Manuale Governance Privacy ai sensi del GDPR UE 2016/679
"POLICY AZIENDALI SULLA PRIVACY"

ED.	REV.	DATA	DESCRIZIONE	APPROV
00	00	18 /05/2018	Prima emissione	Il titolare del trattamento Cooperativa Sociale Nuova Sair *Rosario Riccioluti*
00	01	26/10/2018	Aggiornamento per revisione	Il titolare del trattamento Cooperativa Sociale Nuova Sair *Rosario Riccioluti*

INDICE

1 SCOPO

Scopo del presente manuale è quello di descrivere come la Cooperativa Sociale Nuova Sair Onlus gestisce i processi aziendali nel rispetto ed in ottemperanza della normativa sulla privacy, con particolare riferimento al Regolamento UE (GDPR) 2016/679 e s.m.i. e del D.Lgs. 196/2003 e s.m.i. in materia di protezione dei dati personali.

2 APPLICABILITA'

La presente procedura si applica alle attività svolte da Cooperativa Sociale Nuova Sair Onlus per tutte le attività interne, gestione del personale, gestione dei processi relativi ai clienti e gestione dei processi relativi agli utenti delle attività di carattere socio-sanitario gestite.

3 RIFERIMENTI

- UNI EN ISO 9001:2015 Sistema di Gestione per la Qualità - Requisiti
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e ss.mm.ii.
- Regolamento UE (GDPR) 2016/679 in materia di protezione dei dati personali e ss.mm.ii.

Valgono le definizioni riportate nella citata norma UNI EN ISO 9000 e nel Regolamento UE (GDPR) 2016/679 in materia di protezione dei dati personali.

4 RESPONSABILITÀ

La responsabilità generale delle attività descritte nella presente procedura è affidata al Titolare del Trattamento dei Dati.
Revisioni: Il presente documento è aggiornato a cura del Titolare del Trattamento con cadenza almeno annuale.

5 DIRETTIVE

Le seguenti direttive hanno lo scopo di fornire le istruzioni e le modalità operative necessarie da utilizzare come traccia per gli adempimenti richiesti dal Regolamento UE (GDPR) UE 2016/679. Queste direttive devono essere considerate complementari alle copie delle lettere di incarico e delle informative richieste dalla normativa.

- DIRETTIVA PER LA CLASSIFICAZIONE DEI DATIDIRETTIVA PER LA CLASSIFICAZIONE DEI TRATTAMENTI
- CRITERI PER LA DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI PERSONALI
- DIRETTIVA PER IL CONTROLLO DI ACCESSO AI DATI PERSONALI ED ALLE RISORSE DI TRATTAMENTO
- DIRETTIVA SULLE CREDENZIALI DI AUTENTICAZIONE
- DIRETTIVA PER LA PROTEZIONE FISICA DELLE AREE E DEI LOCALI
- DIRETTIVA PER IL CONTROLLO DEGLI ACCESSI FISICI
- DIRETTIVA PER L'INTEGRITÀ DEI DATI PERSONALI
- DIRETTIVA PER L'UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE E PER LE OPERAZIONI DI MANUTENZIONE O RIPARAZIONE
- DIRETTIVA PER LA PROTEZIONE DA PROGRAMMI MALIZIOSI, PER L'INDIVIDUAZIONE DI INTRUSIONI, PER GLI AGGIORNAMENTI DEI SOFTWARE
- DIRETTIVA PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI PERSONALI IN CASO DI INCIDENTE, DISASTRO O DATA BREACH
- DIRETTIVA PER LA TRASMISSIONE DEI DATI PERSONALI

- DIRETTIVA PER GARANTIRE L'ADOZIONE DI MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI ALL'ESTERNO DELL'ORGANIZZAZIONE
- PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA DEI DATI PERSONALI
- DIRETTIVA PER L'ANALISI DEI RISCHI

5.1 DIRETTIVA PER LA CLASSIFICAZIONE DEI DATI

SCOPO Per poter garantire una adeguata protezione ai dati personali occorre che questi siano conosciuti, ovvero riconosciuti e classificati almeno secondo i livelli di particolarità previsti dalla normativa vigente.
Questa Direttiva ha lo scopo di fornire lo strumento, in conformità a quanto previsto dal Regolamento UE (GDPR) 2016/679, per procedere alla classificazione dei dati trattati dal Titolare.
Sulla base della classificazione dei dati vengono determinati: il grado di protezione che deve essere applicato, il livello di conoscibilità (se ad es. possono essere conosciuti anche da terzi, ovvero possono essere diffusi, oppure se invece hanno una conoscibilità, o comunicabilità, limitata e, dunque, non devono essere conosciuti all'esterno della struttura, o comunicati, senza le prescritte autorizzazioni).
DATI Per dati si intendono tutte le informazioni che sono archiviate o condivise o comunque trattate dal Titolare o per conto di questi con qualsiasi mezzo ed a qualsiasi titolo senza che la successiva elencazione debba considerarsi tassativa, ad esempio: informazioni in formato elettronico, cartaceo, informazioni scambiate oralmente o visivamente (ad esempio per telefono o videoconferenza). Questi Criteri Generali devono essere applicati in modo coordinato alle attività normali dell'organizzazione affinché siano evitati disturbi e/o interferenze con la normale attività di questa.
AMBITO Tutti i dati trattati dal Sistema Informativo della struttura devono essere classificati nel rispetto della presente direttiva. Tutti coloro i quali partecipano a processi di trattamento dati, o svolgono incarichi, nell'ambito del sistema informativo siano essi dipendenti e/o collaboratori, anche esterni e saltuari, ovvero enti od organizzazioni autonome sono tenuti al rispetto della presente direttiva. Ai terzi che eventualmente dovessero trattare dati personali raccolti o prodotti o comunque di responsabilità del Titolare deve essere richiesto di applicare i medesimi criteri di protezione ove non ne siano adottati di più rigorosi, unitamente alla nomina di Responsabile esterno del Trattamento dei Dati.
Ogni quesito inerente la classificazione dei dati deve essere inoltrato al responsabile gerarchico; le domande e/o le osservazioni relative al presente Manuale devono essere rivolte ai Responsabili del Trattamento, al Titolare del Trattamento o al Responsabile per la Protezione dei Dati (RDP – DPO) dpo@nuovasair.it
CLASSI DI DATI Tutti i dati trattati si distinguono, in ordine di protezione crescente, come:
ANONIMI, COMUNI, PERSONALI, PARTICOLARI, GIUDIZIARI
Si considerano DATI ANONIMI esclusivamente quelle informazioni che in origine, o a seguito di trattamento, non possono essere associati ad una persona, sia essa fisica o giuridica, identificata od identificabile.
Si considera DATO PERSONALE qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificate od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (es Id_Cliente).
Nell'ambito dei dati personali:
Si considerano DATI PARTICOLARI i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Si considerano DATI GIUDIZIARI, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di Procedura Penale.
Di seguito si riportano i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n.313:
a. i provvedimenti giudiziari penali di condanna definitivi, anche pronunciati da autorità giudiziarie straniere se riconosciuti ai sensi degli articoli 730 e seguenti, del codice di procedura penale, salvo quelli concernenti contravvenzioni per le quali la legge ammette la definizione in via amministrativa, o l'oblazione limitatamente alle ipotesi di cui all'articolo 162, del codice penale, sempre che per quelli esclusi non sia stata concessa la sospensione condizionale della pena;

