e di legge e a quelli conseguenti alle finalità sopra indicate.

Dati riguardanti convinzioni religiose, filosofiche o di altro genere (non indispensabili e comunque il loro eventuale mancato conferimento non pregiudica la possibilità di avere accesso ai servizi dell'ente) potrebbero essere facoltativamente riferiti dall'interessato o dal suo rappresentante e conseguentemente trattati dall'ente al fine di adempiere a obblighi di legge o dare riscontro a particolari richieste dell'interessato stesso.

Immagini personali
Nell'esercizio di fini connessi ad attività correlate al perseguimento di finalità proprie dell'Ente (socializzazione, animazione, svago, mantenimento di rapporti tra l'utente e il territorio) il trattamento, previa specifica autorizzazione (la base giuridica è il consenso), potrebbe avvenire anche tramite la raccolta e l'utilizzo di immagini personali dell'interessato (raccolti in filmati e/o fotografie). Per finalità di gestione delle suddette attività il ritratto personale e fotografico dell'interessato potrebbe essere diffuso tramite pubblicazione sul giornalino/notiziario della A.P.S.P. o su altro materiale istituzionale dell'Ente. Alcune immagini fotografiche ritraenti l'interessato potrebbero essere esposte su cartelloni affissi all'interno della struttura. Il ritratto fotografico dell'interessato potrebbe inoltre essere affisso in prossimità della porta di

ingresso della stanza ove dimora in modo tale da agevolarne un immediato riconoscimento. Le immagini personali potrebbero inoltre essere diffuse mediante loro esposizione sul sito internet dell'Ente. L'autorizzazione a tale trattamento è sempre facoltativa e l'interessato in ogni momento può opporsi o revocare il consenso mediante semplice richiesta inoltrata agli uffici.
In ogni caso, e indipendentemente dal rilascio del consenso, una fotografia dell'interessato sarà utilizzata, per i fini di riconoscimento e cura dell'ospite, all'interno della cartella sanitaria.

Base giuridica del trattamento
Alla luce degli artt. 2-ter, 2-sexies del Codice in materia di protezione dei dati personali e degli artt. 6, paragrafo 1, lett. c), e) e art. 9, paragrafo 2, lettere g), h) ed i) del Regolamento UE 16/679, i trattamenti dei Suoi dati personali (comprensivi di quelli appartenenti a categorie particolari di dati, ad esempio, quelli riguardanti lo stato di salute) non rendono necessario il Suo consenso quando vengono effettuati dal predetto titolare nell'esercizio delle proprie funzioni istituzionali nell'ambito di attività sanitarie relative all'attività di prevenzione, diagnosi, cura e riabilitazione; attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione; programmazione, gestione, controllo e valutazione dell'assistenza sanitaria.
Per quanto concerne l'allocazione dei Sui dati nel sistema di gestione informatizzata della cartella sanitaria (dossier sanitario) e per la diffusione del ritratto fotografico, la base giuridica del trattamento è rappresentata dal Suo consenso.

Modalità del trattamento
I dati acquisiti (raccolti presso l'interessato, enti o soggetti atti a tutelarne gli interessi nonché presso i servizi a ciò preposti da parte dell'A.P.S.S.) vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. I dati non saranno trattati mediante processi decisionali automatizzati. Tutti i dati conferiti sono trattati secondo i principi di correttezza, liceità e trasparenza sia in forma cartacea che elettronica e protetti mediante misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR.

Dossier sanitario e fascicolo sanitario elettronico
Il trattamento di dati personali, comuni e riferiti allo stato di salute, potrà essere effettuato, previo specifico consenso, attraverso procedure volte a informatizzare la gestione della cartella sanitaria. Tale modalità prevede l'elaborazione in formato elettronico delle informazioni inerenti allo stato di salute dell'interessato relativamente ad eventi clinici presenti e trascorsi (p.es.: referti, documentazione relativa a ricoveri, dati clinici, immagini di indagini diagnostiche, ecc.) al fine di permettere e documentare la storia clinica e migliorare le prestazioni di prevenzione, diagnosi e cura. Tale sistema prevede che dati comuni e riferiti allo stato di salute siano elaborati presso il nostro ente con modalità informatiche e allocati su banche dati idonee a rendere accessibile la consultazione, differenziata per ambiti specifici e profili di autorizzazione, da parte di personale incaricato al loro trattamento del rispetto dei principi di necessità, indispensabilità e pertinenza (*dossier sanitario*).
Per quanto riguarda il trattamento connesso al Fascicolo sanitario elettronico si fa rinvio all'informativa elaborata dalla APSS.

Videosorveglianza
Si segnala che presso alcuni varchi e lungo alcune aree perimetrali dell'Ente è attivo un sistema di videosorveglianza per ragioni di tutela della salute e sicurezza dei degenti, dei visitatori e del personale nonché del patrimonio dell'Ente, adeguatamente segnalato da appositi cartelli informativi.

