POLICY PRIVACY

REGOLAMENTO DELL'ENTE

INFORMAZIONI DOCUMENTO:

Titolo	Regolamento Dell'Ente Privacy
Data di emissione	11/06/2024

SOMMARIO

PARTE PRIMA: INTRODUZIONE 7
PREMESSA DI CARATTERE NORMATIVO 7
PREMESSA DI CARATTERE ORGANIZZATIVO 7
PREMESSA DI CARATTERE METODOLOGICO 8
PARTE SECONDA: DISPOSIZIONI GENERALI 10
OGGETTO DEL REGOLAMENTO 10
FINALITÀ' DEL REGOLAMENTO 10
SENSIBILIZZAZIONE 10
DEFINIZIONI 11
PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI 13
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI) 14
TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI) 15
COMUNICAZIONE DI DATI VERSO L'ESTERNO 15
CARTELLA SANITARIA ELETTRONICA 16
PARTE TERZA: DIRITTI DELL'INTERESSATO 17
INFORMATIVA SUL TRATTAMENTO DEI DATI 17
CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI 18
DIRITTO DI ACCESSO DELL'INTERESSATO 19
DIRITTO DI RETTIFICA 22
DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO) 23
DIRITTO DI LIMITAZIONE AL TRATTAMENTO 23
DIRITTO ALLA PORTABILITA' DEI DATI 23
DIRITTO DI OPPOSIZIONE 24
PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE) 24
PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO 26
TITOLARE DEL TRATTAMENTO 26
CONTITOLARI DEL TRATTAMENTO 27
DELEGATO DEL TRATTAMENTO DEI DATI 27

RESPONSABILE DEL TRATTAMENTO DEI DATI 29
AUTORIZZATO AL TRATTAMENTO DEI DATI 31
RESPONSABILE DELLA PROTEZIONE DEI DATI 32
PARTE QUINTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO 34
PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA 34
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO 34
PROTEZIONE E SICUREZZA DEI DATI PERSONALI 35
NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO 35
VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI 36
TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO 36
PARTE SESTA: ATTUAZIONE IN AMBITO DELL'ENTE DEGLI ADEMPIMENTI EUROPEI 37
ENTRATA IN VIGORE E PUBBLICITA' 37
DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI' 37
ALLEGATO A – REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA 38
ALLEGATO B – DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO 42
ALLEGATO C – PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI – DATA BREACH 45
NORMATIVA DI RIFERIMENTO 45
PREMESSA E SCOPO 45
CAPO DI APPLICAZIONE 46
DEFINIZIONI GENERALI 46
DESTINATARI DELLA PROCEDURA 47
DOCUMENTAZIONE DELLE ATTIVITA' SVOLTE CON RIFERIMENTO ALLA GESTIONE DEI DATA BREACH 47
TIPOLOGIE DI VIOLAZIONE 48
FASI DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI 48
FASE 1: Scoperta e rilevazione del data breach 48
FASE 2: Qualificazione e valutazioni inziali 50
FASE 3: Valutazione della gravità della violazione e stima del rischio per gli interessati 50
FASE 4: Notifica all'autorità di controllo 51
FASE 5: Comunicazione agli interessati 52

FASE 6: Risoluzione dell'incidente 54
ALLEGATI 55
Allegato A - Fac simile di notifica all'Autorità di Controllo 55
Allegato B - Esempi commentati di violazione 55
Allegato C - Modello di comunicazione agli interessati della violazione dei dati 58
Allegato D - Riepilogo adempimenti 61
REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI DELL'ENTE 62
RIFERIMENTI NORMATIVI 62
PREMESSE E FINALITÀ DEL REGOLAMENTO 62
CAMPO DI APPLICAZIONE 63
NORME DI COMPORTAMENTO GENERALI DA ADOTTARE NELL'USO DEGLI STRUMENTI DELL'ENTE 63
ASSEGNAZIONE, GESTIONE E REVOCA DELLE CREDENZIALI DI ACCESSO 65
OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO 66
MEMORIZZAZIONE E PROTEZIONE DEI DATI 67
REGISTRAZIONE DEGLI ACCESSI 67
UTILIZZO DI COMPUTER E COMPUTER PORTATILI 68
UTILIZZO DI INTERNET 68
UTILIZZO DELL'INFRASTRUTTURA DI RETE 70
UTILIZZO DELLA POSTA ELETTRONICA 71
USO PERSONALE 75
SOFTWARE 75
ANTIVIRUS 76
SISTEMA DI CRITTOGRAFIA E SCAMBIO DATI 76
UTILIZZO DI TELEFONO FISSO/ CELLULARE/ SMARTPHONE/ TABLET/ FAX 76
UTILIZZO DI SISTEMI DI RIPRODUZIONE 77
SISTEMI IN CLOUD 77
ASSISTENZA DEGLI UTENTI E MANUTENZIONE 78
CONTROLLI SUGLI STRUMENTI (AD INTEGRAZIONE DELL'INFORMATIVA PRIVACY GIA' CONSEGNATA) 78
CONSERVAZIONE DEI DATI 81

ISTRUZIONI IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO O DI COLLABORAZIONE 81
SOCIAL MEDIA 82
DISPOSITIVI PERSONALI 82
SANZIONI 83
NORME FINALI 83
ALLEGATO 1: Informativa privacy per gli utenti degli strumenti Dell'Ente 84
ALLEGATO 2: Informativa sui controlli 86
ALLEGATO 3: Modulo Nomina Fiduciario 89
SOCIAL MEDIA POLICY 90
DENOMINAZIONE DELLE PAGINE ISTITUZIONALI E DESCRIZIONE 90
I NOSTRI ACCOUNT 91
SOCIAL MEDIA POLICY ESTERNA 92
COSA POSTIAMO? 92
COSA NON POSTIAMO? 92
MODERAZIONE 92
NETIQUETTE 93
PRIVACY 94
CONTATTI 94
SOCIAL MEDIA POLICY INTERNA 95
RESPONSABILITA' DEI PROFILI ISTITUZIONALI 95
PUBBLICAZIONE E STILE COMUNICATIVO 95
USO PRIVATO DEI SOCIAL NETWORK 97
POLICY SULL'USO DI WATHSAPP 98
DENOMINAZIONE DEL "PROFILO DELL'ENTE" E DESCRIZIONE 98
POLICY ESTERNA 99
CONTENUTO DEI MESSAGGI 99
MODERAZIONE 99
NETIQUETTE 99
PRIVACY 100

CONTATTI 100
POLICY INTERNA 100
RESPONSABILITA' DELL'APPLICAZIONE 101
RISPOSTE E STILE COMUNICATIVO 101

PARTE PRIMA: INTRODUZIONE

PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali (così detta "privacy") è uno strumento di applicazione del vigente Decreto Legislativo 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy") e, in particolare, del nuovo **Regolamento Europeo n. 2016/679**, nell'ambito dell'organizzazione del Centro Residenziali Anziani "S. Scalabrin".

Dal 25 maggio 2018 ha trovato diretta applicazione, sul territorio nazionale, il nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

In data 19/09/2018 è entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

È necessario pertanto, come Ente, di dotarsi sin da ora di un apposito "Regolamento" che disciplini compiti, attività e *policy* interne che garantiscano l'assolvimento degli adempimenti imposti dalle norme europee.

Il presente Regolamento Dell'Ente si rende inoltre necessario per recepire, in un unico testo, i precetti normativi di maggior rilevanza, sia di carattere Dell'Ente che nazionale in tema di trattamento dei dati personali.

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

PREMESSA DI CARATTERE ORGANIZZATIVO

Un' attenta disamina della normativa vigente in materia di privacy ha fatto emergere una necessità imprescindibile di cambiamento della mentalità che porti alla piena tutela della stessa, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge all'Ente, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali nonché dignità del singolo individuo. Per questi motivi, la "cultura della privacy" necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questo Ente. A tale scopo è necessario che il Centro Residenziali Anzini "S. Scalabrin" per mezzo del proprio personale si adoperi affinché possa crescere e rafforzarsi una maggiore consapevolezza in materia e ciò, non solo con una conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa nel trattamento dei dati, ma anche ponendo in essere tutti gli adempimenti di carattere tecnico ed organizzativo per contribuire concretamente al miglioramento della qualità del rapporto con l'utenza ed implementare il "processo di umanizzazione" in corso di realizzazione, nell'ambito di questo Ente, oramai da molti anni.

PREMESSA DI CARATTERE METODOLOGICO

Vengono allegati a questo Regolamento una serie di **documenti tecnici** atti a dare compiuta attuazione ai dettami della nuova "privacy europea".

Tali documenti, ai quali viene data massima pubblicità e diffusione tramite la pubblicazione sul sito *internet* Dell'Ente, sono:

A. Regole per l'adozione delle misure di sicurezza;
B. Disciplinare per l'autorizzato al trattamento;
C. Procedura per la gestione delle violazioni – data breach;
D. Regolamento per l'utilizzo degli strumenti Dell'Ente;
E. Social Media Policy;
F. Regolamento WhatsApp;

Si sottolinea come il principio cardine della "responsabilizzazione" (accountability nell'accezione inglese), introdotto dal nuovo Regolamento UE, imponga al Titolare del trattamento dei dati l'obbligo di attuare delle politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della **"conformità"** o

compliance nell'accezione inglese); e ciò anche attraverso dei comportamenti proattivi, atti a dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

La normativa vigente lascia al Titolare ampia autonomia decisionale in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Pertanto, questa Ente si sta impegnando, a far proprio i dettami del Legislatore europeo relativo all'*accountability* ed alla *compliance*. anche attraverso la predisposizione di questo documento.

PARTE SECONDA: DISPOSIZIONI GENERALI

OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Ente, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

FINALITÀ' DEL REGOLAMENTO

L'Ente garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali* dell'Unione Europea.)

SENSIBILIZZAZIONE

Il Centro Residenziali Anzini "S. Scalabrin" sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto agli ospiti e ai loro familiari.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Ente.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza contenute nel presente Regolamento Dell'Ente, al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Personale, ad ogni dipendente *(oltre che ad ogni collaboratore, consulente ...)* una specifica nomina in materia di privacy,

con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali **"autorizzati al trattamento dei dati"** o **"responsabili al trattamento"** ai sensi del Regolamento UE 2016/679.