b. i provvedimenti giudiziari definitivi concernenti le pene, compresa la sospensione condizionale e la non menzione, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere;
c. i provvedimenti giudiziari concernenti le pene accessorie;
d. i provvedimenti giudiziari concernenti le misure alternative alla detenzione;
e. i provvedimenti giudiziari concernenti la liberazione condizionale;
f. i provvedimenti giudiziari definitivi che hanno prosciolto l'imputato o dichiarato non luogo a procedere per difetto di imputabilità, o disposto una misura di sicurezza;
g. i provvedimenti giudiziari definitivi di condanna alle sanzioni sostitutive e i provvedimenti di conversione di cui all'articolo 66, terzo comma e all'articolo 108, terzo comma, della legge 24 novembre 1981, n. 689;
h. i provvedimenti giudiziari del pubblico ministero previsti dagli articoli 656, comma 5, 657 e 663, del codice di procedura penale;
i. i provvedimenti giudiziari di conversione delle pene pecuniarie;
l. i provvedimenti giudiziari definitivi concernenti le misure di prevenzione della sorveglianza speciale semplice o con divieto o obbligo di soggiorno;
m. i provvedimenti giudiziari concernenti la riabilitazione;
n. i provvedimenti giudiziari di riabilitazione, di cui all'articolo 15, della legge 3 agosto 1988, n. 327;
o. i provvedimenti giudiziari di riabilitazione speciale relativi ai minori, di cui all'articolo 24 del regio decreto-legge 20 luglio 1934, 1404, convertito, con modificazioni, dalla legge 27 maggio 1935, n. 835, e successive modificazioni;
r. i provvedimenti giudiziari relativi all'espulsione a titolo di sanzione sostitutiva o alternativa alla detenzione, ai sensi dell'articolo 16, del decreto legislativo 25 luglio 1998, n. 286, come sostituito dall'art. 15 della legge 30 luglio 2002, n. 189;
s. i provvedimenti amministrativi di espulsione e i provvedimenti giudiziari che decidono il ricorso avverso i primi, ai sensi dell'articolo 13, del decreto legislativo 25 luglio 1998, n. 286, come sostituito dall'art. 12 della legge 30 luglio 2002, n. 189;
t. i provvedimenti di correzione, a norma di legge, dei provvedimenti già iscritti;
u .qualsiasi altro provvedimento che concerne a norma di legge i provvedimenti già iscritti, come individuato con decreto del Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro della giustizia.
Di seguito si riportano gli articolo 60 e 61 del Codice di Procedura Penale:
Art. 60 Assunzione della qualità di imputato
1. Assume la qualità di imputato la persona alla quale e' attribuito il reato nella richiesta di rinvio a giudizio, di giudizio immediato, di decreto penale di condanna, di applicazione della pena a norma dell`art. 447 comma 1, nel decreto di citazione diretta a giudizio emesso a norma dell`art. 555 e nel giudizio direttissimo.
2. La qualità di imputato si conserva in ogni stato e grado del processo, sino a che non sia più soggetta a impugnazione la sentenza di non luogo a procedere, sia divenuta irrevocabile la sentenza di proscioglimento o di condanna o sia divenuto esecutivo il decreto penale di condanna.
3. La qualità di imputato si riassume in caso di revoca della sentenza di non luogo a procedere e qualora sia disposta la revisione del processo.
Art. 61 Estensione dei diritti e delle garanzie dell'imputato
1. I diritti e le garanzie dell'imputato si estendono alla persona sottoposta alle indagini preliminari.
2. Alla stessa persona si estende ogni altra disposizione relativa all'imputato, salvo che sia diversamente stabilito.
Nell'ambito dei dati personali particolari:
si considerano DATI SANITARI quei dati idonei a rivelare lo stato di salute e la vita sessuale dell'interessato. Ogni informazione non ancora classificata deve essere trattata con le medesime misure di sicurezza previste per i DATI SANITARI. Nel dubbio i dati devono essere classificati nella categoria di protezione maggiore.

5.2 DIRETTIVA PER LA CLASSIFICAZIONE DEI TRATTAMENTI

SCOPO Per poter garantire una adeguata protezione ai dati personali occorre che siano conosciute le specifiche modalità di trattamento, ovvero i processi ed i flussi dati che vi sono legati procedendo ad una

classificazione ai fini della sicurezza secondo i livelli di protezione legati sia alla particolarità dei dati interessati sia alla strategicità del processo in relazione alla operatività del Sistema Informativo.
Tale attività e' peraltro prevista dall'articolo 30 del GDPR UE 2016/679 ove è prescritto che "Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità". A tal fine la Cooperativa Sociale Nuova Sair Onlus si è dotata di un proprio registro dei trattamenti che contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del GDPR UE 2016/679.

Questa Direttiva ha lo scopo di fornire lo strumento metodologico, per procedere alla individuazione elencazione e classificazione dei trattamenti di dati personali effettuati dal Titolare.
La classificazione dei trattamenti di dati personali in particolare, costituisce attività necessaria al fine di:

- Redigere il registro dei trattamenti ai sensi dell'art. 30 del GDPR UE 2016/679;
- Verificare che i sistemi informativi ed i programmi informatici siano configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, 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 in conformità a quanto prescritto dal GDPR UE 2016/679;
- Verificare che i dati personali oggetto di trattamento, in conformità alle previsioni del GDPR UE 2016/679 siano: trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; esatti e se necessario aggiornati; pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- Definire il grado di protezione che deve essere applicato, il livello di conoscibilità (se ad es. possono essere conosciuti anche da terzi, ovvero possono essere diffusi, oppure se invece hanno una conoscibilità, o comunicabilità, limitata e, dunque, non devono essere conosciuti all'esterno della struttura o comunicati, senza le prescritte autorizzazioni).
- Verificare, nel caso di trattamento non conforme alle disposizioni di Legge, che gli eventuali dati personali non siano utilizzati in conformità alle previsioni normative del GDPR UE 2016/679.
- Verificare se il trattamento di dati personali diversi da quelli particolari e giudiziari, in relazione alla natura dei dati od alle modalità di trattamento, o agli effetti che può determinare, possa presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, al fine di effettuare nel caso una Valutazione di Impatto come prescritto dal GDPR UE 2016/679.
- Proteggere i dati personali, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta, così come prescritto dall'art GDPR UE 2016/679.

