AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA
CASA PER ANZIANI
Viale Trieste, n. 42
Cividale del Friuli - C.A.P. 33043 (UD)
Tel. 0432 731048 / 732039 - Fax 0432 700863
Part. IVA 02460260306
email: protocollo@aspcividale.it *pec:* postacert@pec.aspcividale.it
www.aspcividale.it

Regolamento Privacy attuativo del Regolamento UE/2016/679 (GDPR - General Data Protection Regulation) in materia di protezione dei dati personali

Approvato con delibera del Consiglio di Amministrazione n. 15 del 24/09/2020

Sommario

Articolo 1
Finalità

Il presente Regolamento disciplina il trattamento dei dati personali raccolti presso l'Azienda pubblica di servizi alla persona presso "A.S.P. Casa per Anziani di Cividale del Friuli", di seguito denominata Azienda, nel rispetto di quanto previsto dal D.lgs. n.196 del 30.06.2003 e successive modificazioni e dal Regolamento (UE) 2016/679 (General Data Protection Regulation), di seguito denominato GDPR.

Articolo 2
Oggetto del trattamento

E' oggetto di trattamento qualsiasi informazione riguardante una persona fisica identificata o identificabile direttamente o indirettamente attraverso il nome, un numero di identificazione, dati relativi allocazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Per trattamento si intende 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.

Articolo 3
Principi per il trattamento dei dati personali

I dati vengono trattati nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato nonché degli obblighi di correttezza, liceità e trasparenza imposti dal D.lgs. n.196 del 30.06.2003 e successive modificazioni e dal Regolamento UE 2016/679 GDPR.
La finalità e la base giuridica del trattamento, cui sono destinati i trattamenti dei dati personali rientrano nei compiti istituzionale dell'Azienda e riguardano in particolare:

- l'esercizio delle funzioni amministrative e fiscali che riguardano gli Ospiti/Clienti;
- la gestione dei dati socio-sanitari contenuti nelle cartelle individuali degli Ospiti/Clienti;
- la gestione dei dati anagrafici dei famigliari degli utenti ai fini delle attività amministrative;
- la gestione delle rilevazioni statistiche al fine di ottimizzare l'efficienza organizzativa;
- la programmazione e pianificazione/esecuzione delle attività di animazione e socializzazione;
- l'erogazione di prestazioni e interventi, socio-assistenziali e socio-sanitari ed attività amministrative connesse.

Articolo 4
Titolare del trattamento

Il Titolare del trattamento (data controller) è l'Azienda pubblica di servizi alla persona "A.S.P. Casa per Anziani di Cividale del Friuli" ", rappresentata dal legale rappresentate pro tempore – Viale Trieste, 42 33043 Cividale del Friuli - e-mail: protocollo@aspcividale.it; PEC: postacert@pec.aspcividale.it
Ai sensi dell'articolo 24 del Regolamento UE 2016/679 GDPR (General Data Protection Regulation), il Titolare del trattamento è tenuto in particolare a:

- mettere in atto le misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente
- garantire la riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- designare il responsabile del trattamento a cui affidare mansioni importanti e di elevata professionalità, in fase di gestione dei dati personali;
- designare gli incaricati del trattamento tra le persone dell'organizzazione aziendale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni

organizzative di loro competenza.

Articolo 5
Responsabile della protezione dati o DPO (Data Protection Officer)

Il Responsabile del trattamento e della protezione dei dati (DPO) dell'Azienda viene individuato ai sensi della normativa vigente in materia.

I dati del DPO sono pubblicati sul sito istituzionale dell'Azienda, sezione Amministrazione trasparente, oltre che nella sezione "privacy".

Al DPO sono affidate le seguenti competenze:

- informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il DPO può indicare al Titolare i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
- sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare del trattamento;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessment - valutazione d'impatto sulla protezione dei dati) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il DPO in merito all'opportunità di condurre o meno una DPIA e sulle modalità da adottare per attivare tale procedura;
- cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione;
- altri compiti e funzioni a condizione che il Titolare del trattamento si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

II DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Articolo 6
Responsabile esterno del trattamento

Per il conseguimento degli scopi istituzionali dell'Azienda, i dati personali possono essere comunicati a Terzi opportunamente designati "Responsabili esterni del trattamento", quali altri Enti pubblici e Istituzioni centrali e periferiche, società di servizi di digitalizzazione dati, di archiviazione, dematerializzazione, conservazione documentale, gestione di posta elettronica, di banche dati, nonché istituti previdenziali, assicurativi, del Servizio Sanitario Nazionale e Regionale, Istituzioni giurisdizionali, Tesoriere dell'Azienda, Enti fornitori di servizi, Revisore dei conti.