Il Regolamento, pubblicato sul sito Dell'Ente, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), all'atto di sottoscrivere il contratto di lavoro e la relativa documentazione, è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare Dell'Ente si intende per:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

g) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

h) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

i) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

l) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

m) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

n) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

o) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; a proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento europeo non utilizza la definizione ***"dati sensibili"*** per la quale, quanto meno sino all'emanazione della legge italiana di revisione del D.lgs. 196/20013, si fa espresso rinvio all'articolo n. 4 del vigente Codice della privacy (D.lgs. 196/2003): definizione che, quindi, al momento rimane nell'utilizzo e nel linguaggio corrente per la materia di cui si tratta.

p) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *(«**liceità, correttezza e trasparenza**»);*

b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali *(«**limitazione della finalità**»);*

c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati *(**«minimizzazione dei dati»**).* A tale proposito, il Regolamento UE ricalca i principi sostanziali di ***"necessità, pertinenza, indispensabilità e non eccedenza"*** (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.

d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati *(«**esattezza**»);*

e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca

scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato *(«**limitazione della conservazione**»);*

f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali *(«**integrità e riservatezza**»).*

Come stabilito dal Regolamento UE, il Titolare del trattamento è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'*«**accountability**»* o *«**responsabilizzazione**»).*

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche,* le *convinzioni religiose* o *filosofiche*, o *l'appartenenza sindacale*, nonché trattare *dati genetici, dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "g" applicabile a questo Ente, ai sensi della quale "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*", nonché quella di cui alla lettera "h", applicabile a questo Ente, ai sensi della quale *"il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero **gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri** o conformemente al contratto con un professionista della sanità (..)"*.

Si fa presente, inoltre, che il Regolamento UE consente di *"mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute"* (articolo n. 9, paragrafo n. 4).

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare al "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi

dell'art.21, comma 1 del D.Lgs 10 Agosto 2018, n. 101" del Garante della Privacy, pubblicato in Gazzetta Ufficiale il 05 Giugno 2019.

TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, *"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."*

Il Regolamento UE 2016/679 pertanto ravvisa quali condizioni necessarie per il trattamento su detto la presenza di una base giuridica che lo giustifichi (l'art. 6, paragrafo 1 del GDPR) ed altresì il controllo dell'autorità pubblica l'autorizzazione del diritto dell'Unione o degli Stati membri, nel rispetto delle garanzie appropriate per i diritti e le libertà degli interessati.

La dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. "Statuto dei Lavoratori" (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata e sottoscritta dagli interessati.

La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita.

L'eventuale **comunicazione di dati particolari e giudiziari tra soggetti pubblici,** è ammessa solo in presenza di una normativa o di un regolamento che la giustifichino e, in ogni caso, qualora risulti necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi.

CARTELLA SANITARIA ELETTRONICA

La cartella socio sanitaria viene gestita in maniera informatizzata attraverso specifico software operativo.

Il software è installato in un server fisico dell'Amministrazione in cui sono memorizzati i dati della cartella socio sanitaria per il quale sono previste le misure per garantire la sicurezza dei dati volte ad impedire accessi da parte di soggetti non autorizzati e perdite o danneggiamento dei dati conservati.

E' prevista inoltre la conservazione documentale sostitutiva a norma dei documenti sanitari ex DPCM 3 dicembre 2013 affidata ad un fornitore esterno sulla base di un apposito contratto con assunzione di specifiche responsabilità ed obblighi da parte del fornitore relativamente alla sicurezza dei dati.

L'accesso al software per la gestione informatizzata della cartella socio sanitaria avviene attraverso specifiche credenziali di accesso che vengono assegnate dalla Direzione/Uffici amministrativi, previa formale richiesta del Responsabile dell'Ufficio/Area nell'ambito del quale verrà inserito o andrà a collaborare l'Utente. La richiesta dovrà contenere le generalità dell'Utente e l'indicazione della qualifica e delle mansioni che andrà a svolgere.

La medesima procedura andrà utilizzata qualora sia necessario apportare variazioni alle abilitazioni di accesso o procedere alla loro disattivazione per cessazione del rapporto di lavoro o collaborazione.

Le credenziali consistono in un codice identificativo dell'Utente (username o user id) ed una password.

I destinatari sono responsabili di tutte le attività svolte attraverso l'uso delle proprie credenziali. Pertanto, la password è personale e riservata e dovrà essere conservata con la massima cura e diligenza, senza comunicarla a terzi o divulgarla.

Al primo accesso la password dovrà essere modificata a cura dell'Utente e, successivamente, dovrà essere variata periodicamente secondo la cadenza prevista dal sistema che provvederà ad interdire in automatico l'accesso in caso di mancata variazione prima della scadenza di tale termine.

I profili degli utenti per l'accesso alla cartella socio sanitaria sono differenziati per abilitazioni e permessi tenendo conto della qualifica e delle mansioni dell'utente in modo che la conoscenza di dati, ed in particolare dati sensibili, degli Ospiti della struttura sia limitate alle effettive esigenze di servizio.

La Direzione, attraverso l'utente amministratore del software, può interrogare i log relativi agli accessi degli utenti al software di gestione delle cartella socio sanitaria ed agli accessi ai fascicoli degli Ospiti Utenti finali del servizio.

PARTE TERZA: DIRITTI DELL'INTERESSATO

INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni:**

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b. i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni necessarie** per garantire un trattamento corretto e trasparente:

g. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h. 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;
i. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j. il diritto di proporre reclamo a un'autorità di controllo;

k. 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 tali dati;

l. l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo Ente, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, sia fa rinvio al vigente **Prontuario (Massimario) Dell'Ente di conservazione e scarto.**

Per prontuario (massimario) di conservazione e di scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette di gestire in modo organizzato l'archivio Dell'Ente, permettendo di conservare solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità** diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del Regolamento.

In particolare:

- **il consenso deve essere "esplicito"** o il trattamento deve basarsi sul verificarsi dei casi previsti dal GDPR;
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle già puntate" su un modulo);
- deve essere manifestato attraverso **"dichiarazione o azione positiva inequivocabile"** (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Il Regolamento EU prevede tuttavia, sempre all'art. 6, ulteriori fattispecie in cui il trattamento è lecito, senza dover ricorrere al consenso. In particolare:

- il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso: La sussistenza tra le parti di un contratto o di una fase precontrattuale rappresenta un rapporto basato su uno scambio di volontà tale da implicare tacitamente la volontà necessaria per il trattamento dati. Tale presupposto legittimante il trattamento va interpretato in senso restrittivo, solo qualora il trattamento sia una condizione necessaria alla corretta esecuzione degli adempimenti contrattuali e precontrattuali;
- il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento: si intende a prescindere dalla natura giuridica dell'Ente (pubblica o privata), purché il compito sia di interesse della collettività.
- **Interesse legittimo prevalente di un titolare o di un terzo** presuppone invece che sia il titolare stesso ad effettuare un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato e non sia più compito dell'Autorità. Pertanto, l'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità. Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere **l'accesso** ai dati personali e alle seguenti informazioni:

a. le finalità del trattamento;
b. le categorie di dati personali in questione;

c. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f. il diritto di proporre reclamo a un'autorità di controllo;
g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h. l'esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il **diritto di accesso**, si fa rinvio alle vigenti diposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale nonché dal Garante per la privacy.

In questo Ente, la competenza sulla materia *de quo* è affidata al **Responsabile Dell'Ente della Trasparenza e della Prevenzione della Corruzione**

A tale riguardo, nel rinviare a quanto pubblicato al sito web Dell'Ente, si fa presente che:

a. per ***accesso documentale*** si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti dell'Ente, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184). Possono fare domanda tutti i cittadini portatori di un interesse *'diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso'* (art. 22, Legge 241/1990). Per presentare domanda, è necessario utilizzare il modello messo a disposizione sul sito internet dell'Ente (https://www.crascalabrin.it/altra-documentazione-e-modulistica/). Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).

b. per ***accesso civico*** si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 *"Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche*", e Decreto Legislativo 33 del 14/03/2013: *'Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni'*). La richiesta viene presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza dell'Ente utilizzando il modulo prodotto sul sito internet Dell'Ente. L'Ente, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Ente indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web Dell'Ente) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.

c. per ***accesso generalizzato*** si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013

('Decreto Trasparenza') e del D.lgs. 97/2016 (così detto *Freedom of Information Act* o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico. La richiesta viene presentata:

a. all'Unità Operativa che detiene i dati, le informazioni o i documenti;
b. all'Ufficio Relazioni con il Pubblico utilizzando il modulo pubblicato sul sito internet Dell'Ente.

Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza, con la comunicazione dell'esito al richiedente e agli eventuali contro interessati. Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato. Se il documento risulta già pubblicato nel sito Dell'Ente nel rispetto della normativa vigente, l'Ente indica al richiedente il relativo collegamento ipertestuale. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il **diritto "all'oblio",** che si configura come un diritto alla cancellazione dei propri dati personali **in forma rafforzata.**

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1).

DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** *(in attesa di tale rettifica da parte del titolare)* **o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento** *(in attesa della valutazione da parte del titolare).*

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze *(consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).*

Il diritto alla limitazione prevede che il dato personale sia **"contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, l'interessato ha il **diritto di opporsi in qualsiasi momento,** per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la **profilazione,** che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO

Il ***"Titolare"*** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della privacy, è il Centro Residenziali Anzini "S. Scalabrin".

Il Titolare, avvalendosi della supervisione e collaborazione del ***Data Protection Officer***, provvede:

a. a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
b. a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali,* impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
c. a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;
d. a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
e. a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **"responsabilizzazione"** (***accountability*** nell'accezione inglese) di titolari e responsabili, ovverossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questa Ente sta lavorando attivamente per far proprio l'approccio del Legislatore europeo relativo all'*accountability*.

CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento.** Essi determinano in modo trasparente, mediante un *accordo interno,* le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

DELEGATO DEL TRATTAMENTO DEI DATI

Secondo il D.lgs. 196/2003, s'intende per Responsabile del trattamento dei dati, *'la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali".*

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno", questo Ente, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario, come sempre avvenuto in passato, continuare a designare in ambito Dell'Ente i ***Delegati del trattamento dei dati personali,*** conferendo l'incarico a quei dirigenti apicali che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Delegato del trattamento deve:

1. trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento Dell'Ente nonché le specifiche istruzioni impartite dal Titolare;
2. garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
3. adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
4. tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;
5. mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;
6. contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il Responsabile per il trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il **Data Protection Officer (DPO) Dell'Ente**, al fine di:

a. comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti.*

b. utilizzare il modello Dell'Ente di *Informativa e Consenso* approvato con il presente Regolamento, verificandone il rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;

c. rispondere alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

d. contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Ente siano applicate all'interno dell'Ente stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;

e. informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Questo Ente ha provveduto alla **nomina dei Delegati del trattamento dei dati**, dandone comunicazione personale a ciascun Responsabile all'uopo nominato.