Per trattamento di dati si intende qualunque operazione o complesso di operazioni su dati, effettuate anche senza l'ausilio di strumenti elettronici, concernenti:

- la raccolta,
- la registrazione
- l'organizzazione

- la conservazione
- la consultazione
- l'elaborazione
- la modificazione
- la selezione
- l'estrazione
- il raffronto
- l'utilizzo
- l'interconnessione
- il blocco
- la comunicazione
- la diffusione
- la cancellazione
- la profilazione
- la distruzione

Per processo di trattamento o servizio, si intendono quelle operazioni di trattamento che sono predisposte ed organizzate tra loro al fine di raggiungere un determinato fine operativo della Cooperativa Sociale Nuova Sair Onlus, quali ad esempio: registrazione delle fatture, buste paga, gestione dei dati dei dipendenti e degli utenti, etc. I principi contenuti nella presente Direttiva devono essere applicati in modo coordinato alle attività normali dell'organizzazione affinché siano evitati disturbi e/o interferenze con la normale operatività di questa.
AMBITO Tutti i processi di trattamento effettuati con il Sistema Informativo della struttura devono essere classificati nel rispetto della presente direttiva. Tutti coloro i quali partecipano a processi di trattamento dati, o svolgono incarichi, nell'ambito del sistema informativo della struttura, siano essi dipendenti e/o collaboratori, anche esterni e saltuari, ovvero enti od organizzazioni autonome sono tenuti al rispetto della presente direttiva. Ai terzi che eventualmente dovessero trattare dati personali raccolti o prodotti o comunque di responsabilità della struttura deve essere richiesto di applicare i medesimi criteri di protezione o ve non ne siano adottati di più rigorosi.
CRITERI DELLA ATTIVITÀ DI CLASSIFICAZIONE Ciascun processo deve essere identificabile in modo univoco. La particolarità di ciascun processo è determinata sulla base del livello di particolarità massimo applicato ai dati che ne sono coinvolti, ad es: processi che coinvolgono dati sanitari, massima particolarità, processi che coinvolgono esclusivamente dati anonimi minima particolarità. Ogni processo non ancora classificato deve essere considerato di massima particolarità. Nel dubbio i processi devono essere classificati nella categoria di protezione maggiore.
MODALITÀ I processi devono essere classificati prima di essere attivati. Il personale dipendente e non, saltuario e non, della struttura, o coloro che trattano dati per conto dell'organizzazione, devono trattare i dati PERSONALI secondo le modalità prescritte, e secondo le finalità di trattamento, nei limiti del ruolo ricoperto. Qualsiasi dubbio sul trattamento di un dato deve essere immediatamente espresso al designato "Responsabile" superiore gerarchico. La classificazione dei processi di trattamento spetta al Titolare del Trattamento, coadiuvato dal Responsabile della Protezione dei Dati, cui spetta anche l'obbligo di provvedere all'aggiornamento e tenuta del registro dei trattamenti di cui all'art. 30 del GDPR UE 2016/679.
CONTENUTO L'attività di classificazione ai fini della compilazione del registro dei trattamenti deve tenere almeno conto dei seguenti elementi:

- breve descrizione del trattamento
- finalità del trattamento
- categorie del trattamento
- modalità di trattamento
- tipologia e natura dei dati trattati
- eventuale presenza di Responsabili esterni del trattamento
- categorie di interessati
- eventuali destinatari dei trasferimenti di dati
- misure di sicurezza

DATO PERSONALE, si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificate od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
DATI PARTICOLARI, si intendono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
DATI GIUDIZIARI, si intendono i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di Procedura Penale.

5.3 CRITERI PER LA DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI PERSONALI

SCOPO Il presente documento ha lo scopo di individuare i criteri generali per determinare ed attribuire compiti e responsabilità sotto il profilo della privacy e della sicurezza delle informazioni, nell'ambito delle strutture preposte al trattamento dei dati personali.

AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali sotto la responsabilità del Titolare del trattamento.
CONTENUTO A ciascun bene dell'Ente, incluse informazioni, software, dispositivi ed attrezzature di trattamento, deve essere assegnato un "proprietario". Il proprietario è responsabile ed è titolare dei diritti sulla risorsa assegnatagli. Il vertice amministrativo dell'organizzazione, congiuntamente all'organo preposto alla sicurezza del sistema informativo e con la collaborazione dei responsabili operativi delle aree organizzative della struttura è investito dell'obbligo di progettare, implementare, rendere effettive, monitorare, rivedere, mantenere ed incrementare il programma di sicurezza. Tale impegno deve essere reale e visibile a tutti i dipendenti dell'organizzazione. In particolare spettano al titolare del trattamento ed ai responsabili del trattamento, i compiti dettagliati nei sotto paragrafi seguenti.

- Approvare e fissare i criteri di sicurezza dell'organizzazione;
- Garantire che gli obiettivi ed i piani di sicurezza del sistema informativo dell'organizzazione siano inequivocabilmente individuati e determinati;
- Individuare ed assegnare ruoli e responsabilità per la sicurezza del sistema informativo;
- Comunicare ai dipendenti e collaboratori dell'organizzazione l'importanza di perseguire gli obiettivi di sicurezza e di essere conformi ai criteri di sicurezza fissati;
- Assicurare che sufficienti risorse (sia umane che hardware e software) siano assegnate per lo sviluppo, l'implementazione, l'operatività ed il mantenimento del sistema informativo dell'organizzazione;
- Stabilire i livelli di rischio accettabili nel rispetto delle misure di sicurezza, dei compiti istituzionali e delle disposizioni inderogabili di legge vigenti.

Spettano al Titolare del trattamento le decisioni in ordine alle finalità, alle modalità di trattamento ed alle misure di sicurezza a tutela dei dati personali. Definizioni:
TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
RESPONSABILE: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
UTENTE: si intende colui che utilizza una o più risorse del trattamento dati.

5.4 DIRETTIVA PER IL CONTROLLO DI ACCESSO AI DATI PERSONALI ED ALLE RISORSE DI TRATTAMENTO

SCOPI La presente Direttiva ha lo scopo di individuare i criteri generali per controllare l'accesso ai dati ed agli strumenti di trattamento al fine di rispettare gli obblighi normativi di cui al GDPR UE 2016/679.
AMBITO I principi contenuti nella presente Direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali sotto la responsabilità del Titolare del trattamento.
PRINCIPI COMUNI Gli accessi agli elaboratori o dispositivi di trattamento, alla rete, alle applicazioni, ai locali, interessati per il trattamento di dati personali di cui è responsabile l'azienda, come pure ai dati medesimi indipendentemente dal supporto su cui sono conservati, deve essere effettuato e consentito in modo controllato ovvero sicuro, in relazione alla particolarità dei dati trattati. Il controllo degli accessi deve essere conforme alle necessità operative ed istituzionali dell'organizzazione, al fine di garantire oltre alla integrità e confidenzialità delle informazioni, la disponibilità delle stesse. Conseguentemente le necessità operative ed istituzionali dell'organizzazione per l'accesso ai dati personali devono essere individuate e documentate per iscritto a cura del titolare del trattamento, o di chi da questi all'uopo delegato. Coloro i quali devono effettuare a qualsiasi titolo trattamento di dati personali di responsabilità dell'organizzazione devono essere preventivamente individuati conformemente ai criteri di sicurezza organizzativi. Coloro i quali hanno accesso ai dati personali trattati dall'organizzazione devono essere informati in modo chiaro ed univoco che i dati personali e le attrezzature di trattamento devono essere protetti, come pure che usi non conformi possono comportare conseguenze disciplinari e costituire violazioni di legge.
DATI SU SUPPORTO NON-ELETTRONICO Salvo quanto già previsto dalla Direttiva per la protezione fisica delle aree e dei locali, l'accesso agli archivi ove sono custoditi dati particolari/giudiziari deve essere controllato; in modo specifico, coloro i quali accedono ai suddetti archivi al di fuori degli orari di lavoro devono essere identificati e registrati. In relazione a particolari condizioni ambientali ed alla natura dei dati custoditi, particolari e specifiche misure di sicurezza potranno essere adottate.
DATI SU SUPPORTO ELETTRONICO In ogni caso, coloro i quali sono designati al trattamento, od hanno diverso titolo di accesso ai dati personali di responsabilità dell'organizzazione, trattati mediante sistemi di elaborazione automatica, devono comunque essere forniti di Credenziali di Autenticazione in conformità a quanto previsto dalla Direttiva delle Credenziali di Autenticazione. A tal fine devono essere adottate specifiche procedure per la registrazione e cancellazione di coloro ai quali deve essere garantito il diritto di accesso ai dati personali di responsabilità dell'organizzazione secondo specifici Profili di Autorizzazione. L'attribuzione di privilegi dovrà essere strettamente connessa alle esigenze operative ed istituzionali dell'organizzazione e conformata al rispetto delle normative vigenti in materia di trattamento dei dati personali. I Profili di Autorizzazione devono essere individuati e configurati anteriormente all'inizio del trattamento e con cadenza almeno annuale deve essere verificata la sussistenza delle condizioni per la conservazione dei Profili di Autorizzazione. L'acceso agli elaboratori preposti al trattamento di dati personali, deve essere protetto mediante un Sistema di Autenticazione basato su Credenziali di Autenticazione legate a specifici Profili di Autorizzazione.