L'esecuzione dei trattamenti da parte di un Responsabile esterno del trattamento è disciplinata da un atto di nomina, contenente:

- la durata del trattamento;
- la natura e le finalità del trattamento;
- il tipo di dati personali e le categorie di soggetti interessati;
- i compiti e le responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà delle persone fisiche interessate.

In particolare, il Responsabile esterno del trattamento è tenuto a:

- garantire la riservatezza delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a

conoscenza durante l'esecuzione della prestazione;

- utilizzare i dati solo per le finalità connesse allo svolgimento dell'attività oggetto del contratto, con divieto di qualsiasi altra diversa utilizzazione;
- adottare preventive misure di sicurezza atte 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, nel rispetto delle disposizioni contenute nel GDPR;
- adottare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- garantire di essere in regola con la normativa relativa al trattamento, conservazione e diffusione dei dati personali e sensibili di cui al GDPR;

Al Responsabile esterno è vietata:

- la produzione di copie dei dati personali e ogni tipo di trattamento non attinente allo scopo dei servizi offerti;
- a diffusione e la comunicazione di dati diversi da quelli previsti nel contratto o necessari per l'adempimento dello stesso. In nessun caso il Responsabile esterno acquisisce la proprietà intellettuale di dati e informazioni trattati nell'ambito di svolgimento del contratto.

Articolo 7
Incaricati interni del trattamento dati

Gli Incaricati interni del trattamento sono le persone fisiche, dipendenti dell'Azienda, incaricate del trattamento dei dati personali nello svolgimento della propria attività.
L'esecuzione dei trattamenti da parte di un Incaricato interno è disciplinata da un atto di nomina, diversificato in relazione alla tipologia di prestazioni svolte, contenente tutte le modalità cui i dipendenti dell'Azienda che vengono o possono venire a conoscenza dei dati personali degli Ospiti/Clienti, devono attenersi nel trattamento dei dati e l'indicazione dell'ambito del trattamento consentito.

Articolo 8
Incaricati esterni del trattamento dati

Le persone fisiche, non subordinati dell'Azienda che, in qualità di personale dipendente delle Ditte affidatane dei servizi assistenziali, tirocinanti, volontari, borsisti, soggetti sottoposti a misure alternative alla pena, che nello svolgimento delle attività concordate con i servizi/Enti territoriali competenti vengono o possono venire a conoscenza dei dati personali degli Ospiti/Clienti sono tenuti all'osservanza delle misure di sicurezza previste dal presente regolamento nonché alla sottoscrizione di un accordo, in merito all'obbligo di riservatezza su a ogni informazione e dato personale riferiti all'Azienda, clienti e dipendenti, con i quali dovessero anche accidentalmente venire a contatto.

Articolo 9
Informativa

L'informativa contiene tutte le informazioni che il Titolare del trattamento è tenuto a fornire al soggetto di cui deve trattare i dati personali e in particolare:

a. l'identità e i dati di contatto del Titolare del trattamento;
b. i dati di contatto del Responsabile del trattamento e della protezione dei dati;
c. le finalità del trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento;
d. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e. il periodo di conservazione dei dati personali;
f. l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

g. qualora il trattamento sia stato espresso per il consenso al trattamento dei dati personali per una o più specifiche finalità, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
h. il diritto di proporre reclamo a un'autorità di controllo;
i. se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tal dati;
j. l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art.22, paragrafi 1 e 4 del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato.