RESPONSABILE DEL TRATTAMENTO DEI DATI

Nell'ambito di questo Ente, sono inoltre individuati quali **Responsabili del trattamento dei dati personali**, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Ente, trattino dati di cui è titolare l'Ente medesimo e qualora siano in possesso dei requisiti previsti dall'articolo 28 del Regolamento EU (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
- trattare i dati personali, anche di natura sensibile e giudiziaria, degli ospiti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con l'Ente e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio

di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento" che possono anche essere definite dal Titolare del Trattamento;
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo *(sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati),* tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso l'Ente, il Responsabile del trattamento.

La designazione del Responsabile viene effettuata mediante "accordo di nomina" sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Ente.

Dopo l'approvazione del presente Regolamento, la UOC Affari Generali provvederà a trasmettere il presente Regolamento a tutte le strutture Dell'Ente interessate, evidenziando la necessità di provvedere alle nomine dei Responsabili utilizzando la modulistica adottata.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

AUTORIZZATO AL TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'*incaricato* al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere *"autorizzato"* al trattamento (articoli 4 e 10 del Regolamento).

Come già stabilito nel presente Regolamento, al momento dell'ingresso in servizio è fornita ad ogni interessato una specifica nomina in materia di privacy, con la quale detti soggetti vengono nominati quali **"autorizzati al trattamento dei dati"** ai sensi del Regolamento UE 2016/679.

Contestualmente alla nomina dovrà essere data copia del presente Regolamento o, in alternative, indicazioni per poterla scaricare dal sito internet Dell'Ente o intranet.

Il Regolamento contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di autorizzato), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

Nel caso di Autorizzati "esterni", l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del ***Data Protection Officer*** (DPO, in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come **attività principali i dati sensibili su larga scala**, come ospedali, assicurazioni e istituti di credito.

Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in **conflitto di interessi** in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

I suoi compiti sono:

- **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**
- **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

- **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;

- **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.** In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
- **operare alle dipendenze del titolare oppure sulla base di un contratto di servizio** (RPD esterno);
- **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

L'Ente ha provveduto al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte ai sensi dell'articolo 39 del Regolamento UE,

L'Ente ha previsto la pubblicazione dei dati di contatto del DPO sul sito istituzionale, inoltre, i suoi dati di contatto sono presenti all'interno di tutte le informative privacy.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese ***"data protection by default and by design"***, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso",* secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'Ente o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle caratteristiche questo Ente, non può che avere forma elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Il 05 Giugno 2019 il Garante della Privacy ha emanato il "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs 10 agosto 2018 n.101*" contenente le indicazioni specifiche per alcune fattispecie di trattamenti.

NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque *"senza ingiustificato ritardo",* ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di ***"Data Breach".***

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre *"senza ingiustificato ritardo";* fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento, nonché dalle "*Linee Guida in materia di notifica delle violazioni di dati personali – WP250, definite in base alle previsioni del Regolamento UE 2016/679*" adottate dal Gruppo di Lavoro Art.29 il 03 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) e dal Provvedimento del Garante sulla notifica delle violazioni dei dati personali del 30 Luglio 2019.

Il Titolare del trattamento, sentito il Data Protection Officer Dell'Ente, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento.**

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77 del GDPR); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36 del GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

PARTE SESTA: ATTUAZIONE IN AMBITO DELL'ENTE DEGLI ADEMPIMENTI EUROPEI

ENTRATA IN VIGORE E PUBBLICITA'

Il presente Regolamento entrerà in vigore dalla data di adozione con atto deliberativo del Consiglio di Amministrazione.

Il Regolamento verrà pubblicato sul sito internet dell'Ente e reso disponibile attraverso il portale web dedicato alle comunicazioni con il personale dipendente.

DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'

Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del CdA, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.

Quanto, invece, agli **Allegati tecnici** al presente Regolamento, si stabilisce quanto segue: poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità Dell'Ente che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione.

Gli eventuali aggiornamenti ai *documenti tecnici allegati* verranno, pertanto, inseriti in tempo reale sul sito internet Dell'Ente nell'apposita sezione dedicata alla "privacy europea", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo della mail *"everyone"*, così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.

ALLEGATO A – REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA

La valutazione delle misure di sicurezza da adottare deve essere vista nel contesto del rischio a cui è rivolta. Pertanto le misure di sicurezza vanno viste nel loro senso più ampio del termine partendo dal principio che l'art. 32 del Regolamento EU recita "*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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

Di seguito vengono riportate ad esempio alcune regole e principi di base per diverse misure di sicurezza che verranno implementate nel tempo.

Misure	**Regole / Principi da osservare**
Presenza di un sistema di allarme	E' importante che l'Ente si doti di impianto d'antifurto a tutela del patrimonio delle informazioni contenute al suo interno.
Custodia dei dati in armadi blindati e/o ignifughi	E' importante che gli uffici che trattano dati sensibili e giudiziari possano disporre di queste strutture per archiviare in modo consono tali informazioni.
Sistemi UPS e Generatori di corrente che garantiscano la continuità elettrica	Fondamentale a tutela delle attività soprattutto per gli strumenti elettronici. Da adottare necessariamente per tutti i server e per quei pc locali che non archiviano le informazioni sul server. Infatti questi ultimi non hanno delle procedure pianificate di backup e quindi è importante ridurre al minimo i rischi che gli sbalzi di tensione possono provocare sugli hard disk.
Digitazione password all'accensione del PC	Tutti i PC devono avere la password di Windows all'accensione del terminale, questo non vale solo come regola ma viene considerata una misura base di sicurezza.

Manutenzione programmata degli strumenti	Come tutte le macchine che si rispettano anche il sistema informativo va manutenzionato periodicamente sia attraverso l'aggiornamento dei suoi componenti sia con la pulizia periodica delle macchine stesse.
Utilizzo di un sistema firewall	Obbligatorio viste le forme di attacco sempre più intelligenti.
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente.
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Controllo degli accessi a siti internet non sicuri – Protezione della posta elettronica	E' importante la conoscenza da parte degli operatori della navigazione in Internet e dell'uso della posta elettronica. A questo proposito è stato introdotto il regolamento per l'uso del PC.
Utilizzo di un filtro antispam	All'interno dello spam (posta indesiderata) si annidano spesso dei fenomeni di illegalità informatica. E' importante dotare l'Ente di tale strumento
Utilizzo di un antivirus	Per quanto precedentemente detto, è importante la presenza di un antivirus in ogni posto di lavoro, considerata misura di sicurezza e ovviamente che sia aggiornato
Aggiornamento periodico di programmi per il controllo della vulnerabilità	E' importante che ogni pc sia periodicamente aggiornato sulle proprie vulnerabilità con gli appositi software.
Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro	E' importante che l'operatore conosca il regolamento per quanto concerne l'assenza dal posto di lavoro con il PC acceso.
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati e dei profili di autorizzazione	Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare

Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione	Rientra nel concetto della formazione del personale
Aggiornamento periodico delle credenziali di autenticazione	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Procedure di verifica sull'operato degli incaricati	È un compito ispettivo che il Responsabile della sicurezza dei dati personali può demandare anche a società esterne
Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio	Rientra nel concetto della formazione del personale
Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione	Rientra nel concetto della formazione del personale
Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento	Rientra nel concetto della formazione del personale
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati	Il backup deve essere metodico, non affidato alle singole volontà. E' per questo importante nominare l'Incaricato delle copie di sicurezza delle banche dati
Definizioni di responsabilità e sanzioni disciplinari	Rientra nel concetto della formazione del personale nonché è necessario integrare il codice di comportamento includendo sanzioni disciplinari nei casi in cui ci sia un comportamento difforme da quando indicato dal presente Regolamento
Formazione professionale	Rientra nel concetto della formazione del personale
Distruzione del cartaceo	E' importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi distruggi documenti
Per accedere sono attive le credenziali di autenticazione	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati	Il salvataggio dei dati è fondamentale in qualsiasi organizzazione

I dati cartacei sono chiusi in un armadio	Ogni documento deve essere possibilmente chiuso in un armadio. Qualora questo non possa essere possibile, sicuramente che possano essere chiusi i dati sensibili e quelli giudiziari

ALLEGATO B – DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni.

Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati Dell'Ente che contengono i già menzionati dati personali.

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.

L'Autorizzato al trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente

Ogni Autorizzato al trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Autorizzati al trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.

La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'Autorizzato.

L'Autorizzato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.

In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.

Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.

Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'Autorizzato del trattamento non dovrà lasciarli mai incustoditi.

L'Autorizzato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.

Al termine dell'orario di lavoro l'Autorizzato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.

I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.

Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.

Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro Autorizzato debitamente autorizzato.

Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.

È inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.

Documenti contenenti dati personali che, per una qualunque ragione, siano da cestinare, devono assolutamente essere distrutti in modo da risultare illeggibili a soggetti terzi non autorizzati che ne potrebbero entrare in possesso (es. addetti alle pulizie).

Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'Autorizzato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.

L'Autorizzato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.

È proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un autorizzato a potere trattare i dati in questione.

Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

ALLEGATO C – PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI – DATA BREACH

NORMATIVA DI RIFERIMENTO

La normativa di riferimento per la stesura del presente documento è la seguente:

Regolamento Europeo 679/2016 (o anche GDPR)	Regolamento generale sulla protezione dei dati
D.lgs. n.196/2003 e s.m.i.	Codice in materia di protezione di dati personali
Working Party 250 adottate il 3 ottobre 2017	*Linee Guida Sulla Notifica Delle Violazioni Dei Dati Personali Ai Sensi Del Regolamento (Ue) 2016/679*
Linee guida adottate dall'EDPB n. 1/2021	*Guidelines on examples regarding Data Breach Notification*
Raccomandazioni adottate dall'EDPB il 20 dicembre 2013	*Recommendations for a methodology of the assessment of severity of personal data breaches*

PREMESSA E SCOPO

La presente procedura ha lo scopo di determinare la procedura per la gestione e le segnalazioni dei **Data Breach** in conformità al GDPR. In particolare, è volta a stabilire un flusso di informazioni e attività da attuare in tali casi.

Si precisa che il GDPR definisce il Data Breach, ossia la violazione dei dati personali, come **una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati**.