5.5 DIRETTIVA SULLE CREDENZIALI DI AUTENTICAZIONE

SCOPI Per superare la procedura di autenticazione informatica i designati devono essere dotati di Credenziali di Autenticazione. Questa Direttiva ha lo scopo di fornire i principi su cui devono essere basate le Credenziali di Autenticazione.
AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.
Per CREDENZIALI DI AUTENTICAZIONE si intendono i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
Per AUTENTICAZIONE INFORMATICA si intende l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
Le Credenziali di Autenticazione consistono in:

- un codice univoco per l'identificazione del designato associato ad una parola chiave riservata conosciuta solamente dal medesimo;

- un dispositivo di autenticazione in possesso e uso esclusivo del designato, eventualmente associato ad un codice identificativo o ad una parola chiave (PIN);
- in una caratteristica biometrica, eventualmente associata ad un codice identificativo o ad una parola chiave (PIN).

Spetta al Titolare del trattamento decidere, in base alla analisi dei rischi, al livello di sicurezza richiesto, alle specifiche modalità di trattamento ed alle disponibilità tecniche, i tipi di Credenziali di Autenticazione da adottare. Nel Sistema Informativo possono coesistere diversi tipi di Credenziali di Autenticazione, a ciascun designato possono essere assegnate od associate individualmente una o più credenziali per l'autenticazione. Spetta all'organo preposto alla sicurezza del Sistema Informativo assegnare od associare le Credenziali di Autenticazione alle persone dei designati. Spetta ai vertici amministrativi dell'organizzazione o a chi da questi delegato, redigere e mantenere aggiornati i Profili di Autorizzazione per ciascun designato o per classe omogenea di designati in modo da limitare l'accesso dei designati ai soli dati necessari per effettuare le operazioni di trattamento (need to know). È onere di chi ha la responsabilità dei Profili di Autorizzazione comunicare ogni variazione all'organo preposto alla sicurezza del Sistema Informativo in modo da consentire l'immediata disattivazione delle Credenziali di Autenticazione in caso di perdita della qualità che consente all'designato l'accesso ai dati personali. Spetta all'organo preposto alla sicurezza del Sistema Informativo verificare sull'uso corretto delle Credenziali di Autenticazione e procederne se del caso alla disattivazione dandone comunicazione ai responsabili dei Profili di Autorizzazione.

ACCESSO ESCLUSIVAMENTE MEDIANTE LA COMPONENTE RISERVATA DELLE CREDENZIALI DI AUTENTICAZIONE Quando l'accesso ai dati ed agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della Credenziale di Autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'designato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema.

In tal caso la custodia delle copie delle Credenziali di Autenticazione è organizzata dal titolare garantendo la relativa segretezza ed individuando preventivamente per iscritto i soggetti designati della loro custodia, i quali devono informare tempestivamente il designato dell'intervento effettuato. Definizioni:

PAROLA CHIAVE (PASSWORD - PIN) si intende la componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri od altri dati in forma elettronica.

PROFILO DI AUTORIZZAZIONE si intende l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

SISTEMA DI AUTORIZZAZIONE si intende l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

STRUMENTI ELETTRONICI si intende gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

5.7 DIRETTIVA PER LA PROTEZIONE FISICA DELLE AREE E DEI LOCALI

SCOPI I criteri qui individuati sono finalizzati a garantire la custodia ed il controllo dei dati personali oggetto di trattamento mediante il sistema informativo della Cooperativa Sociale Nuova Sair Onlus al fine di ridurre al minimo, in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di:

- DISTRUZIONE
- PERDITA anche accidentale dei dati stessi;
- ACCESSO NON AUTORIZZATO;
- NON ACCESSIBILITÀ DEL DATO
- TRATTAMENTO NON CONSENTITO o NON CONFORME alle finalità individuate dal GDPR UE 2016/679;

AMBITO I principi contenuti nella presente direttiva si applicano all'interno dell'azienda ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità di azienda.

CONTENUTO All'interno dei settori fisici (uffici, aree operative) della Cooperativa Sociale Nuova Sair Onlus sono individuate, a cura del Titolare le aree di sicurezza secondo il livello di misure di protezione che devono esservi adottate in relazione alla particolarità dei dati che ivi vengono trattati. L'individuazione delle aree di sicurezza ha lo scopo di prevenire accessi fisici non autorizzati, danni ed interferenze con i processi di

trattamento dei dati. L'Organizzazione usa un sistema di perimetrazione sicuro al fine di proteggere i locali ove sono contenuti dispositivi per il trattamento dei dati.
Le Aree di sicurezza fisica si distinguono in: pubblica, ristretta, protetta.
In una area possono esservi uno o più locali, in un locale possono esservi uno o più settori. Per la attribuzione dei settori si considera la particolarità dei dati ivi trattati, così ad esempio se in un'area viene trattato anche un solo dato particolare/giudiziario, in essa deve essere applicato un settore protetto.
Area Pubblica: e' quella ove non sono trattati dati personali o particolari. Per questa area si applica il seguente criterio generale: durante il normale orario di lavoro è consentito l'accesso del pubblico senza necessità di autenticazione. I locali od i loro accessi sono presidiati al fine di garantire un controllo generico degli accessi al fine di preservare l'integrità dei beni fisici in essi contenuti.
Al di fuori del normale orario di lavoro gli accessi sono invece controllati mediante identificazione e registrazione, l'accesso è consentito solo a coloro i quali ne hanno ragione per motivo della mansione ad essi attribuita.