Condivisione, comunicazione dei dati, responsabili del trattamento:
I dati raccolti sono trattati da parte di personale e collaboratori incaricati in ragione di effettive esigenze lavorative nel rispetto del principio di necessità. Personale amministrativo, infermieristico, fisioterapico, medico socio assistenziale e ausiliario nonché addetto all'animazione, appositamente incaricato in relazione alle mansioni di competenza, potrà entrare a conoscenza dei dati conferiti nel rispetto del principio di indispensabilità.
I relativi allo stato di salute non possono essere diffusi. Gli stessi possono essere resi accessibili, in tutto o in parte ove necessario e comunque per le finalità del trattamento in oggetto o nei casi previsti dalla legge ai seguenti soggetti: A.P.S.S., strutture o aziende sanitarie, professionisti del servizio sanitario, servizi socio assistenziali e sanitari per fini di tutela della salute dell'interessato e nell'adempimento delle prestazioni sanitarie erogate a suo favore; enti locali e amministrazioni pubbliche in adempimento a obblighi di legge; strutture convenzionate, fornitori di ausili per specifiche finalità riferite alla prestazione indicata; società informatiche e amministratori di sistema per finalità di gestione e manutenzione dei sistemi informativi e dei programmi installati, enti assicurativi; eventuali consulenti ed enti di certificazione per le correlate finalità. Ai dati possono avere accesso anche organi ispettivi e di controllo in obbligo di legge, banche e istituti di credito per l'appoggio degli effetti bancari; istituti previdenziali.
Ai sensi del d.lgs 175/2014 l'elenco delle prestazioni di carattere sanitario erogate e fatturate nei confronti dell'interessato, salvo esercizio del diritto di opposizione, saranno trasmesse in modalità telematica al Sistema Tessera Sanitaria gestito dal Ministero dell'Economia e Finanze. Ciascun interessato può opporsi, in tutto o in parte, a tale comunicazione facendo richiesta presso i nostri Uffici amministrativi ovvero chiedere all'Agenzia delle Entrate che tutti o taluni dati (spese ed eventuali rimborsi) non vengano utilizzati per l'elaborazione della dichiarazione dei redditi pre compilata.

Oltre ai soggetti sopra specificati i dati conferiti potranno essere trattati da parte di altri soggetti terzi, nominati responsabili del trattamento (associazioni professionisti per prestazioni di infermiere professionali o cooperative incaricate alla preparazione dei pasti, appaltatori di servizi, consulenti, fornitori di servizi, ecc.) nella misura in cui ciò sia necessario per l'espletamento dell'attività da essi svolta a favore dell'Ente e nei limiti dei profili di autorizzazione per essi individuati. Il loro elenco è accessibile mediante semplice richiesta.
I Suoi dati personali e relativi a particolari categorie di dati (art 9 del Regolamento), saranno inoltre trattati al fine di adempiere agli obblighi previsti da leggi, regolamenti e dalla normativa comunitaria nonché alle disposizioni impartite dalle autorità a ciò legittimate dalla legge.
Al di fuori delle suddette ipotesi, la comunicazione a terzi di dati personali conservati dall'Azienda avverrà nei limiti e secondo le modalità e forme stabilite dalla legge.

Ambito di diffusione dei dati
Non è prevista la diffusione dei dati riferiti allo stato di salute. I dati acquisiti non saranno trasferiti in Paesi extra UE.
L'eventuale diffusione avrà luogo unicamente in adempimento ad obblighi normativi.
La A.P.S.P. nell'esercizio di alcune competenze e per il perseguimento di alcune delle finalità sopra esposte opera in regime di contitolarità con l'Azienda Provinciale per i Servizi Sanitari della Provincia Autonoma di Trento. Sulla base di tale assetto, alcuni dati dell'interessato (comuni e riferiti allo stato di salute), qualora strettamente necessari per consentire l'erogazione dei servizi sopra evidenziati, potranno essere condivisi tra i contitolari. Ogni informazione riferita a tale rapporto di contitolarità può essere richiesta presso i nostri uffici.

Durata del trattamento e periodo di conservazione
L'ente si impegna ad applicare i criteri di conservazione stabiliti dalla normativa vigente e dal proprio Massimario di scarto. Le cartelle cliniche sono per legge soggette a conservazione illimitata.

Diritti dell'interessato
Relativamente ai dati medesimi l'interessato o un suo rappresentante può esercitare, senza particolari formalità, i diritti previsti dagli articoli dal 18 al 21 del GDPR, tra cui chiedere se esistano o meno dati relativi alla sua persona e ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione; ricevere informazioni sull'uso dei dati personali; chiedere l'accesso, la rettifica, la cancellazione, la portabilità, la trasformazione in dati anonimi, il blocco, la limitazione o l'opposizione al trattamento che la riguarda. Infine, per motivi legittimi, può opporsi, in tutto o in parte, alla raccolta e all'utilizzo dei dati personali, facendo riferimento al predetto responsabile del trattamento presso gli uffici amministrativi dell'ente.
L'interessato può rivolgersi al titolare per ottenere ogni informazione nel merito del trattamento svolto, con particolare attenzione alla gestione informatizzata della propria documentazione sanitaria, nonché per revocare l'eventuale consenso al loro trattamento mediante dossier sanitario per esercitare la facoltà di oscuramento di alcuni eventi clinici ivi riportati.
L'interessato può inoltre proporre reclamo al Garante per la protezione dei dati personali mediante le coordinate di contatto o protocollo@pec.gpdp.it o anche tramite la procedura messa a disposizione dal titolare.