Qualora l'Azienda intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, dovrà fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Per assolvere all'obbligo di informazione previsto dall'articolo 13 del Regolamento (UE) 2016/679 in relazione ai dati personali forniti direttamente dell'interessato o dalle persone autorizzate l'Azienda ha predisposto l'informativa sul trattamento dei dati personali diversificata in relazione alla tipologia dei dati forniti nelle seguenti tipologie:

- per il trattamento dei dati personali degli Ospiti/Clienti;
- per il trattamento dei dati personali del personale dipendente;
- per il trattamento dei dati personal de i diversi soggetti che svolgono all'interno dell'Azienda attività di tirocinio, volontariato, borsa lavoro, misure alternative alla pena, ecc.;

Nelle altre ipotesi di trattamento dei dati in sede di bandi di gara, contratti, convenzioni, bandi di concorso pubblico, segnalazioni di disservizio ecc,.. sarà utilizzata la seguente informativa di massima, adattabile alla specifica fattispecie: *''Ai sensi del D.Lgs 196 del30.06.2003 e del DPGR UE/679/2016, i dati personali, anche di natura sensibile e giudiziaria, forniti in relazione alla presente procedura, saranno trattati esclusivamente per le finalità di gestione della medesima e dell'eventuale rapporto contrattuale ad essa conseguente'.*

Articolo 10
Consenso al trattamento dei dati

Il consenso è la libera manifestazione dell'interessato o dalle persone autorizzate ad acconsentire al trattamento dei suoi dati personali, dopo che è stato preventivamente informato tramite l'informativa di cui al precedente articolo 9.
Il consenso deve essere espresso mediante un atto positivo inequivocabile con il quale l'interessato o le altre persone autorizzate manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali.

Articolo 11
Sicurezza del trattamento

Il principio di integrità e riservatezza stabilisce che i dati devono essere sempre trattati in modo da garantirne una sicurezza adeguata. Pertanto l'Azienda è tenuta ad adottare misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.
Le misure tecniche ed organizzative di sicurezza messe in atto e che si intende adottare per ridurre i rischi del trattamento comprendono:

- la pseudonimizzazione (utilizzo di sigle per identificare l'utente);
- la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- sistemi di autenticazione alle postazioni di lavoro (password personali e riservate per ogni incaricato

trattamento dati rinnovate ogni 3 mesi);
- sistemi di autorizzazione all'accesso degli applicativi;
- sistemi di protezione (antivirus; firewall; antintrusione);
- sistemi di rilevazione di intrusione (allarme attivato in ogni struttura ed in sede);
- registrazione accessi (tramite apposito software che rileva ogni accesso agli archivi dati);
- sistemi di archiviazione e conservazione di archivi elettronici con accesso univoco e solo previa autorizzazione, effettuato esclusivamente da personale addetto;
- altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

L'Azienda e il DPO, tenendo conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, si impegnano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

Articolo 12
Registro delle attività di trattamento

Il Registro delle attività di trattamento è un documento contenente le seguenti informazioni relative alle operazioni di trattamento svolte:

a. il nome ed i dati di contatto dell'Azienda, ai sensi del precedente art.4;
b. le finalità del trattamento;
c. la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e. l'eventuale trasferimento di dati personali verso un ente terzo;
f. ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

L'Azienda redige il Registro, con personale all'uopo incaricato, in forma cartacea o informatizzata e lo conserva presso gli uffici amministrativi.

Esso rappresenta un elemento di accountability, dal momento che risulta essere un valido strumento per fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile ai fini della valutazione o analisi del rischio.

Articolo 13
Valutazioni d'impatto sulla protezione dei dati

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Azienda, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, GDPR.
Fermo restando quanto indicato dall'art. 35, p. 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a. trattamenti valutativi o di scoring, compresa la probazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;
e. trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f. combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g. dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche/organizzative;
i. tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che l'Azienda ritenga motivatamente che non può presentare un rischio elevato.
L'Azienda può inoltre motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri occorra comunque la conduzione di una DPIA.
L'Azienda garantisce l'effettuazione della DPIA ed è responsabile della stessa e può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Azienda.
Il DPO può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.
La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non verranno modificate, sostituite od abrogate.
La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a. descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b. valutazione della necessità e proporzionalità dei trattamenti, sulla base:
    - delle finalità specifiche, esplicite e legittime;
    - della liceità del trattamento;
    - dei dati adeguati, pertinenti e limitati a quanto necessario;
    - del periodo limitato di conservazione;
    - delle informazioni fornite agli interessati;
    - del diritto di accesso e portabilità dei dati;
    - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
    - dei rapporti con i responsabili del trattamento;
    - delle garanzie per i trasferimenti internazionali di dati;
    - consultazione preventiva del Garante privacy;
c. valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità

dei dati) dal punto di vista degli interessati;

d. individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

L'Azienda può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

L'Azienda è tenuta a consultare il Garante Privacy prima di procedere al trattamento nelle seguenti fattispecie:

- se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato;
- nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

E' pubblicata sul sito istituzionale dell'Azienda e, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Articolo 14
Violazione dei dati personali

Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Azienda.