Area ristretta: è quella ove sono trattati dati personali, ma non particolari/giudiziari.
L'accesso a questa area è sempre controllato in modo tale che coloro i quali non hanno titolo al trattamento dei dati non possano accedervi. Nello specifico i designati "Responsabili" del trattamento prescrivono che i designati al trattamento abbiano accesso solo ai dati personali la cui conoscenza è strettamente necessaria all'adempimento dei compiti loro assegnati. Gli atti ed i documenti devono essere conservati in archivi ad accesso selezionato e, se consegnati agli designati del trattamento, devono essere da questi restituiti senza ritardo al termine delle operazioni loro affidate. Atti e documenti non possono essere trasferiti neppure in copia al di fuori del perimetro aziendale senza autorizzazione espressa da parte del Responsabile del trattamento. Definizioni:
Area protetta: è quella ove sono trattati dati particolari/giudiziari e le informazioni relative al trattamento dei dati personali o particolari/giudiziari. Coloro i quali accedono in questa area, sia durante il normale orario di lavoro sia extra orario, devono essere autorizzati. Oltre a quanto sopra previsto gli atti o documenti contenenti dati particolari se affidati ad autorizzati del trattamento devono essere da questi conservati sino alla restituzione in armadi/cassetti muniti di serratura. Misure di controllo supplementari per il lavoro nei settori di sicurezza possono essere adottate al fine di garantire la migliore protezione dei dati. I dispositivi di trattamento dei dati devono essere protetti al fine di evitare la perdita od il danneggiamento dei beni e dei dati, ovvero l'interruzione del servizio.
In particolare:

- Occorre considerare la collocazione di archivi e dispositivi di emergenza al fine di ridurre i rischi dovuti sia a fattori naturali/ambientali sia a guasti ed ad accessi non autorizzati;
- Occorre tenere conto dei rischi di improvvise interruzioni od anomalie dell'energia elettrica;
- Occorre proteggere con cablaggi sicuri i cavi di alimentazione e di comunicazione al fine di prevenirne guasti od intercettazioni.
- I dispositivi di trattamento, le attrezzature d'ufficio ed i dispositivi di sicurezza, devono essere regolarmente manutenuti al fine di garantirne la continuità di funzionamento.
- Le copie di documenti contenenti dati personali o particolari/giudiziari, ove non utilizzate, anche se in bozza, devono essere distrutte in modo da impedirne la lettura prima del loro smaltimento.
- I piani di lavoro, specie se collocati in settori non protetti, devono essere lasciati sgombri da documenti contenenti dati personali o particolari/giudiziari.
- Ogni dispositivo od apparecchiatura non potrà essere rimosso dall'area di pertinenza senza la preventiva autorizzazione del titolare del trattamento.

5.6 DIRETTIVA PER L'INTEGRITÀ DEI DATI PERSONALI

SCOPI Questa Direttiva ha lo scopo di fornire i criteri generali che regolano il complesso di misure fisiche, tecniche ed organizzative.
AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.
CONTENUTO I dati personali oggetto di trattamento, per il periodo dello stesso, devono essere mantenuti integri, disponibili per l'uso previsto e riservati. Periodicamente, con frequenza almeno settimanale, devono

essere effettuate copie di riserva dei dati personali e particolari. La frequenza delle copie deve essere tale da consentire la minima perdita di dati in caso di guasto o distruzione dei supporti principali.
Tali copie devono essere periodicamente verificate per accertare la corretta disponibilità dei dati in esse contenuti. I supporti contenenti le copie dei dati particolari e personali devono essere sottoposte alle medesime misure di protezione dei supporti principali. I supporti contenenti le copie devono essere ciclicamente aggiornati in modo da garantirne la massima affidabilità, i supporti obsoleti devono essere distrutti in modo permanente o, se riutilizzati sottoposti ai criteri generali per il riuso. Compatibilmente alle esigenze tecniche ed organizzative deve essere mantenuto un registro delle operazioni effettuate sui dati particolari/giudiziari. Devono essere effettuati controlli periodici da parte di personale indipendente su tali registri.

5.7 DIRETTIVA PER L'UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE E PER LE OPERAZIONI DI MANUTENZIONE O RIPARAZIONE

SCOPO Questa Direttiva ha lo scopo di fornire i criteri generali per l'uso ed il riuso dei supporti di memorizzazione rimovibili e per garantire la sicurezza dei dati personali memorizzati su supporti fissi durante le operazioni di manutenzione o riparazione.
AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.
USO I supporti di memorizzazione rimovibili (ad es. Floppy disk, hard disk estraibili, cdrom, DVD, memorie USB, memory stick, flash disk, ecc.) che contengono dati personali devono essere etichettati nel rispetto della Direttiva per la classificazione dei dati. Ai supporti di memorizzazione rimovibili, in relazione alla natura dei dati contenuti, si applicano gli stessi principi di sicurezza e le medesime misure previste per i supporti fissi. Specifiche direttiva d'uso in relazione a particolari modalità di trattamento ed alla natura dei dati trattati potranno essere dettagliate a cura congiunta dei designati "responsabili" dei processi di trattamento e dell'organo preposto alla sicurezza del sistema informativo.
RIUSO I supporti che contengono od hanno contenuto dati personali e/o particolari possono essere riutilizzati o ceduti previa autorizzazione del responsabile della risorsa nel rispetto dei presenti criteri generali. In particolare, i supporti utilizzati per il trattamento, anche temporaneo, di dati particolari devono essere previamente cancellati in modo tale che permanentemente non sia tecnicamente consentito il recupero di tali dati.
MANUTENZIONE, RIPARAZIONI Nel caso in cui i supporti rimovibili o apparecchiature che contengono supporti fissi in cui sono contenuti dati personali debbano essere affidati a terzi per motivi diversi dal trattamento (ad esempio per manutenzione) ove non sia possibile la rimozione dei dati personali, occorre adottare le stesse misure di sicurezza previste per l'uso ed il riuso dei supporti rimovibili.

5.8 DIRETTIVA PER LA PROTEZIONE DA PROGRAMMI MALIZIOSI, PER L'INDIVIDUAZIONE DI INTRUSIONI, PER GLI AGGIORNAMENTI DEI SOFTWARE

SCOPO Questa Direttiva ha lo scopo di individuare e formalizzare i principi su cui devono essere basate le misure di:

- Protezione dai programmi maliziosi (malware, virus ecc.) ex art. 615-quinquies C.P.
- Aggiornamento periodico dei programmi informatici utilizzati
- Protezione dalle intrusioni ex art. 615-ter C.P.

AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.
PROTEZIONE DAI PROGRAMMI MALIZIOSI (MALWARE, VIRUS ECC.) EX ART. 615-QUINQUIES C.P. I dati, le basi dati, i programmi in formato elettronico di responsabilità dell'organizzazione devono essere protetti dai rischi di intrusione e danneggiamento ad opera dei programmi di cui all'art.615-quinquies C.P. Tale protezione si attua sia mediante l'uso di specifici programmi, sia mediante il rigido rispetto dei criteri e delle procedure di sicurezza dell'organizzazione. I programmi di protezione devono essere installati ed operanti, ove tecnicamente possibile, su tutte le macchine interessate, in modo continuativo e non, dal trattamento dati o

connesse, in modo continuativo e non, ad altre macchine che sono interessate al trattamento dati. I programmi di protezione devono essere costantemente aggiornati, anche in modo automatizzato, al fine di garantire sia il contemporaneo aggiornamento di tutte le macchine interessate, sia il tempestivo aggiornamento dei programmi di protezione in relazione all'evoluzione delle minacce. L'aggiornamento, in ogni caso, deve essere effettuato almeno con cadenza semestrale. L'uso della posta elettronica, il trasferimento di file comunque effettuato, l'installazione di programmi su macchine dell'organizzazione o che interagiscono con macchine dell'organizzazione deve essere rigidamente regolamentato in modo da ridurre al minimo il rischio di intrusione o danno ad opera dei programmi di cui all'art. 615-quinquies C.P.