Informazioni sul Titolare del trattamento dati
Il Titolare del trattamento è AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA "SAN GIUSEPPE" DI PRIMIERO
Le coordinate di contatto del titolare sono le seguenti:
telefono Segreteria (0439) 62371 - Infermeria ((0439) 64620
mail: segreteria@apsp-primiero.net
pec: segreteria@pec.apsp-primiero.net

Informazioni sul Responsabile Protezione Dati (RPD)
La nostra Amministrazione ha designato U.P.I.P.A. Sc con sede a Trento, Via Sighele, quale proprio responsabile per la protezione dei dati personali raggiungibile all'indirizzo: serviziodpo@upipa.tn.it.

La versione sempre aggiornata di questa informativa sarà pubblicata sul sito https://www.apsp-primiero.net/privacy-policy alla sezione Privacy che l'interessato è inviata a visitare con regolarità.

CONSENSO AL TRATTAMENTO DEI DATI

Il sottoscritto	

oppure

Il sottoscritto	
In qualità di	**legale rappresentante, famigliare, prossimo congiunto, convivente del signor/della signora** _____

acquisite le informazioni fornite dal titolare del trattamento ai sensi dell'art. 13 del Reg.Ue 16/679

[ ] consente [ ] non consente

alla gestione informatizzata della propria documentazione sanitaria autorizzandone l'allocazione nel dossier sanitario elettronico con

[ ] il recupero dei dati dati storici [ ] senza il recupero dei dati storici

e

[ ] autorizza la consultazione al personale della APSP coinvolto nel processo di cura

L'interessato chiede/non chiede che il proprio nome e cognome venga indicato nella segnaletica posizionata all'ingresso della propria stanza di degenza (in caso di risposta negativa verrà esposto nome per esteso e cognome con iniziale puntata).

luogo, data firma

_____ _____

L'interessato, acquisite le relative informazioni, in riferimento ai

DATI SOGGETTI A MAGGIOR TUTELA DELL'ANONIMATO
(dati relativi a violenza sessuale o pedofilia,
infezioni da HIV,
uso di sostanze stupefacenti, psicotrope, alcool,
interventi di interruzione della gravidanza)

[ ] consente [ ] non consente

all'inserimento/consultazione dei predetti dati nel fascicolo sanitario/dossier sanitario

L'interessato autorizza il titolare del trattamento a poter comunicare i propri dati relativi allo stato di salute, ai soggetti di seguito indicati:

ALTRESÌ

☐ presta
☐ non presta
il proprio consenso per la raccolta e la diffusione del proprio ritratto fotografico per i fini indicati nella predetta informativa

luogo, data firma

_____ _____

Firmato digitalmente da

DANIELA SCALET

CN = SCALET DANIELA
C = IT

AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA
"SAN GIUSEPPE" DI PRIMIERO
Viale Marconi, 19 - Pieve
38054 PRIMIERO SAN MARTINO DI CASTROZZA (TN)
Segreteria ☎ (0439) 62371 - fax 🖷 (0439) 765399
Infermeria ☎ (0439) 64620 - fax 🖷 (0439) 765406
Cod. Fiscale e P.iva 00374850220
E-mail: segreteria@apsp-primiero.net
Posta Elettronica Certificata: segreteria@pec.apsp-primiero.net
Sito Internet: https://www.apsp-primiero.net/

Primiero San Martino di Castrozza, 29/11/2018

DISCIPLINARE AZIENDALE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEI DIPENDENTI E DEI COLLABORATORI REG. UE 16/679

INDICE

PREMESSA

Le indicazioni contenute nel presente documento tengono conto del principio di responsabilizzazione c.d. "accountability" definito dal Regolamento Ue 16/679.

Il presente disciplinare viene adottato sulla base delle indicazioni contenute nel provvedimento generale del Garante per la protezione dei dati personali di data 1 marzo 2007, n. 13 ("Lavoro: le linee guida del Garante per posta elettronica e internet", G.U. n. 58 del 10 marzo 2007) ed ha per oggetto la definizione dei criteri e delle modalità operative di accesso ed utilizzo degli strumenti informatici, tra cui la rete Internet e il sistema di posta elettronica, da parte dei propri dipendenti e collaboratori.

Il presente documento è stato redatto tenuto conto degli obblighi di "adeguata informazione" prescritti dall'articolo 4, della legge n. 300/1970, come riscritto dall'art. 23 del d.lgs. n. 151/2015 ed entra in vigore nella data della sua sottoscrizione.

Si rende noto a tutti gli incaricati ammessi all'utilizzo di strumenti informatici del titolare che personale incaricato è autorizzato a compiere interventi tecnici e/o manutentori diretti a garantire la sicurezza e la salvaguardia del sistema informatico del titolare stesso (aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). Detti interventi potranno comportare l'accesso in qualunque momento ai dati ivi allocati, ivi compresi gli archivi di posta elettronica, nonché la possibilità di conoscere quali siano i siti internet acceduti dagli utenti abilitati alla navigazione. La stessa facoltà, per i medesimi fini, è estesa all'amministratore di sistema designato dal titolare.