A titolo esemplificativo ma non esaustivo, si ricorda che possono configurare violazioni di dati personali le seguenti casistiche:

- cyber-attacco mediante cui vengono rubati dati personali;
- sottrazione/perdita di materiale/dispositivi contenenti dati personali (es. pc, chiavette, documenti cartacei,…);
- furto di documentazione negli uffici o un furto di posta nella cassetta postale o il recupero di documenti non distrutti gettati nei rifiuti contenente dati personali;
- invio di un messaggio di posta elettronica contenete una lista di interessati con indicazione dei loro recapiti a destinatario errato;
- condivisione/diffusione di verbali riservati con soggetti non autorizzati;

- attacco ransomware che causa la crittografia dei dati e, dunque, la loro indisponibilità foss'anche temporanea;
- la serratura di un armadio contente archivi cartacei relativi alle carriere del personale tecnico amministrativo è stata forzata;
- circostanze impreviste quali incendi o allagamenti.

È opportuno precisare, inoltre, che ai sensi del Considerando 85 del GDPR, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Alla luce di tali disposizioni normative, il Titolare del Trattamento è tenuto a segnalare, ove necessario sulla base della normativa stessa e in accordo con le linee direttive della presente procedura, le violazioni che avesse subito all'Autorità di controllo, Autorità che per lo Stato italiano è da identificarsi nel Garante per la Protezione dei Dati Personali. Inoltre, nell'ipotesi in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche alla segnalazione dovrà seguire specifica comunicazione agli interessati.

Si segnala, infine, che in caso di mancata segnalazione il Titolare del Trattamento è passibile di sanzione ai sensi dellì'art. 83 del GDPR.

CAPO DI APPLICAZIONE

La presente procedura si applica a tutte le ipotesi di violazioni di dati personali trattati dall'Ente, siano esse sospette o confermate. Tali ipotesi devono essere prontamente individuate e vagliate dall'Ente quand'anche quest'ultimo trattasse suddetti dati in qualità di mero Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

DEFINIZIONI GENERALI

***Trattamento**:* qualunque operazione o complesso di operazioni, effettuati 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 e la distruzione di dati, anche se non registrati in una banca di dati.

***Dato personale**:* qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. In tale categoria rientrano per esempio: documenti di identità, indirizzi mail, coordinate bancarie, numeri di telefono,…

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. In tale categoria rientrano per esempio: infortuni, stato di salute, iscrizione al sindacato, gravidanza,…

***Dati giudiziari*:** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza. In tale categoria rientrano per esempio: informazioni del casellario, DASPO,…

Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile esterno del trattamento: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali.

Autorizzato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Designato. In tale categoria rientra il personale e i collaboratori dell'Ente.

Interessato: la persona fisica, cui si riferiscono i dati personali. In tale categoria rientrano per esempio: clienti, potenziali clienti, candidati, dipendenti,…

DESTINATARI DELLA PROCEDURA

L'Ente, coadiuvato dal Responsabile Privacy e dal Responsabile della Protezione dei Dati (DPO), ha il compito di assicurare l'attuazione della presente procedura e la corretta gestione delle violazioni di dati personali.

Ne consegue che la presente procedura dovrà essere condivisa con tutto il personale e da questo rispettata. Si precisa che laddove ci si riferisce al personale nella presente procedura ci si intende riferire, a titolo non esaustivo, ai seguenti soggetti: dipendenti, tirocinanti, consulenti, collaboratori, interinali.

Inoltre, la stessa necessita di essere messa a disposizione dei fornitori che svolgano anche il ruolo di Responsabili o sub-responsabili del Trattamento.

DOCUMENTAZIONE DELLE ATTIVITA' SVOLTE CON RIFERIMENTO ALLA GESTIONE DEI DATA BREACH

Il Titolare del Trattamento dovrà mantenere aggiornato nel corso di tutta la gestione del Data Breach il Registro delle Violazioni presente in One 679. **Il registro delle Violazioni deve essere continuamente aggiornato e messo a disposizione del Garante** qualora l'Autorità chieda di accedervi.

L'incarico di mantenere aggiornato tale documento viene affidato all'Ufficio Amministrativo. Tale documento insieme alla documentazione raccolta, ricevuta o prodotta durante la gestione di ciascuna violazione dovrà essere conservata in maniera strutturata e archiviata agli atti dell'Ente.

TIPOLOGIE DI VIOLAZIONE

A seconda dei casi una violazione può comportare:

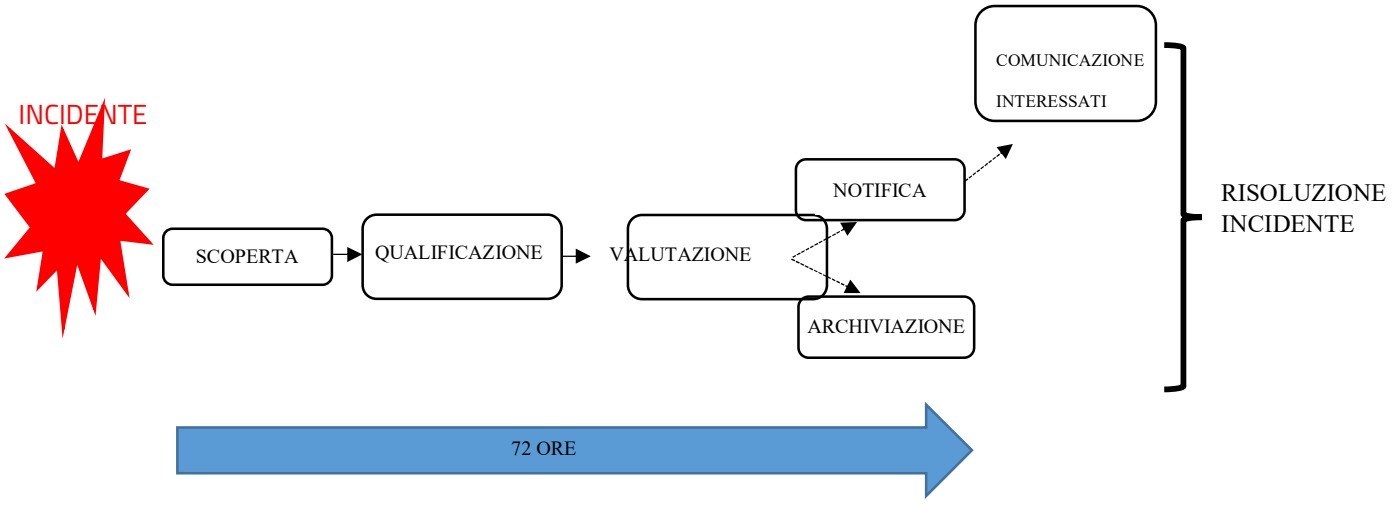
1. una perdita di riservatezza dei dati personali: quanto si ha una divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
2. una perdita di integrità: quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. una perdita di disponibilità: quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

È opportuno, in ogni caso, sottolineare che vi possono essere ipotesi in cui le precedenti casistiche si combinano nel contesto di una unica violazione. A titolo esemplificativo si consideri un attacco hacker che comporti sia la cancellazione dei dati a disposizione dell'Ente sia una loro contestuale diffusione nel dark web così determinando una perdita di riservatezza e integrità.

A di là delle conseguenze che una violazione di dati personali può generare, si significa che risulta di primaria importanza che la stessa venga riconosciuta e presa in considerazione dal Titolare del Trattamento affinché possano essere attuate contromisure o attività preventive.

FASI DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Di seguito si riporta lo schema delle fasi in cui si articola il processo di gestione dei Data Breach.



FASE 1: Scoperta e rilevazione del data breach

Qualunque autorizzato che accerti o riceva comunicazione circa un incidente di sicurezza che possa comportare una violazione di dati personali è tenuto a segnalarlo **immediatamente** al proprio Superiore gerarchico, il quale sarà tenuto ad informarne l'Ufficio Amministrativo e/o il DPO.

Nell'ipotesi in cui una violazione di dati personali dovesse verificarsi e/o essere scoperta al di fuori del normale orario di servizio, la stessa deve essere segnalata appena possibile e, in ogni caso, non appena si rientri in servizio.

In linea generale, il Titolare del Trattamento può essere informato di un incidente di sicurezza:

- dal personale/collaboratori dell'Ente;
- dal DPO;
- dal Responsabile del Trattamento o da un soggetto esterno;
- da un interessato;
- da articoli di stampa.

In linea generale, a seguito della segnalazione al proprio superiore gerarchico, l'autorizzato non è chiamato ad intraprendere ulteriori azioni in merito alla violazione a meno che il superiore gerarchico/Ufficio Amministrativo/DPO non ravvisi la necessità di un ulteriore coinvolgimento.

Ricevuta la segnalazione, il Superiore gerarchico dovrà raccogliere tutte le informazioni necessarie per segnalare i fatti al all'Ufficio Amministrativo e/o al DPO. In particolare, sarà opportuno che il Superiore gerarchico raccolga le seguenti informazioni, al fine di coadiuvare l'Ufficio Amministrativo nella compilazione del Registro delle Violazioni:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione;
- Tipologia di informazioni coinvolte;
- Descrizione dell'evento anomalo avendo cura di evidenziare se lo stesso sia ancora in corso;
- Categorie e numero, se noto, di Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Device Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione;
- Eventuali azioni già intraprese per porre rimedio alla violazione;
- Eventuali soggetti terzi coinvolti (es. fornitori).

Le segnalazioni del Superiore gerarchico devono essere tempestivamente comunicate all'Ufficio Amministrativo e/o al DPO ed in ogni caso entro 12 ore dalla conoscenza della violazione da parte del Superiore gerarchico. Tale comunicazione dovrebbe avvenire ove possibile a mezzo PEC o comunque tramite i canali istituzionali riferibili ai destinatari. Qualora il Superiore gerarchico non avesse provveduto a segnalare l'evento al DPO, l'Ufficio Amministrativo vi dovrà provvedere immediatamente.

Si ricorda che in ipotesi di violazione di dati personali la celerità nella gestione dell'evento è fondamentale al fine di rispettare gli obblighi gravanti sul Titolare del Trattamento. Ciò in quanto lo stesso è chiamato a **notificare la violazione dei dati personali all'Autorità di Controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che il Titolare del Trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite nelle fasi successive senza ulteriore ingiustificato ritardo.
Al fine di stabilire il momento di conoscenza della violazione da parte del Titolare del Trattamento si fa riferimento al momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Il Superiore gerarchico/Ufficio Amministrativo dovrà fin da subito attenzionare della vicenda i vertici direzionali dell'Ente e provvedere ad aggiornare gli stessi anche con riferimento alle fasi successive del processo di gestione del Data Breach.