AGGIORNAMENTI PERIODICI DEI PROGRAMMI INFORMATICI. I programmi informatici vengono continuamente aggiornati dai produttori al fine di prevenirne vulnerabilità e correggerne i difetti. Tutti i programmi utilizzati nel Sistema Informativo (ad es. Sistemi operativi, applicativi, software di comunicazione, ecc.) dell'organizzazione devono quindi essere costantemente mantenuti aggiornati secondo l'ultimo aggiornamento disponibile rilasciato dal produttore. A tal fine dovranno essere effettuati tutti i settaggi al fine di automatizzare, per quanto possibile, l'attività di sincronizzazione (update). In ogni caso la frequenza di verifica di nuovi aggiornamenti non può essere inferiore ad un anno per il software destinato al trattamento di dati personali e a sei mesi per il software destinato al trattamento di dati particolari/giudiziari.

PROTEZIONE DALLE INTRUSIONI EX ART. 615-TER C.P. Al fine di prevenire intrusioni ovvero accessi ed usi non autorizzati o comunque non legittimi del Sistema Informativo dell'organizzazione, sono predisposti idonei strumenti software e/o hardware per il monitoraggio della rete dell'organizzazione in conformità a quanto previsto nel Programma per le verifiche delle misure di sicurezza. I dati risultanti dalla attività di monitoraggio sono trattati e custoditi con i medesimi criteri previsti per i dati particolari/giudiziari. Definizioni: PROGRAMMI MALIZIOSI si intendono quei programmi informatici, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

5.9 DIRETTIVA PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI PERSONALI IN CASO DI INCIDENTE, DISASTRO O DATA BREACH

SCOPO Questa Direttiva ha lo scopo di fornire i criteri generali per il ripristino della disponibilità dei dati in seguito a distruzione, danneggiamento o data breach ai sensi del GDPR UE 2016/679 nonché i principi su cui devono essere basate le specifiche procedure attuative.

AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura del Titolare ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.

CRITERI GENERALI Sulla base delle risultanze dell'Analisi dei Rischi (cfr. Direttiva per l'Analisi dei Rischi) il Titolare del trattamento procede alla valutazione dei processi di trattamento dati effettuati dall'organizzazione secondo i seguenti criteri:

- per ciascun servizio deve essere espressa l'importanza strategica sia in considerazione dell'incidenza sull'operatività dell'organizzazione, sia in relazione alla natura dei dati trattati ed agli obblighi di legge relativi.
- Per ciascun servizio deve essere considerato l'impatto che l'interruzione può comportare per l'operatività della struttura, per i dati personali trattati, per gli adempimenti di Legge e contrattuali.
- Per ciascun servizio deve essere considerata, insieme ai responsabili del servizio, una specifica procedura per garantire la continuità del servizio ovvero per il trasferimento dei rischi connessi all'interruzione ove possibile.
- Per ciascun servizio, sulla base della soluzione di continuità prescelta, deve essere indicato il termine di riattivazione previsto.
- I risultati della superiore valutazione vengono documentati per iscritto e devono essere aggiornati periodicamente almeno una volta l'anno ed ogni qualvolta siano introdotti nuovi servizi o processi di trattamento, ovvero ogniqualvolta intervengano particolari mutamenti che interessano il Sistema Informativo.
- Gli autorizzati al trattamento, a cura dei responsabili dei servizi, devono ricevere adeguata formazione riguardo le strategie e soluzioni di continuità adottate per lo specifico servizio.

- Periodicamente, vengono effettuati test e simulazioni per verificare la funzionalità dei programmi di continuità operativa adottati.

LE PROCEDURE DI CONTINUITÀ devono considerare le ipotesi di breve interruzione (non superiore alle 12 ore consecutive), media interruzione (non superiore a sette giorni consecutivi), lunga interruzione (superiore a sette giorni consecutivi), tenendo conto che per i servizi che riguardano dati personali deve essere ripristinata la disponibilità dei dati nel più breve tempo possibile ai sensi del GDPR UE 2016/679. In particolare dovranno essere considerati almeno i seguenti aspetti:

- le condizioni di attivazione del piano di continuità, le attività di emergenza che dovranno essere seguite (incluse le istruzioni per il rapporto delle cause dell'interruzione),
- le specifiche attività che dovranno essere eseguite per rimediare temporaneamente l'interruzione (ad es: lo spostamento di servizi essenziali in locazioni temporanee, l'adozione di processi alternativi temporanei, ecc.),
- le attività che dovranno essere eseguite per il ripristino delle normali attività,
- un programma di verifica e test della procedura,
- un programma di formazione per addestrare gli designati ad eseguire la procedura correttamente,
- la individuazione dei responsabili per l'esecuzione delle procedure predisponendo anche un piano di reperibilità,
- la scala dei tempi di reazione e ripristino alla normalità dal verificarsi dell'evento che ha causato l'interruzione.

5.10 DIRETTIVA PER LA TRASMISSIONE DEI DATI PERSONALI

SCOPO Questa Direttiva ha lo scopo di fornire gli elementi di forma standard e di contenuto per garantire la sicurezza nella trasmissione di dati personali e particolari trattati dall'azienda, in conformità a quanto previsto dal D.Lgs. 196/2003 e ss.mm.ii. e dal GDPR UE 2016/679

Nello specifico la riduzione del rischio ha lo scopo di ridurre il rischio di perdita, danneggiamento od uso improprio dei dati personali di cui é responsabile l'azienda.

AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.

MODALITÀ

- Per trasmissione di dati si intende il trasferimento di dati contenuti su qualsiasi supporto effettuato in qualsiasi modo. A titolo meramente esemplificativo costituiscono trasmissione dati: l'invio per posta di un documento cartaceo o di un floppy disk, l'invio a mezzo fax, l'invio di dati mediante e-mail, il trasferimento di file attraverso reti, ecc.
- Possono essere trasmessi al di fuori dell'azienda soltanto i dati personali di cui é consentita la comunicazione o la diffusione, nei limiti e secondo le modalità previste.
- I dati personali di cui é consentita la diffusione possono essere trasmessi secondo le normali procedure di trasmissione avendo cura che i dati non possano essere modificati da terzi.
- I dati personali di cui é consentita la comunicazione devono essere trasmessi in modo da garantire la non modificabilità dei dati ed in modo che solo il destinatario abilitato alla ricezione possa leggerne il contenuto.
- Nel caso in cui terzi debbano intervenire e modificare i dati ad essi trasmessi o diffusi é necessario che sia garantita la verifica delle modifiche intervenute.
-

5.11 DIRETTIVA PER GARANTIRE L'ADOZIONE DI MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI ALL'ESTERNO DELL'ORGANIZZAZIONE

SCOPO Questa Direttiva ha lo scopo di fornire i criteri generali che devono essere seguiti per il rispetto dell'obbligo di cui sopra.