L'Azienda, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante della Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

Il DPO è obbligato ad informare l'Azienda, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari). Se l'Azienda ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve essere effettuata con le modalità indicate dall'art. 33 del GDPR.

Devono essere opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di

verificare il rispetto delle disposizioni del GDPR.

Articolo 15
Rinvio

Per tutto quanto non espressamente disciplinato dal presente Regolamento, si applicano le disposizioni previste dal D. Lgs 196 del 30.06.2003, i provvedimenti specifici del Garante per la protezione dei dati personali, nonché le disposizione del Regolamento Europeo 679/2016.

Il Decreto Legislativo 30 giugno 2003 n. 196 sulla tutela della riservatezza nel trattamento di dati personali ha introdotto rilevanti obblighi, obblighi la cui inosservanza è sanzionata penalmente ed espone a responsabilità civili.
Questa decreto ha la finalità di garantire che il trattamento di dati personali si svolga nel pieno rispetto dei diritti dell'interessato, sia esso persona fisica che società, ente od associazione.
La legge prescrive (art. 30) che vengano impartite da parte del titolare specifiche istruzioni agli "incaricati del trattamento" e, cioè, a coloro che, nell'ambito dell'organizzazione stessa ed in relazione alle mansioni affidate, trattano dati personali sia mediante sistemi informatici che mediante documenti cartacei.

Accesso a banche dati

Le banche dati cui è autorizzato ad accedere per effettuare i trattamenti (sia informatici che cartacei), sono strettamente pertinenti alle mansioni svolte e per le finalità previste, il trattamento rispetta i principi fondamentali sanciti dall'art. 11 del decreto legislativo n.196/2003. Senza preventiva autorizzazione del titolare del trattamento non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso. L'incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai soggetti esterni come previsto da specifiche normative in merito. Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta.

Misure di sicurezza

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dall'Ente, nonché quelle che in futuro verranno comunicate.

Accesso ai locali

Il primo livello di protezione di qualunque sistema è quello fisico. È certamente vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo o comunque una persona non autorizzata entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania o visibili su uno schermo.
Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre chiudete i documenti a chiave nei cassetti e/o negli armadi ogni volta che potete: non lasciate in nessun caso documenti incustoditi. I documenti stessi, una volta utilizzati, dovranno essere mantenuti nei luoghi e negli armadi designati come archivi per tale tipologia di dati.
L'accesso agli archivi contenenti dati sensibili o giudiziari dev'essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate.

Sistemi informatici

Credenziali di accesso
Per ogni incaricato viene creata una "credenziale di autenticazione" che consente l'accesso in rete ai dati, attraverso una procedura di autenticazione Ad ogni incaricato è stata assegnata in via riservata una credenziale per l'autenticazione che consiste in un codice identificativo (user id) ed una parola chiave riservata (password).
La parola chiave deve essere composta da almeno 8 caratteri (di cui un carattere numerico) e non deve contenere riferimenti facilmente riconducibili all'utilizzatore. Deve essere custodita dall'incaricato con la massima diligenza pertanto non può essere divulgata/comunicata ad altri. La password deve essere cambiata al suo primo utilizzo e, successivamente, almeno ogni sei mesi (trimestrale in caso di trattamento di dati sensibili o giudiziari). Non si dovranno in nessun caso utilizzare delle password già adoperate nel passato.
Si ricorda che l'Ente, titolare del trattamento, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall'incaricato ed agli strumenti informatici in dotazione allo stesso sia per le esigenze produttive sia per la sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), potrà accedere mediante intervento del custode delle credenziali nominato.

Allontanamento dalla postazione
La postazione informatica non va lasciata incustodita lasciando accessibili i dati. Ogni qualvolta sorgerà la necessità di assentarsi temporaneamente, non lasciare mai il computer utilizzato privo di una protezione di accesso. Per attuare ciò, in sistemi Windows, attivare la funzionalità di "blocca computer", richiedendo così la digitazione della password al successivo accesso e salvaguardando nel contempo il lavoro corrente. In tutti gli altri casi in cui non sia disponibile una funzionalità del tipo descritto, attivare necessariamente un salvaschermo con password, avendo cura di verificare che lo stesso sia entrato in azione prima di abbandonare il computer medesimo.