FASE 2: Qualificazione e valutazioni inziali

Al ricevimento della segnalazione il Superiore gerarchico/Ufficio Amministrativo con il supporto del DPO e, se del caso, dell'Amministratore di sistema dovrà valutare se la violazione sia ancora in corso e, in tale ipotesi, stabilire le misure appropriate da adottare, mantenendo sul punto aggiornato il Registro delle Violazioni.

Qualora la violazione riguardi dati trattati dall'Ente in qualità di Responsabile esterno del Trattamento, le informazioni di cui all'elenco riportato nella Fase 1 dovranno essere immediatamente condivise con il Titolare del Trattamento. In tali ipotesi l'Ente dovrà supportare il Titolare nelle diverse fasi di gestione del Data Breach.

La Fase 2 del processo di gestione dovrà essere portata a termine **entro le 24 ore dalla conoscenza della violazione da parte del Superiore gerarchico/Ufficio Amministrativo**.

FASE 3: Valutazione della gravità della violazione e stima del rischio per gli interessati

La Fase 3 sarebbe opportuno che venisse condotta **entro le 48 ore dalla conoscenza della violazione da parte del Superiore gerarchico** al fine di permettere di inviare tempestivamente l'eventuale comunicazione all'Autorità Garante.

Il Superiore gerarchico/Ufficio Amministrativo, coadiuvato dalle altre funzioni competenti e dal DPO, provvederà, redigendo apposito documento riepilogativo che rimarrà agli atti, ad integrare le informazioni finora raccolte al fine di stabilire:

- **Tipologia del breach** (riservatezza, integrità, disponibilità) e presenza di un eventuale **intento malevolo**.
- **Natura e volume dei dati** coinvolti dal breach.
- **Facilità di identificazione** degli interessati.
- **Criticità delle conseguenze per gli interessati.**
- **Numero degli interessati** coinvolti del breach.
- **Caratteristiche del Titolare** dei dati oggetto del breach.
- **L'eventuale intellegibilità dei dati coinvolti**.

La valutazione della gravità della violazione verrà condotta sulla base della metodologia definita dall'ENISA nel documento *Recommendations for a methodology of the assessment of severity of personal data breaches*.

La violazione deve essere valutata secondo i livelli di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO
- MOLTO ALTO

L'analisi permetterà di stabilire in primo luogo la necessità di attivare le procedure di comunicazione e di notifica all'Autorità Garante. **Tale notifica si renderà necessaria in ipotesi di violazioni di gravità MEDIO-ALTA**. Rimane inteso che la metodologia sopracitata non è in grado di coprire tutte le possibili casistiche del caso concreto e, dunque, il Titolare del Trattamento può considerare di modificare i punteggi attribuiti alle categorie della metodologia in base agli elementi concreti che caratterizzano l'evento. In tali ipotesi, qualora gli elementi del caso concreto dovessero condurre a non ritenere necessaria la comunicazione nonostante il punteggio ottenuto, sarà opportuno che le motivazioni alla base della mancata segnalazione sia adeguatamente documentate e giustificate.

Fin da tale Fase, l'Ente dovrebbe provvedere ad individuare le misure tecniche ed organizzative per porre rimedio alla violazione ad attenuarne gli effetti negativi nonché quelle per prevenire che simili violazioni future avvengano.

FASE 4: Notifica all'autorità di controllo

Qualora, in base alle valutazioni di cui alla Fase 3, si stabilisse la necessità di effettuare una segnalazione all'Autorità Garante sarà necessario che la procedura di segnalazione sia effettuata collegandosi al portale dell'Autorità stesse fornendo le informazioni presenti anche nell'**Allegato A**. Per ultimare la procedura stessa sarà necessario attenersi alle istruzioni del portale riportate nella seguente pagina web https://www.garanteprivacy.it/regolamentoue/databreach.

Sarà compito del Ufficio Amministrativo, unitamente ai referenti interni incaricati della gestione della privacy, e con la costante supervisione del DPO, provvedere alla redazione della notifica e curarne il relativo invio in concerto con la Direzione.

La notifica dovrà pervenire all'Autorità possibilmente entro le 72 ore dall'avvenuta conoscenza della violazione. Diversamente si dovrà provvedere a motivare il ritardo nella segnalazione.

Qualora il Titolare non sia già in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva dell'infrazione, può adottare alcune tecniche o modalità che permettono di bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza.

Approssimazione: il Titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.

Notificazione in fasi: in questo caso il Titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'Autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica preliminare, tutte le informazioni per fasi successive, aggiornando di volta in volta l'Autorità sui nuovi riscontri.

Notifica differita: dopo le 72 ore previste dall'art. 33 del GDPR. È il caso in cui, per esempio, un'impresa subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al Titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il Titolare è autorizzato ad eseguire un'unica notifica aggregata di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Una volta effettuata la notifica il Ufficio Amministrativo e il DPO avranno cura di mantenere i rapporti e i contatti con l'Autorità Garante supportandola in ogni operazione e rispettando eventuali indicazioni dalla stessa provenienti.

FASE 5: Comunicazione agli interessati

Il GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunichi la violazione agli interessati senza ingiustificato ritardo. Tra i potenziali impatti da considerare sotto tale profilo si richiamo, a titolo esemplificativo, i seguenti:

- Danni economici o sociali

- Danni fisici, materiali o morali
- Perdita del controllo dei dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Decifratura non autorizzata della Pseudoanimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati protetti da segreto professionale (sanitari, giudiziari)
- Conoscenza da parte di terzi non autorizzati

Al fine di valutare se la comunicazione agli interessati sia dovuta si dovranno considerare sia gli esiti delle valutazioni di cui alla Fase 3 sia le ipotesi esemplificate contenute nell'**Allegato B** della presente procedura (tratte dal WP 250) e quelle presenti nelle *Guidelines 01/2021 on examples regarding Data Breach Notification*.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano uno dei seguenti casi:

- quando il Titolare del Trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).
- quando il Titolare del Trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.
- quando la comunicazione stessa richiederebbe sforzi sproporzionati e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

Rimane, in ogni caso, possibile per il Titolare ottenere, all'atto di notifica della violazione, una consulenza da parte della stessa Autorità di Controllo circa la necessità di informare le persone interessate.

Qualora fosse necessario operare la comunicazione agli interessati, devono sempre essere **privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti).** Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di *update* generali o *newsletter*, che potrebbero essere facilmente fraintesi dai lettori. Inoltre, dovrebbe tenere conto di possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es. l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile).

Inoltre, nelle ipotesi in cui si ritenga eccessivamente onerosa una segnalazione diretta, le modalità di comunicazione pubblica devono mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre

può ritenersi adeguata la comunicazione fornita attraverso evidenti *banner* o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa.

La comunicazione agli interessati dovrà avere i seguenti contenuti:

- descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali.
- nome e dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- descrizione delle probabili conseguenze della violazione dei dati personali.
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La predisposizione del messaggio agli interessati e la scelta delle modalità di comunicazione sono rimesse al Ufficio Amministrativo coadiuvato dal DPO e dovranno essere avvallate dalla Direzione.

All'**Allegato C** è possibile reperire una bozza di comunicazione agli interessati.

FASE 6: Risoluzione dell'incidente

Il Titolare del Trattamento, all'esito dell'incidente di sicurezza – a prescindere da una segnalazione all'Autorità Garante – e in virtù di quanto eventualmente precisato all'atto di notifica all'Autorità di Controllo, dovrà verificare l'efficacia delle misure preventive già adottate nonché implementare le stesse con le misure tecniche e organizzative necessarie sia per porre rimedio alla violazione e/o attenuarne gli effetti sia per prevenire eventi simili.

Occorrerà quindi revisionare correggere le lacune di sicurezza identificate, considerando, a titolo esemplificativo:

- le attuali misure di sicurezza;
- i metodi di trasmissione e la loro sicurezza;
- il livello di condivisione dei dati valutando l'effettiva necessità di tale condivisione;
- la necessità di condurre o aggiornare eventuali valutazioni d'impatto sulla protezione dei dati;
- il luogo e le modalità di archiviazione;
- la necessità di aggiornare le procedure interne e/o la modulistica;
- la formazione del personale in materia di protezione dei dati e il suo aggiornamento;
- la conoscenza delle procedure interne e dei regolamenti in capo al personale.

ALLEGATI

Allegato A - Fac simile di notifica all'Autorità di Controllo

Allegare il pdf scaricabile al seguente link

https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni

Allegato B - Esempi commentati di violazione

Esempio 1

Un supporto (cd/dvd/cassetta/ecc.) contenente un backup criptato con dati personali viene perso o rubato.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Se i dati vengono crittografati con un algoritmo di ultima generazione, esistono dei backup dei dati e la chiave privata non è compromessa, non è necessario notificare la violazione. Tuttavia, se venisse compromessa anche successivamente, la notifica diverrebbe necessaria.

Esempio 2

Durante un cyber-attacco al sito web vengono rubati dati personali.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e se è alto il livello di gravità dei potenziali danni.

Commento: Se il rischio non è elevato, consigliamo al titolare del trattamento di informare l'interessato, a seconda delle circostanze del caso. Ad esempio, la notifica potrebbe non essere necessaria in caso di violazione della riservatezza per una newsletter relativa ad un programma televisivo, mentre la notifica può essere richiesta se questa newsletter può portare a conoscenza del punto di vista politico del soggetto interessato.

Esempio 3

Una breve interruzione dell'alimentazione del call center del titolare del trattamento, che comporta l'impossibilità dei clienti di chiamare il titolare del trattamento e di accedere ai propri dati.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Questa non è una violazione dei dati personali da notificare, ma solo un incidente di cui tenere nota ai sensi dell'art. 33, paragrafo 5.
Il titolare del trattamento dovrà redigere un apposito registro.

Esempio 4

Un titolare del trattamento subisce un attacco ransomware che causa la crittografia di tutti i dati. Nessun back-up è disponibile e i dati non possono essere ripristinati. Al momento dell'indagine, risulta evidente che l'unico scopo del ransomware era quello di crittografare i dati e che nessun altro malware veniva rilevato nel sistema.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati, visto che questo attacco comporta una perdita di disponibilità dei dati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e dal possibile effetto della perdita di disponibilità dei dati, così come altre probabili conseguenze.

Commento: Se fosse disponibile un backup e se i dati potessero essere ripristinati in tempo utile, non sarebbe necessario segnalare al Garante o agli interessati poiché non ci sarebbe stata perdita permanente di disponibilità o riservatezza. Tuttavia, il Garante potrebbe considerare di verificare la conformità dei requisiti di sicurezza più ampi previsti dall'art. 32.