1. DEFINIZIONI

POSTAZIONE DI LAVORO: personal computer, PC portatile o thin-client collegato alla rete informatica del titolare tramite il quale l'utente accede ai servizi informatici.
UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica.
LOG: archivio delle attività effettuate in rete dall'utente.
CREDENZIALI DI AUTENTICAZIONE: codice utente e password richieste dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.
WHITE LIST: elenco di siti che il datore di lavoro ritiene comunemente attinenti all'attività lavorativa svolta.
BLACK LIST: elenco di siti che presentano contenuti non attinenti all'attività lavorativa e, per questa ragione, sottoposti a filtri che si attivano qualora l'utente cerchi di accedervi.
TITOLARE DEL TRATTAMENTO: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 Reg UE 16/679).
INCARICATO: persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento di dati personali.
DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 Reg UE 16/679).

2. UTILIZZO DELLA RETE E DEL PERSONAL COMPUTER

2.1. L'utilizzo di tutti gli strumenti informatici di proprietà del titolare deve avvenire osservando regole di buona diligenza e prudenza, con senso di responsabilità e seguendo le istruzioni impartite dal titolare e dalle persone delegate.
2.2. L'uso degli strumenti informatici aziendali (PC, attrezzatura informatica, notebook, accesso alla rete internet, telefoni mobili, ecc.) è consentito unicamente agli utenti autorizzati mediante attribuzione di apposito incarico al trattamento. Ogni utilizzo dei predetti beni non inerente all'attività lavorativa è tassativamente vietato.
2.3. Le unità di rete sono aree di condivisione di dati ed informazioni strettamente legati all'attività lavorativa. I file ivi dislocati devono avere attinenza con le attività svolte da ciascun incaricato e qualunque file che non sia legato all'attività lavorativa non può essere ivi dislocato, nemmeno per brevi periodi. Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi.
2.4 Ogni utente è responsabile per l'uso riferito al proprio account ed è personalmente tenuto a conformarsi a modalità di utilizzo atte ad impedire accessi da parte di terzi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

2.5. Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, contribuiranno a garantire la sicurezza nell'accesso:
a) scegliere una password composta da almeno 8 caratteri alfanumerici che non contenga riferimenti che riconducano agevolmente all'incaricato;
b) la stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il blocco del computer;
c) la password è personale, riservata e non può essere ceduta o comunicata ad alcuno. E' pertanto vietato l'uso della password di altri utenti;
d) è obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta o almeno regolarmente ogni tre/sei mesi (trattamento dati sensibili/comuni);
e) per esigenze operative o di sicurezza e integrità del sistema e dei dati, il titolare, tramite l'Amministratore di sistema ha facoltà di modificare la password degli utenti;
f) qualsiasi attività svolta utilizzando un codice utente e la relativa password sarà ricondotta nella sfera di responsabilità dell'utente assegnatario del codice. L'utente è civilmente responsabile di ogni danno cagionato al titolare, all'Internet Provider e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi il suo codice utente e password;
2.6. Per evitare il pericolo di introdurre virus informatici o di alterare la stabilità delle applicazioni è vietato scaricare ed installare programmi, salva espressa autorizzazione da parte del titolare o dell'Amministratore di sistema.
2.7. Non è consentito modificare le configurazioni del proprio PC. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.
2.8. Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
2.9. Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni, deve darne immediata comunicazione al titolare o all'Amministratore di Sistema. Salvo preventiva espressa autorizzazione non è consentito eseguire operazioni di manutenzione ordinaria o straordinaria autonomamente.
2.10 Non è consentito archiviare sul proprio pc, sul server o su qualunque altra area condivisa, file e dati non inerenti alla propria attività lavorativa.
2.11 E' vietato l'uso masterizzatori o altri supporti di registrazione di dati (ad es. dischi fissi esterni, chiavette USB, ecc.) per registrare dati salvi i casi direttamente autorizzati.
2.12 Il titolare del trattamento si riserva la facoltà di procedere alla rimozione di ogni applicazione o file ritenuti pericolosi per la sicurezza del sistema, non attinenti all'attività lavorativa o acquisiti ed installati in violazione del presente disciplinare, sia sui PC degli incaricati sia sulle unità di rete.
2.13 L'utente è tenuto alla periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili o duplicati onde evitare un'archiviazione ridondante.
2.14 L'utente deve limitare le stampe dei dati solo a quelle strettamente necessarie, ritirandole prontamente dai vassoi delle stampanti comuni.
2.15 E' fatto divieto di accedere contemporaneamente con lo stesso account da più PC.
2.16 Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di: utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti, utilizzare software rivolti alla violazione della sicurezza del sistema e della privacy; sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate; modificare le configurazioni impostate dall'amministratore di sistema; limitare o negare l'accesso al sistema a utenti legittimi; effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc.); distruggere o alterare dati altrui; collegare in rete personal computer non di proprietà del titolare.