AMBITO I principi contenuti nella presente direttiva si applicano all'interno della struttuaovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità del Titolare.

ACCESSO DI TERZE PARTI Nel caso in cui i rapporti con terzi esterni alla organizzazione prevedano l'accesso al Sistema Informativo, occorre:

- che sia preliminarmente effettuata una specifica analisi dei rischi legati all'attività in conformità a quanto previsto dalla Direttiva per l'analisi dei rischi
- Che gli accessi alle informazioni e l'uso degli strumenti di trattamento siano controllati in conformità alle direttive:
- Che idonee garanzie contrattuali siano state previste e sottoscritte al fine di garantire il rispetto delle misure di sicurezza in conformità a quanto di seguito prescritto.

ASPETTI CONTRATTUALI Nei contratti aventi ad oggetto il trattamento di dati personali di responsabilità dell'organizzazione o comunque che coinvolgono dati personali di responsabilità dell'organizzazione, occorre siano considerati, in relazione alle specifiche attività di trattamento coinvolte:

- la conoscenza ed accettazione del contraente della politica dell'organizzazione in materia di sicurezza dei dati personali e delle informazioni in genere;
- in modo specifico la conoscenza ed accettazione del contraente delle misure di sicurezza adottate per la protezione dei dati personali con particolare riferimento a:
- protezione dei dati e delle risorse di trattamento, incluse:
- le procedure per proteggere i dati personali, compresi gli strumenti materiali ed immateriali (p.es. Software) di trattamento, le procedure di verifica della compromissione di dati personali, le misure per garantire la corretta distruzione di dati personali, le misure per garantire l'integrità e la disponibilità dei dati personali, le restrizioni sulle attività di copia di dati personali,
- le misure per garantire la riservatezza dei dati personali in relazione alle diverse situazioni contrattuali verificabili (p. es: cessazione del rapporto, risoluzione, recesso, contestazione ecc.)
- deve essere resa disponibile la descrizione dei servizi o processi di trattamento coinvolti;
- deve essere stabilito un livello minimo ed ottimale di servizio;
- devono essere previste le modalità per eventuali trasferimenti di personale;
- devono essere previste le condizioni per eventuali cessioni del rapporto contrattuale;
- devono essere definite le rispettive responsabilità delle Parti (anche in considerazione delle normative in materia di Privacy specie se sono previsti trasferimenti di dati personali all'estero);
- devono essere definiti gli accordi in materia di diritto d'autore o marchi sulle attività svolte in collaborazione;
- devono essere definite ed accettate le condizioni per il controllo degli accessi;
- devono essere definite le condizioni e le modalità per verifiche (anche presso le strutture del contraente condotte sia direttamente dall'organizzazione sia mediante terze parti specializzate);
- devono essere definite le conseguenze e le eventuali sanzioni in caso di inosservanza (p. es: clausole di risoluzione espressa, recesso, risarcimento danni, penali ecc.)
- deve essere previsto un percorso a tappe per la risoluzione di eventuali problemi;
- devono essere definite le responsabilità per la gestione e manutenzione di hardware e software;
- deve essere definita una struttura chiara per la redazione di rapporti e deve esserne concordato il formato;
- devono essere concordati e definiti eventuali strumenti per il controllo del rispetto degli obblighi assunti;
- deve essere prevista la formazione di utenti ed amministratori per i metodi e le procedure di sicurezza;
- devono essere definiti gli strumenti da utilizzare per proteggersi da software maliziosi;
- deve essere concordata una procedura per il ripristino della disponibilità dei dati personali in caso di grave guasto o disastro in conformità a quanto previsto nella Direttiva per il ripristino della disponibilità dei dati personali in caso di incidente o disastro;
- deve essere previsto l'obbligo per il contraente di trasferire tutti gli adempimenti in materia di sicurezza nel caso di uso di sub-contraenti.

5.12 PIANO DI FORMAZIONE IN MATERIA DI SICUREZZA DEI DATI PERSONALI

SCOPI Il GDPR UE 2016/679 richiede espressamente la programmazione e progettazione di interventi formativi destinati al Titolare, ai Responsabili e designati al trattamento dei dati, per renderli edotti almeno:

- dei rischi che incombono nel trattamento dati
- delle misure disponibili per prevenire eventi dannosi,
- dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività,
- delle responsabilità che ne derivano,
- delle modalità per aggiornarsi sulle misure di sicurezza adottate dall'azienda.

Questo documento ha lo scopo di individuare i criteri generali per gli interventi formativi dell'organizzazione in materia di sicurezza dei dati personali.

AMBITO Tutti coloro i quali partecipano a processi di trattamento dati, o svolgono incarichi, nell'ambito del sistema informativo, siano essi dipendenti e/o collaboratori, anche esterni e saltuari, ovvero enti od organizzazioni autonome sono tenuti al rispetto della presente direttiva. Ai terzi che eventualmente dovessero trattare dati personali raccolti o prodotti o comunque di responsabilità dell'azienda deve essere richiesto di applicare i medesimi criteri di protezione ove non ne siano adottati di più rigorosi.
CONTENUTO Qualsiasi intervento in materia di sicurezza dei dati personali richiede la massima collaborazione da parte dei designati.
Ciò presuppone la consapevolezza da parte dei designati:

- dell'importanza per l'organizzazione dei dati personali trattati,
- dei rischi specifici individuati mediante l'analisi dei rischi e la valutazione d'impatto
- degli obiettivi di sicurezza adottati dall'organizzazione,
- delle misure di sicurezza adottate dall'organizzazione,
- degli obblighi derivanti dalla legge, regolamenti, statuti, contratti in relazione agli specifici processi di trattamento,
- delle conseguenze che possono derivare per l'organizzazione dal verificarsi di un rischio,
- delle responsabilità che gravano sui designati,
- delle conseguenze che possono derivare a chi non ottempera agli obblighi di sicurezza adottati.

L'attività di formazione deve essere pianificata ed attuata in modo selettivo, ovvero in relazione alle necessità di conoscenza relative a ciascuna attività esercitata dagli designati o gruppi omogenei di designati. La formazione deve essere tempestiva in relazione all'evolvere delle necessità di protezione, chiara e completa. A tal fine possono essere utilizzati diversi strumenti di comunicazione (seminari, corsi, convegni, anche online, pubblicazioni sia telematiche o digitali che cartacee, ecc.) anche combinati tra loro e, per casi specifici ove è richiesto un alto livello di protezione, in maniera ripetuta o ridondante. Ciascun intervento formativo deve essere associato a verifiche al fine di accertare l'efficacia dello stesso ed eventualmente predisporre azioni correttive. La predisposizione degli interventi formativi spetta a livello generale ai vertici amministrativi dell'organizzazione congiuntamente al Titolare del trattamento, ed in caduta ai designati "responsabili" del trattamento e della sicurezza per i settori ad essi affidati.
Gli interventi formativi devono essere svolti in modo da poter essere documentati e comprovati (p.es. Registri presenze, autenticazioni per formazione online, ecc.). La formazione deve essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