Esempio 5

Un interessato denuncia all'Ente una violazione di dati. Il soggetto ha ricevuto un documento contenente dati di qualcun altro.
Il titolare del trattamento intraprende una breve indagine (che va completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ciò è stato causato da un difetto sistemico che comporti il potenziale interessamento di altri soggetti.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: Vengono notificati i soggetti interessati solo se esiste un rischio elevato ed è chiaro che altri soggetti non sono stati coinvolti.

Commento: Se, dopo ulteriori indagini, si è stabilito che sono interessati più soggetti, sarà necessario aggiornare il Garante ed il titolare del trattamento dovrà intraprendere, come azione supplementare, la notifica ad altri soggetti, in caso di loro rischio elevato.

Esempio 6

Una società di hosting web individua un errore nel codice che controlla l'accesso da parte degli utenti. L'anomalia comporta che qualunque utente possa accedere ai dettagli dell'account di qualsiasi altro utente.

- Comunicazione al Garante: Come responsabile del trattamento, la società di hosting web deve notificare tempestivamente al Garante quali suoi clienti (titolari del trattamento) sono coinvolti. Supponendo che la società di

hosting web abbia effettuato una propria indagine, i titolari coinvolti dovrebbero essere ragionevolmente sicuri di sapere o meno di aver subito una violazione. Pertanto, è da considerarsi "avvisato" una volta è stato oggetto di notifica dalla società di hosting (il responsabile del trattamento). Il titolare dovrà in seguito notificare la violazione all'autorità di vigilanza.

- Comunicazione agli interessati: Se non esiste un rischio elevato per i soggetti interessati, la notifica non è necessaria.

Commento: La società di hosting web (responsabile) deve considerare tutti gli altri obblighi di notifica (ad esempio, nell'ambito della direttiva NIS).
Se non vi è alcuna prova che questa vulnerabilità sia stata sfruttata da un particolare soggetto titolare, una notifica di violazione non può aver luogo ma è probabile che sia registrabile o che rientri nei casi di non conformità, ai sensi dell'art. 32.

Esempio 7

Un attacco informatico causa la non disponibilità dei registri medici in un ospedale per il periodo di 30 ore.

- Comunicazione al Garante: Sì, l'ospedale è tenuto a notificare al paziente che potrebbe verificarsi un alto rischio per il suo benessere e la sua privacy.
- Comunicazione agli interessati: Sì, la notifica è necessaria.

Esempio 8

I dati personali di 5000 studenti sono inviati per errore ad una mailing list sbagliata con più di 1000 destinatari.

- Comunicazione al Garante: Sì, la notifica è necessaria.
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda dell'ambito e tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Esempio 9

Una e-mail di marketing diretto viene inviata ai destinatari nel campo "a:" o "cc:", consentendo così a ciascun destinatario di visualizzare l'indirizzo di posta elettronica di altri destinatari.

- Comunicazione al Garante: Sì, la notifica all'autorità di vigilanza può essere obbligatoria se è coinvolto un numero elevato di soggetti, se vengono rivelati dati sensibili (ad esempio una mailing list di un psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la mail contiene le password iniziali).
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda del tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Commento: La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili o se viene rivelato solo un numero ristretto di indirizzi di posta elettronica.

Allegato C - Modello di comunicazione agli interessati della violazione dei dati

G.mo Utente,

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, L'Ente _____, titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (data breach) che si è verificata in data _____[1], alle ore_____;[2] data_____alle ore_____;

NATURA DELLA VIOLAZIONE

_____
_____
_____

TIPO DI VIOLAZIONE:

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ _____
  _____

DISPOSITIVO OGGETTO DI VIOLAZIONE:

- ☐ Computer,
- ☐ Rete,
- ☐ Dispositivo mobile

[1] A. Tra il __e il____
B. In un tempo non ancora determinato
C. È possibile che sia ancora in corso

[2] Indicare l'ora se nota, altrimenti indicare l'ora in cui si viene a conoscenza della violazione.

☐ Strumento di backup

☐ Documento cartaceo

☐ _____

_____

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE PER ESEMPIO:

☐ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)

☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)

☐ Dati personali idonei a rivelare l'origine razziale ed etnica

☐ Dati personali idonei a rivelare le convinzioni religiose

☐ Dati personali idonei a rivelare filosofiche o di altro genere

☐ Dati personali idonei a rivelare le opinioni politiche

☐ Dati personali idonei a rivelare l'adesione a partiti

☐ Dati personali idonei a rivelare sindacati,

☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso,

☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico,

☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico

☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale

☐ Dati personali idonei a rivelare lo stato di salute

☐ Dati personali idonei a rivelare la vita sessuale

☐ Dati giudiziari

☐ Dati genetici

☐ Dati biometrici

☐ Copia per immagine su supporto informatico di documenti analogici

☐ Ancora sconosciuto

☐ _____

___

NOME E DEI DATI DI CONTATTO DEL DPO O UN ALTRO PUNTO DI CONTATTO PRESSO CUI OTTENERE PIÙ INFORMAZIONI:

_____
_____
_____
_____

DESCRIZIONE DELLE PROBABILI CONSEGUENZE DELLA VIOLAZIONE:

_____
_____
_____

DESCRIZIONE DELLE MISURE ADOTTATE O DI CUI SI PROPONE L'ADOZIONE PER PORRE RIMEDIO ALLA VIOLAZIONE DEI DATI PERSONALI[3]

_____
_____
_____

Scusandoci per quanto avvenuto rimaniamo a Sua disposizione per eventuali chiarimenti.

Firma Ente

[3] e anche, se del caso, per attenuarne i possibili effetti negativi

Allegato D - Riepilogo adempimenti

Per schematizzare gli adempimenti ricollegabili alle valutazioni sopracitate si riporta la seguente tabella che può essere un supporto sebbene solo indicativo per la gestione dei Data Breach.

LIVELLO DI RISCHIO	ADEMPIMENTI
Rischio assente o basso	1. Compilazione del Registro delle Violazioni
Rischio medio	1. Compilazione del Registro delle Violazioni 2. Notifica al Garante
Rischio elevato	1. Compilazione del Registro delle Violazioni 2. Notifica al Garante 3. Comunicazione agli interessati

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI DELL'ENTE

RIFERIMENTI NORMATIVI

- **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati) – GPDR;
- **Decreto Legislativo 196/2003** (Codice in materia di protezione dei dati personali) e s.m.i. – Codice della privacy;
- **Lavoro: le linee guida del Garante per posta elettronica e internet**, Garante della protezione dei dati, Gazzetta Ufficiale n. 58 del 10 marzo 2007, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1387522;
- **Misure e accorgimenti prescritti ai Titolari dei Trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema,** Garante della protezione dei dati, Gazzetta Ufficiale n. 300 del 24 dicembre 2008, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499;
- **Legge 20 maggio 1970, n. 300** (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento) – Statuto dei Lavoratori.

PREMESSE E FINALITÀ DEL REGOLAMENTO

L'Ente mette a disposizione Strumenti Dell'Ente - ossia dotazioni hardware e software nonché risorse informatiche/telematiche quali, a titolo esemplificativo, PC, notebook, tablet, smartphone, stampanti, email, software, applicativi, … – quali strumenti di lavoro atti a rendere la prestazione lavorativa/professionale.

Conseguentemente, l'Ente ha deciso di adottare il presente Regolamento al fine di fornire un quadro preciso di indicazioni per i Lavoratori e gli altri Destinatari (definiti infra) in merito alle corrette modalità di funzionamento degli strumenti sopracitati. Tali indicazioni, infatti, permetteranno di evitare problemi, disservizi, maggiori costi (di manutenzione o altri) nonché di minimizzare rischi/minacce alla sicurezza dei sistemi in uso e/o dei dati in essi contenuti (siano essi dati personali o pertinenti al patrimonio e all'attività dell'Ente).

L'uso di tali strumenti deve sempre ispirarsi ai principi di diligenza, buona fede e correttezza cui devono costantemente uniformarsi i soggetti che sono autorizzati all'uso degli stessi.

Il Regolamento ha, dunque, il precipuo fine di guidare il comportamento dei Destinatari affinché gli stessi non espongano sé o l'Ente a sanzioni pecuniarie o penali derivanti da un uso scorretto o illecito degli Strumenti ovvero a conseguenze pregiudizievoli per il patrimonio e/o per immagine dell'Ente.

Ulteriore fine del presente documento è rappresentato dalla volontà di codesta Ente di dare attuazione alle disposizioni contenute nel Regolamento UE 2016/679 (GDPR) nonché di allinearsi ai provvedimenti emanati dall'Autorità Garante della Protezione dei Dati (cfr. le linee guida sopracitate) al fine di garantire sia la protezione dei dati personali trattati mediante gli Strumenti Dell'Ente sia la salvaguardia del patrimonio informativo Dell'Ente.

Ne consegue che, ai fini del presente Regolamento, per "dati" deve intendersi l'insieme delle informazioni di cui i Destinatari vengano a conoscenza e di cui devono garantire riservatezza e segretezza (a prescindere dalla circostanza che si tratti o meno di dati personali). Ogni dato nell'accezione sopradescritta, infatti, è da considerarsi riservato.

Al contrario, non rientra tra le finalità del presente Regolamento il controllo a distanza e/o in forma occulta delle attività, delle abitudini o delle opinioni dei lavoratori.

Nel rispetto, dunque, delle previsioni di cui allo Statuto dei Lavoratori (cfr. art. 4 e 8 dello stesso) il Regolamento è atto a disciplinare le modalità di raccolta dei dati tramite gli Strumenti Dell'Ente nonché l'eventuale potere disciplinare in capo a codesta Ente in casi di uso improprio o non autorizzato dei sopracitati Strumenti.

Le prescrizioni di seguito previste integrano e specificano le istruzioni già impartite agli autorizzati ai sensi del GDPR e le informazioni già fornite agli interessati ai sensi dell'art. 13 del medesimo Regolamento Europeo, anche in ordine ai possibili controlli e alle conseguenze disciplinari in caso di violazione delle stesse ai sensi dell'art. 4, co. 3, dello Statuto dei Lavoratori.