3. UTILIZZO DI PC PORTATILI

3.1 L'utente al quale venga assegnato un computer portatile ne è responsabile e dovrà custodirlo con la dovuta diligenza sia durante l'utilizzo nel luogo di lavoro.
3.2 In caso di utilizzo all'esterno del luogo di lavoro, i notebook dovranno essere custoditi con attenzione e conservati in luogo sicuro. PC portatili e Tablet potrebbero essere dotati della funzione di localizzazione geografica. Tale funzionalità deve essere disattivata dall'utente.
3.3 Al computer portatile si applicano le regole sopra indicate per i PC connessi in rete, con particolare attenzione alle disposizioni concernenti i profili di accesso (password).
3.4 Sull'hard disk devono essere conservati solo i file strettamente necessari all'attività lavorativa, rimuovendo comunque, prima della restituzione, quelli elaborati ed ivi salvati.
3.5 E' necessario collegarsi periodicamente e, almeno, con cadenza settimanale, alla rete interna per consentire gli aggiornamenti dell'antivirus, del sistema operativo, nonché la sincronizzazione della posta elettronica e relative cartelle pubbliche.
3.6 E' fatto divieto di utilizzare abbonamenti Internet privati per collegarsi alla rete.

4. UTILIZZO DELLA RETE INTERNET

4.1 L'accesso alla rete Internet può essere effettuato da qualsiasi utente che sia autenticato (credenziali di accesso) su una qualsiasi postazione di lavoro connessa. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
4.2 Il lavoratore deve ricordare che Internet è uno strumento di lavoro e quindi che è possibile che il datore di lavoro, per ridurre i casi di utilizzo improprio (es: visione di siti non correlati all'attività lavorativa, download di file e software, uso della rete per finalità completamente estranee alla propria mansione, ecc.), adotti misure atte ad evitare l'esercizio di un controllo a posteriori dei lavoratori. Fra queste misure si possono enumerare l'individuazione di white list (composte da soli siti istituzionali, rispetto ai quali la navigazione è correlata e funzionale allo svolgimento della prestazione lavorativa) o black list (composte da tutti quei siti che, oltre a non avere attinenza con il lavoro, presentano contenuti non in linea con le politiche di gestione adottate dal titolare) ovvero tramite l'impostazione di filtri sul firewall (soluzione adottata dal titolare).
4.3 E' vietato il download di software gratuiti (freeware) e shareware nonché di file video o musicali prelevati da siti Internet, salvi i casi direttamente autorizzati dal titolare.
4.4 E' vietata ogni forma di registrazione a siti, newsletter, blog e quant'altro assimilabile, salvi i casi direttamente autorizzati. È vietata la partecipazione a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) salvi i casi direttamente autorizzati.
4.5 È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvi i casi direttamente autorizzati.
4.6 Non è consentito accedere ed utilizzare la rete internet in modo difforme da quanto previsto dal presente disciplinare e, ovviamente, dalle leggi penali, civili ed amministrative in materia. In ogni caso, ogni utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.
4.7 Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni è tenuto a darne immediata comunicazione al titolare.
4.8 Gli eventuali controlli, compiuti dal titolare per il tramite di personale incaricato, potranno avvenire mediante un sistema di analisi dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre un mese, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del titolare.

5. UTILIZZO DELLA POSTA ELETTRONICA

5.1 Il sistema di posta elettronica attivato sulla rete della società è da intendersi quale strumento di lavoro e come tale deve essere utilizzato.
5.2 Può essere assegnato un account di posta elettronica ad ogni utente della rete informatica o indirizzi condivisi tra più utenti.
5.3 L'accesso al sistema di posta elettronica è protetto dalla richiesta di autenticazione.
5.4 Le disposizioni di seguito riportate sono enucleate al fine di garantire un corretto utilizzo della strumento di posta elettronica:
a) all'utente non è consentito servirsi dell'account fornito dal titolare per l'invio di mail non connesse con l'attività e la mansione svolta (es: mail a contenuto privato, giochi, appelli, petizioni, catene di S. Antonio, ecc.);
b) si deve evitare di allegare al testo delle comunicazioni materiale potenzialmente insicuro o file di dimensioni eccessive. In quest'ultimo caso si dovranno utilizzare formati compressi (zip, rar, ecc.);
c) nel caso di mittenti sconosciuti o di messaggi dall'oggetto insolito, è consigliata l'eliminazione senza l'apertura del messaggio. Lo stesso vale nel caso di messaggi provenienti da mittenti conosciuti che tuttavia presentano allegati con particolari estensioni (es: .exe, .scr, .pif., .bat..);
d) nel caso in cui si debba inviare un documento all'esterno, è preferibile utilizzare un formato protetto da scrittura (es: Acrobat);
e) si deve evitare l'invio di mail che contengano categorie particolari di dati personali; qualora ciò sia necessario per determinate esigenze, questi devono essere inviati comunicando al richiedente un codice identificativo per ogni soggetto e trasmettendo separatamente il documento privo del nominativo dell'interessato e crittografando i file con password che dovrà essere comunicata al destinatario del messaggio per altro mezzo;
f) qualora il messaggio debba essere inviato a più soggetti, gli indirizzi vanno inseriti solo nel campo "CCn" per tutelare la riservatezza dei medesimi, che ricevono il messaggio conoscendo solamente il mittente;
g) prevedere, in caso di assenza prolungata del lavoratore (es: ferie), l'invio di messaggi di risposta automatica che indichino la durata dell'assenza ed il nominativo del soggetto al quale è possibile rivolgersi;
h) l'iscrizione a mailing list o newsletter è concessa solo per motivi strettamente professionali: prima di iscriversi è necessario verificare l'affidabilità ed ottenere l'autorizzazione del titolare;
i) l'intestatario dell'account ha facoltà di delegare ad altri il diritto d'accesso allo strumento in caso di assenza prolungata ai fini di garantire la continuità nell'attività lavorativa. Il fiduciario dovrà essere scelto e nominato fra i colleghi e, qualora dovesse accedere alla casella di posta della persona assente, non potrà comunque considerare i messaggi che presentino contenuto non attinente alle motivazioni per cui si effettua l'accesso.
l) il titolare, l'Amministratore di sistema o chi da essi incaricato può avere accesso all'account a seguito del riscontro di situazioni che abbiano pregiudicato il funzionamento del sistema.
5.5 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
5.6 I documenti inerenti il know how aziendale tecnico o commerciale protetto non possono essere comunicati all'esterno senza la preventiva autorizzazione del titolare.