5.13 DIRETTIVA PER L'ANALISI DEI RISCHI

SCOPO Questa Direttiva ha lo scopo di fornire lo strumento metodologico, per procedere alla analisi dei rischi basata sulle risultanze delle attività di classificazione e valutazione di dati e processi di trattamento.
AMBITO L'analisi dei rischi è condotta all'interno della struttura ovvero presso qualsiasi entità esterna che, in virtù di specifici accordi, tratta dati personali nella responsabilità dell'azienda.
PRINCIPI GENERALI L'attività di analisi deve essere condotta in modo coordinato alle attività normali dell'organizzazione affinché siano evitati disturbi e/o interferenze con la normale operatività di questa. La competenza per l'analisi dei rischi spetta al Titolare del trattamento, mentre la gestione dei rischi spetta ai vertici amministrativi dell'organizzazione. L'analisi dei rischi viene rivista ed aggiornata costantemente almeno una volta l'anno ed ogni volta che intervengono modifiche che incidono sensibilmente sul sistema informativo. Ogni nuova attività o processo di trattamento che deve essere adottato è preceduto da una specifica analisi dei rischi per consentire l'individuazione ed implementazione delle idonee misure di sicurezza.

MODALITA' Per ciascun processo viene effettuata una analisi che tenuto conto della natura dei dati trattati e delle specifiche modalità di trattamento individua tutte le possibili minacce che possono affliggere i dati oggetto del processo e tutte le risorse di trattamento incluse quelle umane. Le minacce sono valutate in termini percentuali di probabilità di accadimento. Le minacce sono quindi correlate con le vulnerabilità specifiche individuate per ciascun bene da proteggere. Le vulnerabilità sono valutate secondo il grado di rischio indicato con i valori "basso", "medio", "alto". Ciascuna associazione minaccia-vulnerabilità rappresenta un rischio. La gravità del rischio è espressa in base alla probabilità di accadimento della minaccia, il grado di debolezza della vulnerabilità e la gravità del danno che può derivare al sistema Informativo nel caso in cui il rischio si avveri. La valutazione del rischio spetta congiuntamente all'organo preposto alla sicurezza del sistema Informativo ed ai vertici amministrativi della organizzazione. Sulla base dei rischi rilevati viene quindi effettuato l'inventario delle contromisure applicabili valutandole in termini di capacità di riduzione del rischio cui sono associate.
REVISIONI Il presente documento viene aggiornato a cura del Titolare e dei Responsabili del Trattamento con cadenza almeno annuale attraverso il software PIA rilasciato dal Garante e la scheda misure di sicurezza sul registro dei trattamenti.

5.14 PROGRAMMA PER LE VERIFICHE DELLE MISURE DI SICUREZZA

SCOPO Questo documento ha lo scopo di fornire lo strumento metodologico, ed i criteri generali per gestire le attività di verifica e monitoraggio quali elementi essenziali dell'intero processo di sicurezza.
AMBITO Tutti coloro i quali partecipano a processi di trattamento dati, o svolgono incarichi, nell'ambito del sistema informativo siano essi dipendenti e/o collaboratori, anche esterni e saltuari, ovvero enti od organizzazioni autonome sono tenuti al rispetto della presente direttiva.
Ai terzi che eventualmente dovessero trattare dati personali raccolti o prodotti o comunque di responsabilità dell'Azienda deve essere richiesto di applicare i medesimi criteri di protezione ove non ne siano adottati di più rigorosi.
PRINCIPI GENERALI Occorre verificare periodicamente:

- l'effettiva implementazione delle misure adottate;
- l'efficacia delle misure adottate;
- la funzionalità delle misure adottate rispetto alle necessità operative dell'organizzazione.

AUDIT Le verifiche devono essere effettuate e condotte periodicamente da parte del DPO in modo da garantire la massima obiettività del risultato ed in modo da non interferire con la normale operatività dell'organizzazione. A tal fine i verificatori potranno procedere con controlli a campione ovvero mediante l'analisi dei dati di monitoraggio del Sistema Informativo.
Il risultato delle verifiche deve essere sempre documentato e registrato in modo da evidenziare le singole attività di verifica, le anomalie o deficienze eventualmente riscontrate. Gli strumenti di monitoraggio e verifica come pure i dati prodotti da tali attività devono essere custoditi con la massima cura e con la riservatezza prevista per i dati particolari/giudiziari e i relativi strumenti di trattamento. In caso di trattamento dati effettuato all'esterno della struttura del titolare devono essere effettuate regolarmente le medesime verifiche previste per il Sistema Informativo interno.

6 CONCLUSIONI

Il regolamento GDPR rappresenta la più significativa evoluzione normativa sulla privacy dei dati. Richiede la gestione dei dati personali e sensibili in modo da garantire un'adeguata riservatezza, un compito che comporta l'adozione di misure di sicurezza sia tecniche che organizzative.
La policy aziendale contiene tutte le informazioni necessarie su come La cooperativa Nuova Sair intende far fronte ai rischi derivanti dal trattamento dei dati personali e sensibili. In breve alcuni punti su cui porre maggiore attenzione:
1. mantenere segrete le proprie credenziali di accesso (password e/o pin);
2. non lasciare libero accesso ai propri dispositivi in caso di assenza momentanea dalla propria postazione lavorativa;

3. controllare l'accesso ad internet ed ai servizi di posta elettronica;
4. evitare per l'uso di dispositivi aziendali al di fuori dell'ambito lavorativo;
5. l'uso della penna USB o dispositivi di memoria removibili non è consentita a meno che non sia strettamente necessario, giustificando l'uso al coordinatore del servizio. In tal caso, premessa l'esistenza di una valida password di accesso, o l'acquisto di una penna USB crittografata, è necessario caricare/lasciare nella penna esclusivamente i dati che debbano essere trattati nel corso della sessione lavorativa.
6. La pseudonimizzazione è una tecnica che consiste nel conservare i dati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive. In caso di utilizzo di dispositivi USB o similari, fare in modo che i dati salvati non siano riconducibili all'interessato. (Es. uso delle iniziali e/o uso di un codice identificativo: "il sig. 101AB" invece del nome esteso).
Ulteriori dettagli sono descritti sulla Policy Aziendale.

Revisioni

Il presente documento viene aggiornato a cura del Titolare e dei Responsabili del Trattamento con cadenza almeno annuale.

Riferimenti normativi

Decreto Legislativo 196/2003 e ss.mm.ii.
GDPR UE 2016/679

Contatti

TITOLARE DEL TRATTAMENTO	Coop. Sociale Nuova Sair
IN PERSONA DI	Rosario Riccioluti
INDIRIZZO	viale del Tecnopolo 83, 00131 Roma
TELEFONO	0640800472
MAIL	rosario.riccioluti@nuovasair.it
PEC	nuovasair@legalmail.it
CODICE FISCALE	04197741004
PARTITA IVA	04197741004
MAIL UFFICIO PRIVACY	privacy@nuovasair.it
RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)	avv. Anna Natale
INDIRIZZO	viale del Tecnopolo 83, 00131 Roma
TELEFONO	0640800472
MAIL	dpo@nuovasair.it
INCARICO CON PROVVEDIMENTO	25/05/2018