CAMPO DI APPLICAZIONE

Il Regolamento si applica a tutti i soggetti che, a qualsiasi titolo, utilizzano gli Strumenti Dell'Ente (di seguito denominati anche "Destinatari" o "Utenti"). A titolo esemplificativo e non esaustivo, esso si applica:

- ✓ ai lavoratori subordinati, nonché in distacco o in somministrazione, a prescindere dalla durata del rapporto, dall'orario, dal ruolo, dalla funzione ricoperta o dalla modalità in cui viene resa la prestazione (per es. smart working);
- ✓ ai collaboratori dell'Ente indipendentemente dal rapporto contrattuale in essere;
- ✓ altri soggetti che si trovino in possesso di specifiche credenziali di autenticazione per accedere alla rete informatica dell'Ente o che, comunque, utilizzino altri Strumenti Dell'Ente, anche in ipotesi di uso solo temporaneo.

NORME DI COMPORTAMENTO GENERALI DA ADOTTARE NELL'USO DEGLI STRUMENTI DELL'ENTE

L'Utente è consapevole che gli Strumenti Dell'Ente sono di proprietà dell'Ente e sono messi a disposizione al fine di permettere allo stesso di rendere la prestazione. Conseguentemente, unicamente a tale fine tali Strumenti possono essere utilizzati.

I Destinatari del presente Regolamento devono improntare il proprio comportamento in relazione agli Strumenti Dell'Ente attenendosi ai principi di diligenza, correttezza e liceità. In particolare:

- Gli Strumenti non possono essere ceduti a terzi, a qualsivoglia titolo, nemmeno parzialmente (es. sim, auricolari, pc, …) né possono essere utilizzati da soggetti diversi dall'Utente assegnatario;
- Gli Strumenti devono essere correttamente custoditi e mantenuti in buono stato. L'Utente, dunque, è tenuto a segnalare eventuali malfunzionamenti/ disservizi/ comportamenti anomali/ danneggiamenti/ aggiornamenti ed a richiedere all'Ufficio Amministrativo che si provveda con i necessari interventi. Qualora i malfunzionamenti richiedessero un intervento urgente e avvengano durante orari/giorni di chiusura degli Uffici Amministrativi, la segnalazione potrà essere fatta attraverso la procedura informatizzata per le manutenzioni informatiche;
- Quando tali Strumenti dovranno essere restituiti – a prescindere dalle motivazioni che tale restituzione hanno comportato per es. cessazione del rapporto, cambio di mansione con relativa modifica degli Strumenti, … - essi dovranno essere integri ed in buono stato conservativo;
- In caso di furto, smarrimento o danneggiamento degli Strumenti Dell'Ente l'Utente dovrà darne pronta comunicazione all'Ufficio Amministrativo, fornendo allo stessa ogni utile chiarimento e/o informazione;
- Qualora il Destinatario debba allontanarsi dagli Strumenti Dell'Ente, in particolare in caso di apparecchi non fissi, dovrà assicurarsi che gli stessi si trovino in locali chiusi a chiave o siano comunque custoditi in luogo idoneo (es. armadio chiuso a chiave);
- Una diligente custodia degli Strumenti andrà effettuata anche qualora l'Utente sia autorizzato ad utilizzarli al di fuori dei locali Dell'Ente;
- È vietato utilizzare memorie di massa esterne (es. chiavette USB, hard disk, …) o servizi di web drive non esplicitamente autorizzati dal Titolare;
- Non è consentito modificare la configurazione hardware/software degli Strumenti forniti;
- E' vietato installare modem, schede di rete cablate o wireless o qualsiasi altro dispositivo di connessione, salvo espressa autorizzazione;
- Se lo Strumento è dotato di scheda modem o altro dispositivo di trasmissione dati, essi andranno disabilitati laddove si sia connessi alla rete Dell'Ente;
- Si ricorda inoltre che la funzione logout, laddove presente, deve essere utilizzata al termine di ogni giornata lavorativa/utilizzo specifico e che, in caso di assenza momentanea, la sessione di lavoro deve essere bloccata;
- I seguenti comportamenti risultano poi proibiti, salvo espressa autorizzazione del Titolare: installare e/o utilizzare dispositivi hardware esterni per uso non professionale/lavorativo; installare/copiare software/

programmi/ dispositivi; eliminare software/ programmi/ dispositivi installati per configurazione predefinita dal Titolare; connettere gli Strumenti a reti esterne;

- È vietata qualsiasi attività volta a compromettere o anche solo eludere i meccanismi di protezione adottati dal Titolare.

ASSEGNAZIONE, GESTIONE E REVOCA DELLE CREDENZIALI DI ACCESSO

Le credenziali di autenticazione per l'accesso agli Strumenti Dell'Ente vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile dell'Ufficio/Area nell'ambito del quale verrà inserito o andrà a collaborare l'Utente. La richiesta dovrà contenere le generalità dell'Utente e l'elenco degli Strumenti per i quali lo stesso sarà abilitato all'accesso.
La medesima procedura andrà utilizzata qualora sia necessario apportare variazioni alle abilitazioni di accesso.

Le credenziali consistono in un codice identificativo dell'Utente (username o user id) ed una password.
I destinatari sono responsabili di tutte le attività svolte attraverso l'uso delle proprie credenziali. Pertanto, la password è personale e riservata e dovrà essere conservata con la massima cura e diligenza, senza comunicarla a terzi o divulgarla. Ne consegue che è vietato:

- trascrivere le proprie credenziali/password su fogli, biglietti, post-it o altri supporti;
- inserire le credenziali in messaggi di posta elettronica (siano essi in chiaro o crittografati) né possono essere salvate su altri strumenti/documenti informatici (es file excel/word, …) che non siano protetti a loro volta da apposite credenziali;
- digitare la propria password in presenza di soggetti che possano vedere la tastiera;
- utilizzare credenziali diverse da quelle ricevute in quanto assegnate in virtù del ruolo ricoperto e alla luce del rapporto intercorrente con l'Ente.

Al primo accesso la password dovrà essere modificata a cura dell'Utente e, successivamente, dovrà essere variata ogni 3 mesi. In caso di mancata variazione prima della scadenza di tale termine il sistema provvederà ad interdire in automatico l'accesso.

La stessa dovrà avere adeguate caratteristiche di robustezza:

- Numero minimo di caratteri: 12;
- Deve essere composta da caratteri alfabetici sia minuscoli che maiuscoli, da caratteri numerici e da simboli speciali (es. !?/()*…);
- Non deve essere uguale ad altra password utilizzata nei due anni precedenti;
- Non deve contenere riferimenti agevolmente riconducibili all'Utente come il nome, la data di nascita, il numero di matricola, nomi o date relative a familiari, codice fiscale, ecc.

Qualora l'Utente ritenesse che la password abbia perso di riservatezza dovrà provvedere a sostituirla. Nel caso in cui, invece, la password venisse smarrita, l'Utente dovrà provvedere a effettuare un recupero della password per il tramite dell'Amministratore di Sistema.

Nel caso di cessazione del rapporto tra l'Ente e l'Utente, il Responsabile dell'Ufficio/area dovrà comunicare per iscritto all'Amministratore di Sistema la data in cui le credenziali dovranno essere disattivate.

Periodicamente viene effettuata da parte del Referente privacy e dall'Amministratore di Sistema una verifica delle utenze esistenti e dei rispettivi profili di accesso.

I log di accesso sono registrati e possono essere oggetto di controllo dall'Ente, per il tramite dell'Amministratore di sistema.

Potranno dunque effettuarsi controlli come previsto del presente Regolamento.

Le informazioni così raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del presente Regolamento, che costituisce adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del GDPR.

OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

Con riferimento alla postazione di lavoro, il destinatario dovrà osservare le norme di seguito previste.

- Il Destinatario dovrà autenticarsi a ciascun dispositivo/applicativo unicamente con le proprie credenziali e, al termine dell'utilizzo di quel dato dispositivo/applicativo, dovrà effettuare il logout, ossia l'operazione di chiusura della sessione, secondo le regole previste dal singolo Strumento;
- I dispositivi dovranno essere bloccati, laddove possibile, prima delle pause e, in generale, ogniqualvolta ci si allontani dalla postazione o vi sia un prolungato inutilizzo. Similmente si dovrà provvedere a disconnettersi dagli applicativi in uso. A tale fine, il Destinatario dovrà assicurarsi che sia previsto un sistema di logout automatico;
- É necessario accertarsi che persone non autorizzate non possano prendere visione della schermata del dispositivo - e ciò soprattutto quando l'utente inserisce le proprie credenziali - né di documenti/supporti contenenti dati personali;
- Al termine della giornata lavorativa o, comunque, dell'attività condotta, l'utente garantirà che la postazione fisica utilizzata sia priva di materiali o documenti contenenti dati personali. Tale materiale, infatti, andrà custodito in appositi cassetti/armadi debitamente chiusi o ad accesso limitato;
- Se previsto, chiudere i cassetti/armadi/aree ad accesso limitato a chiave;
- Raccogliere gli stampati e i documenti non più necessari e provvedere al loro smaltimento, ossia mediante distruzione degli stessi per il tramite di distruggi documenti o altri strumenti idonei a ridurre in piccoli pezzi gli stessi;

- L'Utente avrà il compito di provvedere alla definitiva eliminazione anche dei file informatici non più necessari. Ad ogni cancellazione dovrà essere svuotato anche il cestino;
- Al termine della giornata lavorativa, l'Utente dovrà provvedere a spegnere lo Strumento – che tale funzionalità preveda (es. pc e tablet) - secondo le modalità di disconnessione specifiche per ogni Strumento.

MEMORIZZAZIONE E PROTEZIONE DEI DATI

L'integrità e la disponibilità dei dati (inteso quali informazioni e dati Dell'Ente, compresi i dati personali trattati dal Titolare) è garantita unicamente qualora gli stessi vengano memorizzati nell'ambito dei sistemi improntati appositamente dal Titolare (es. server, appositi archivi cartacei, …).

Ne consegue che i Destinatari dovranno provvedere a trasferire nei pertinenti archivi/cartelle tutti i dati presenti negli Strumenti Dell'Ente e/o nelle memorie fisse o removibili autorizzate.

Si ricorda, peraltro, che le informazioni memorizzate possono essere unicamente quelle necessarie e sufficienti all'attività lavorativa / professionale ed è, dunque, buona pratica provvedere alla pulizia di file obsoleti, inutili o duplici almeno con cadenza semestrale.

Qualora sia necessario avere copia di tali dati, la stessa andrà salvata solo su supporti autorizzati dal Titolare i quali dovranno essere conservati in luoghi protetti (es. armadi e cassettiere chiusi a chiave). Inoltre, quando gli stessi andranno restituiti al Titolare (anche in ipotesi di sostituzione o distruzione del supporto) o consegnati a terzi, il Destinatario dovrà avere l'accortezza di verificarne il contenuto nonché provvedere a cancellare dati eventualmente non più necessari o non pertinenti.