6. PROTEZIONE ANTIVIRUS

6.1 L'utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico del titolare mediante virus o mediante ogni altro software aggressivo.
6.2. Qualora il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) segnalare l'accaduto all'amministratore di sistema.

6.3. Non è consentito l'utilizzo di cd/dvd rom, cd/dvd rescrivibili, nastri magnetici, chiavette per porte USB di provenienza ignota.
6.4. In caso di utilizzo autorizzato dei suddetti dispositivi, si dovrà procedere alla verifica degli stessi e nel caso in cui vengano rilevate anomalie alla loro consegna all'amministratore di sistema.

7. INTERRUZIONE D'UFFICIO DEL SERVIZIO

7.1 Il titolare si riserva di sospendere temporaneamente il servizio di accesso ad Internet e alla posta elettronica nei seguenti casi:
a) qualora venga meno la condizione di dipendente o collaboratore;
b) qualora si accerti un uso non corretto del servizio e degli strumenti informatici messi a disposizione;
c) in caso di manomissioni e/o interventi impropri su hardware/software;
d) in caso di diffusione o di comunicazione imputabile direttamente o indirettamente all'utente relativamente a profili d'accesso o altre informazioni tecniche riservate;
e) accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione.

8.UTILIZZO DEL TELEFONO

8.1 Il telefono è uno strumento di lavoro e come tale deve esser utilizzato. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.
8.2. Eventuali telefonate a carattere privato potranno essere effettuate con moderazione ed in casi di necessità.
8.3 I cellulari e gli smartphone affidati agli utenti per rendere la prestazione lavorativa sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa. Gli utenti cui è assegnato un cellulare o uno smartphone aziendale sono responsabili del suo utilizzo e della sua custodia. Al cellulare aziendale e allo smartphone si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare o dello smartphone messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
8.4 I cellulari e gli smartphone potrebbero essere dotati della funzionalità di localizzazione geografica. Tale funzione deve essere disattivata dall'utente. E' vietato effettuare il Jailbreak del dispositivo e più in generale è vietata qualsiasi procedura di sblocco del device aziendale assegnato, ad esempio, per installare/utilizzare applicazioni non autorizzate.

9. CONTROLLI E SANZIONI DISCIPLINARI

9.1. Sono interdetti al datore di lavoro controlli del personale dipendente effettuati in maniera diretta, prolungata, costante o indiscriminata (art. 4, Statuto dei lavoratori, l. 300/1970). Ciò premesso, oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo diretto dell'attività lavorativa, è facoltà del titolare tramite gli addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.
9.2. Il titolare può avvalersi di sistemi controllo relativi al corretto utilizzo degli strumenti informatici messi a disposizione dei propri collaboratori e dipendenti che consentano indirettamente un controllo a distanza sull'effettivo adempimento della prestazione lavorativa: tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti per evitare comportamenti anomali.

9.3. I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza. In seguito si espongono le modalità di esercizio di tali controlli: in prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di ufficio o gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole prestabilite.
Il controllo anonimo può dare atto ad un avviso di rilevazione di un utilizzo inadeguato degli strumenti aziendali; contestualmente si diramerà una nota di richiamo invitando tutti i dipendenti e collaboratori ad attenersi ai compiti e alle mansioni impartite tenuto conto del dovere di conformarsi alle presenti regole.
Se si dovesse ripetere l'anomalia sarà facoltà della società procedere con controlli mirati, anche su base individuale, e successivamente, in caso di infrazioni, adottare sanzioni disciplinari.
9.4. L'adozione delle sanzioni disciplinari avverrà a norma dell'art. 2106 c.c. del codice civile, dell'art. 7 dello statuto dei lavoratori (legge 300/1970), del contratto di riferimento e del relativo codice disciplinare vigente.
9.5. I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, possono essere conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza. I file di log potranno essere utilizzati in tali casi:
a) produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima;
b) per l'analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima.

10. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

10.1 Oltre al rispetto del presente regolamento è fatto obbligo di attenersi scrupolosamente alle disposizioni in materia di trattamento dati personali e alle relative misure di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento e nel materiale formativo messo a disposizione di ciascun collaboratore e dipendente osservando con attenzione le prescrizioni del Reg. UE 16/679.
Ciascun incaricato assume la piena responsabilità nel merito dell'osservanza del modello organizzativo, delle misure di sicurezza, delle indicazioni fornite dall'amministratore di sistema o dal responsabile per la protezione dei dati, se designato.
Ciascun incaricato è tenuto a mantenere un costante flusso informativo con il responsabile per la protezione dei dati personali, segnalando a quest'ultimo ogni eventuale criticità o violazione sul sistema di sicurezza adottato.

11. AGGIORNAMENTO E REVISIONE DEL DISCIPLINARE INTERNO

11.1 Il presente Regolamento è soggetto a verifica con eventuali revisioni ed aggiornamenti con periodicità annuale e, comunque, in caso di modifiche e/o integrazioni della normativa di legge.
11.2 Al presente disciplinare interno viene data pubblicità mediante affissione in bacheca anche ai sensi e per gli effetti dell'art. 7 legge 10 maggio 1970 n. 300 in relazione al codice disciplinare del quale costituisce parte integrante.

Primiero San Martino di Castrozza, 29/11/2018

Il titolare
La Presidente
Daniela Scalet

PROCEDURA DA APPLICARE IN CASO DI DATA BREACH
artt. 33 e 34 Regolamento UE 2016/679
Rev. 02/22

LISTA DELLE REVISIONI

REVISIONE N.	DATA	DESCRIZIONE DELLE MODIFICHE
00	25/5/2018	Prima emissione (in allegato al Registro dei trattamenti)
01	ottobre 2019	revisione del documento e degli allegati: registro delle violazioni; modello notifica al Garante
02	22/7/22	Modifica punto 4) dell' istruzione del data breach Allegato nr. 4 "notifica della violazione al Garante". Modifica modalità

DEFINIZIONE DEL DATA BREACH

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "**violazione dei dati personal**i".

L'articolo 4 p.12 del GPDR definisce la "**violazione dei dati personali**" come 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.

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

Le violazioni possono essere classificate in tre macro categorie che, a seconda dei casi, possono riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali (anche in combinazione).

1) "**violazione della riservatezza**" in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

2) "**violazione dell'integrità del dato**" in caso di modifica non autorizzata o accidentale dei dati personali;

3) "**violazione della disponibilità del dato**", in caso di perdita o distruzione accidentali o non autorizzati di dati personali.

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

A seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'Autorità di controllo e la comunicazione alle persone fisiche coinvolte.

Il titolare del trattamento, riscontrata una violazione, dovrà pertanto di volta in volta valutare la probabilità e la gravità del conseguente impatto sui diritti e sulle libertà delle persone fisiche e:

a) documentare la violazione nel proprio Registro delle violazioni (sempre);
b) effettuare la notifica al Garante (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
c) comunicare la violazione ai soggetti interessati (laddove possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte).

SCOPO e CAMPO DI APPLICAZIONE

La presente procedura definisce le modalità di gestione del "data breach" che l'Ente, titolare del trattamento, è tenuto ad osservare e far rispettare ai propri preposti.

RESPONSABILITÀ

La responsabilità legata alla presente procedura è del titolare del trattamento.

RIFERIMENTI NORMATIVI

REGOLAMENTO (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

PROCEDURA DA APPLICARE IN CASO DI DATA BREACH
artt. 33 e 34 Regolamento UE 2016/679

Rev. 02/22

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205) e modifica il d.lgs. 196/03;
LINEE GUIDA IN MATERIA DI NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.

MODALITÀ' OPERATIVE E GESTIONE DELL'EVENTO

In caso di accertamento di violazione che rientra nella definizione di "data breach" il titolare del trattamento procede come di seguito dettagliato:

1. provvedere all'acquisizione e all'immediata gestione della notizia;
2. compiere un'analisi dell'evento;
3. adottare le misure di riduzione del danno;
4. valutare la gravità dell'evento;
5. notificare il "data breach" al Garante Privacy (laddove necessario);
7. procedere con la comunicazione agli interessati (se necessario);
8. inserire l'evento nel proprio Registro delle violazioni;
9. attivare tutte le azioni correttive per ridurre il ripetersi dell'evento.

Si descrivono di seguito le modalità operative per dare esecuzione a quanto sopra:

1) acquisizione e immediata gestione della notizia (da fonti interne o esterne)

La rilevazione/segnalazione di un data breach può essere di fonte interna o esterna all'Ente.