Spegnimento dell'elaboratore
Lasciare un computer acceso non crea problemi al suo funzionamento ed al contrario velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile poiché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza, maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno. Quindi, non lasciate mai il computer acceso se non per brevi assenze nell'arco della giornata. Anche in questo caso attenetevi alle indicazioni riportate nel paragrafo "Allontanamento dalla postazione". L'elaboratore in ogni caso deve essere spento ogni sera prima di lasciare gli uffici (salvo diverse disposizioni o in caso di particolare necessità).

Localizzazione dei dati trattati con strumenti elettronici
I dati trattati con strumenti elettronici dovranno essere conservati unicamente sul server. Tutte le volte che ciò non sia reso possibile, a causa dalle caratteristiche dei programmi utilizzati per specifici trattamenti di dati, concordare comunque con il titolare del trattamento e/o con gli amministratori di rete una idonea politica di backup.

Uso dell'apparecchiatura
Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer e/o di provvedere ad una normale manutenzione sistemica. Assicuratevi sempre dell'identità della persona e delle autorizzazioni ad operare sul vostro PC. In tutti gli altri casi non è consentito l'utilizzo del vostro PC da parte di personale esterno, salvo preventiva autorizzazione del titolare del trattamento. Caso particolare riguarda l'amministratore del sistema, al quale, il titolare o il responsabile concederà direttamente la relativa autorizzazione a procedere.

Installazione software
L'incaricato non può installare ed utilizzare programmi per elaboratore non autorizzati ne privi di licenza che legittimino l'uso. Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale. È quindi espressamente proibito installare autonomamente dei programmi sul

proprio computer; in ogni caso ogni installazione va preventivamente discussa e concordata con l'amministratore di sistema, al fine di valutare l'eventuale insorgenza di problematiche tecniche di altra natura.

Gli strumenti informatici e telematici messi a disposizione (a seconda dei casi: computer, software, navigazione su internet, e- mail) costituiscono degli strumenti di lavoro da utilizzare esclusivamente per l'esecuzione delle mansioni affidate.

Supporti di memoria

Alla conservazione dei supporti di memoria asportabili (CD, chiavette, ecc…) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate assolutamente sicuri che contengano solo informazioni non sensibili (in ogni caso è meglio farlo sempre), riponeteli sotto chiave non appena avete finito di usarli.

Stampe

Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania, recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate, cercate di usare una stampante non condivisa (se disponibile) oppure, ove sia possibile ciò, usate una modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più.
Se trattate dati di particolare riservatezza, non gettate mai documenti cartacei senza averli prima fatti a pezzi o distrutti mediante l'utilizzo della macchina distruggi documenti.

Antivirus

Su ogni postazione è installato un programma antivirus sempre attivo e con aggiornamento automatico della definizione dei virus. Con periodicità vengono eseguite le scansioni del PC, mentre è cura personale effettuare un'eventuale scansione di supporti di memoria esterni (chiavette). La presenza dell'antivirus garantisce una buona copertura di sicurezza, ma nonostante ciò si ricorda di fare attenzione nella navigazione e nell'uso della posta elettronica e si raccomanda di segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro, perché può essere il sintomo di un attacco in corso.

Utilizzo della rete Internet e della posta elettronica

Internet
L'utilizzo degli strumenti per la navigazione su Internet è sottoposto ad un sistema automatico di limitazione attiva.
Dall'interno della rete locale, quindi:

- è da evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione precedentemente menzionati;
- è tassativamente proibita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non connessi all'attività istituzionale, salvo che questi siano stati preventivamente autorizzati dal titolare o dal responsabile del trattamento.

Posta elettronica

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. Il rispetto di alcune semplici regole può aiutare a migliorare ulteriormente l'utilizzo dello strumento.
La casella di posta personale deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.
Evitare di utilizzare la casella di posta per l'invio e la ricezione di messaggi estranei al lavoro.

Per proteggersi da virus ed altri agenti attivi di attacco, diffidate di tutti i dati e programmi che vi vengono inviati o consegnati, anche se la fonte appare affidabile o il contenuto molto interessante.