POSSONO ESSERE FONTI INTERNE: notizie ricevute da parte del personale dipendente; da parte del personale convenzionato/stagisti/tirocinanti; dall'amministratore di sistema (ove presente); dalle figure preposte alla manutenzione degli impianti informatici o alla gestione degli archivi; dagli utenti dei servizi.

SONO FONTI ESTERNE: notizie ricevute da parte delle forze dell'ordine; da parte dei responsabili del trattamento; da parte del DPO; da parte degli interessati; da parte di terzi.

La segnalazione, qualunque sia la forma, deve essere immediatamente messa a conoscenza del legale rappresentante dell'Ente, della Direzione, dell'amministratore di sistema (soggetti che compongono il "**gruppo di gestione del data breach aziendale**") attraverso canali di posta elettronica (pec) e avvertimento verbale/telefonico.

2) analisi dell'evento

Il gruppo di gestione del data breach aziendale è tenuto a compiere un'**analisi dell'evento** riscontrato e/o segnalato verificando che l'episodio rappresenti effettivamente un "data breach" mettendo in atto, laddove possibile, tutte le appropriate misure per l'immediato contenimento del danno.

L'attività di analisi riguarderà:
- una verifica della violazione (se di riservatezza, di integrità o di disponibilità);
- l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- l'identificazione degli interessati;
- il livello di gravità dell'evento;
- le misure di sicurezza presenti;
- le immediate azioni di riduzione delle conseguenze.

Tutte le operazioni effettuate devono essere verbalizzate e la rilevazione della violazione deve contenere almeno i seguenti elementi:

Breve descrizione della violazione dei dati personali	
Quando si è verificata la violazione dei dati personali	
Dove è avvenuta la violazione dei dati	
Dispositivo oggetto della violazione	

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	
Quante persone sono state colpite dalla violazione dei dati personali	
Che tipo di dati sono oggetto di violazione	
Livello di gravità della violazione dei dati personali	
Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future	

Senza ingiustificato ritardo e non oltre 12 ore dall'evento il gruppo di gestione del data breach aziendale comunicherà l'episodio (segnalazione) e la risultanza della prima analisi al DPO mediante le coordinate di posta elettronica pec e avvertimento verbale/telefonico.

3) valutazione della gravità dell'evento
Il gruppo di gestione del data breach aziendale, con il supporto di tutte le risorse competenti, dovrà appurare se l'evento merita di essere notificato al Garante **considerando la probabilità o meno che l'evento possa comportare dei rischi per i diritti e la libertà delle persone.**

Nella fase di valutazione occorre stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli interessati.

La notifica al Garante è necessaria laddove si sia verificata una violazione (distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno dell'Ente) caratterizzata da effetti negativi significativi sulle persone fisiche, che possa causare danni fisici, materiali o immateriali (ad esempio la perdita del controllo da parte degli interessati sui loro dati personali), la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate.

Nella valutazione si devono prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati.

La ponderazione si basa sui seguenti criteri: natura, carattere sensibile e volume dei dati personali violati; facilità di identificazione delle persone fisiche coinvolte; gravità delle conseguenze per le persone fisiche interessate; caratteristiche particolari dell'interessato; caratteristiche particolari del titolare del trattamento; numero di persone fisiche interessate; aspetti generali della violazione.

Nel caso in cui sussista tale possibilità il titolare effettua la notifica al Garante nei termini prescritti (72 ore) mediante il modello di notifica in allegato alla presente procedura.

Quando la verifica dei fatti renda "improbabile" che la violazione subita comporti un rischio per i diritti e le libertà delle persone fisiche, la notifica non è obbligatoria ed il titolare deve riportare l'episodio occorso e l'attività di gestione dello stesso nel proprio Registro delle violazioni.

4) notifica della violazione al Garante
La notifica, effettuata dal legale rappresentante o da persona a ciò delegata, verrà portata a compimento nei termini di legge, previa autovalutazione eseguita applicando lo schema accessibile al link https://servizi.gpdp.it/databreach/s/self-assessment tramite il servizio online disponibile sul sito istituzionale dell'Autorità Garante al link: https://servizi.gpdp.it/databreach/s/compilazione notifica.

5) comunicazione agli interessati
In caso di **elevato rischio per la libertà e i diritti degli individui**, si provvederà ad informare gli interessati tramite i canali istituzionali dell'ente sul fatto avvenuto, sui dati violati e sulle procedure adottate o adottande per ridurre il rischio.

Il titolare del trattamento deve fornire agli interessati almeno le seguenti informazioni:

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

La comunicazione agli interessati non è richiesta laddove:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche, immediatamente dopo una violazione;
- contattare gli interessati richiederebbe uno sforzo sproporzionato.

Copia di ogni comunicazione agli interessati dovrà essere conservata nel Registro delle violazioni.

6) inserimento dell'evento nel Registro delle violazioni
Il titolare documenta qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Il gruppo di gestione del data breach aziendale è responsabile dell'inserimento di tutte le attività indicate sopra nel registro delle violazioni, che devono essere documentate, tacciabili, e in grado di fornire evidenza nelle sedi competenti.