Qualora vi sia un malfunzionamento dei sistemi o un errata configurazione / uso degli stessi, per qualsivoglia causa occorsi, che comportino che il Destinatario venga a conoscenza di dati che non è autorizzato a trattare (si pensi al ricevimento di una mail indirizzata ad altri), lo stesso dovrà esimersi dal consultare il documento e segnalare l'accaduto al proprio Responsabile affinché siano adottate le opportune misure anche in concerto con il Referente Privacy e l'Amministratore di Sistema.

REGISTRAZIONE DEGLI ACCESSI

L'Ente utilizza lo strumento del badge per registrare gli accessi. Gli stessi vengono consegnati esclusivamente al personale con lo scopo di registrarne gli accessi al luogo di lavoro.

I badge sono di proprietà Dell'Ente e affidati direttamente ai singoli Destinatari, i quali ne rispondono ad ogni titolo di legge. Essi non devono essere ceduti, né temporaneamente né per singolo utilizzo, a soggetti terzi quand'anche collaboratori, colleghi o persone di fiducia.

UTILIZZO DI COMPUTER E COMPUTER PORTATILI

I computer ed i computer portatili rappresentano uno dei principali Strumenti Dell'Ente di cui si avvale il Titolare.

Oltre alle disposizioni che riguardano gli Strumenti Dell'Ente in generale oppure una loro specifica modalità di utilizzo (es. uso della posta elettronica, …), si ricorda che trovano applicazione le seguenti regole di comportamento:

- L'accesso avviene mediante le credenziali strettamente personali;
- Non è consentita l'attivazione di password di accensione (BIOS) senza previa autorizzazione dell'Amministratore di Sistema;
- È obbligatorio consentire, al primo momento disponibile, l'installazione degli aggiornamenti di sistema che vengano proposti automaticamente;
- È vietato il loro uso per l'acquisizione/ riproduzione/ condivisione illegale di materiale protetto da copyright.

I log relativi all'utilizzo di tali Strumenti – reperibili nella memoria dello strumento stesso, sul server o sul router - ed i file con essi trattati possono essere oggetto di controllo da parte del Titolare, attraverso l'Amministratore di Sistema. Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

UTILIZZO DI INTERNET

L'Ente consente l'utilizzo di Internet mediante i devices assegnati all'Utente, previa identificazione con nome utente e password, laddove presente.

Inoltre, l'Ente si riserva di consentire l'accesso alla connessione internet Dell'Ente, per un uso occasionale, a collaboratori esterni, clienti o terzi che, comunque, saranno tenuti al rispetto delle regole dettate dal presente Regolamento.

Tutti i Destinatari devono rispettare le seguenti regole di comportamento:

- l'utilizzo del collegamento Dell'Ente al web deve essere effettuato unicamente per scopi connessi all'attività lavorativa e, in ogni caso, nel rispetto dei principi di liceità, diligenza e correttezza nonché del rapporto in essere tra l'Utente e l'Ente;
- la navigazione è consentita per i siti che contengono informazioni utili all'attività lavorativa ovvero forniscono idoneo supporto informativo professionale;
- l'Utente dovrà avvalersi esclusivamente degli internet providers selezionati dall'Ente;
- l'Ente può prevedere, mediante appositi strumenti di "filtro", il blocco di siti/categorie di siti ritenuti pericolosi o estranei alle attività condotte dall'Ente. In caso di blocco accidentale di siti d'interesse, l'Utente potrà contattare l'Amministratore di Sistema per lo sblocco;
- nell'ipotesi in cui si necessiti di una navigazione libera è necessario contattare l'Amministratore di Sistema e la Direzione dell'Ente indicando: Utente, motivo della richiesta, postazione da cui effettuare la navigazione, intervallo di tempo in cui l'attività verrà condotta. Una volta ottenuta l'autorizzazione, l'utente potrà svolgere l'attività richiesta e, al termine della stessa, l'Amministratore di Sistema ripristinerà i filtri;
- in ogni caso, non è consentito all'utente navigare o memorizzare file con contenuto o di natura contraria alle norme di legge, oltraggiosa, violenta, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione o appartenenza politica;
- l'Utente non dovrà installare software gratuiti o in licenza d'uso, di qualsivoglia natura, che non siano autorizzati dall'Ente;
- non è permesso partecipare a forum, utilizzare chat line, bacheche, social network, anche in ipotesi di uso di pseudonimi, per motivi non professionali e senza autorizzazione dell'Ente;
- non è consentito effettuare qualsivoglia tipo di transazione finanziaria (quali, a titolo esemplificativo ma non esaustivo, operazioni di home banking, acquisti online, mining di criptovalute, …) salvo i casi direttamente autorizzati dall'Ente e nel rispetto delle procedure di acquisto;
- è proibito violare la Legge sul Diritto d'Autore e/o le norme a tutela della proprietà industriale, in particolare, scaricando o condividendo illecitamente contenuti di qualsiasi genere (video, testi, immagini, brani, …) protetti dalla sopracitata normativa;
- i file di provenienza esterna o incerta, quand'anche ricollegabili all'attività lavorativa, devono sempre essere sottoposti al controllo dell'antivirus. In caso di dubbio sull'integrità o sulla sicurezza del file l'Utente è invitato a prendere contatti con il personale IT;
- non è consentito connettere gli apparecchi Dell'Ente a reti esterne, siano esse pubbliche o private, tramite collegamento fisico, mobile o wireless, senza esplicita autorizzazione;
- i Destinatari si impegnano a non interferire con il buon funzionamento dei sistemi informatici e di rete dell'Ente;
- l'Utente deve segnalare tempestivamente al personale IT e all'Amministratore di Sistema la presenza di attività sospetta sui propri sistemi o sulla rete;
- è vietato accedere alla webmail della casella di posta elettronica personale;

- per motivi tecnici e di buon funzionamento del sistema informatico è buona regola, salvo comprovate esigenze, non accedere a risorse web che impegnino in modo rilevante la banda;
- per permettere una comoda interazione tra colleghi, l'Ente può mettere a disposizione un sistema di messaggistica istantanea mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Anche per tali strumenti possono essere effettuati i controlli di cui al presente Regolamento.

L'Ente, per il tramite dell'Amministratore di sistema, non controlla in modo sistematico le pagine web né effettua controlli automatici sui dati di navigazione.

Tuttavia, l'Ente, per il tramite dell'Amministratore del Sistema, registra i dati di navigazione (file di log del traffico web) nel firewall fino a saturazione dello spazio disponibile senza però che sia identificato l'utente a cui fa capo il traffico internet.

Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

UTILIZZO DELL'INFRASTRUTTURA DI RETE

L'Ente dispone di una rete Dell'Ente cui possono accedere, mediante credenziali strettamente personali, unicamente gli Utenti a ciò abilitati.

L'accesso alla rete permette all'Utente di accedere alle cartelle sul server per potervi salvare i files rilevanti rispetto all'attività prestata, organizzati per area/ufficio oppure per criteri logici (area tematica, progetto, cliente, …).

Nell'utilizzo delle risorse di rete dovranno essere seguite le seguenti norme:

- le cartelle di rete possono ospitare esclusivamente contenuti professionali. Conseguentemente, non potranno essere salvati né sul server né sui dispositivi in dotazione, file di contenuto o natura personale. Qualora tale materiale dovesse essere reperito dall'Amministratore sul server, quest'ultimo provvederà ai sensi del di quanto previsto *infra* con riferimento ai controlli alla rimozione dello stesso, impregiudicata ogni ulteriore responsabilità civile, penale o disciplinare;
- al di fuori delle risorse di cui al server, l'Amministratore non effettua alcun controllo regolare e non vengono effettuati backup sulle altre risorse (ad es. cartella "desktop" dell'Utente, dispositivi di memorizzazione locale ad uso esclusivo, …). È responsabilità del singolo utente provvedere all'immediato salvataggio dei file di interesse nelle cartelle di rete di pertinenza;

- senza il consenso dell'Ente, è fatto divieto di salvare / trasferire documenti elettronici dai sistemi e strumenti dell'Ente in dispositivi esterni;
- senza il consenso dell'Amministratore di Sistema, è vietato salvare documenti dell'Ente in repository esterne (es. Google Drive, Dropbox, …);
- ciascun utente è responsabile della pulizia periodica degli archivi con cancellazione di file obsoleti o inutili. Particolare attenzione dovrà porsi in caso di file "doppi";
- è possibile accedere alle risorse di rete anche mediante la rete senza fili (wifi), presente all'interno delle sedi lavorative e sempre mediante autenticazione con credenziali;
- i servizi di connettività wireless di ogni tipo (salvo il wifi in caso di collegamento tramite tale modalità alla rete Dell'Ente) disponibili sui dispositivi utilizzati devono essere sempre disabilitati in particolar modo laddove si sia connessi alla rete Dell'Ente;
- è fatto divieto di collegare alla rete dispositivi non assegnati dall'Ente, salvo il caso in cui tale collegamento non sia appositamente autorizzato dall'Ente e vagliato dall'Amministratore di Sistema;
- l'Ente può permettere agli Utenti di accedere alla rete Dell'Ente dall'esterno. Tale accesso potrà avvenire mediante VPN, ossia un canale criptato e privato verso la rete interna, oppure tramite altre modalità congrue. Le richieste di abilitazione a tale modalità di accesso dovranno essere effettuate con le modalità di cui al presente Regolamento.

In ogni caso, l'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete qualora esso avvenga mediante strumenti non adeguatamente aggiornati o protetti.

Inoltre, l'Amministratore di Sistema ed il personale IT potranno provvedere alla rimozione di qualsivoglia file/applicazione che riterranno pericolosa per la sicurezza della rete Dell'Ente.

I log di accesso al sistema o all'intranet sono registrati e possono essere oggetto di controllo dall'Ente, per il tramite dell'Amministratore di sistema.

Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro di cui gli assegnatari sono responsabili sia sotto il profilo della garanzia della riservatezza delle credenziali di accesso sia sotto il profilo del corretto utilizzo.

L'Ente si riserva la possibilità di mettere a disposizione, sulla base di necessità operative/organizzative, indirizzi di posta impersonali per gli uffici/aree/gruppi di lavoro, ad uso comune, condivisi tra più soggetti assegnati al medesimo servizio/area. Di tali indirizzi sono responsabili gli assegnatari sotto i profili sopracitati.

L'utilizzo degli indirizzi impersonali è preferibile per tutte quelle comunicazioni di interesse collettivo.

Le seguenti regole trovano applicazione anche con riferimento agli indirizzi Pec Dell'Ente per i settori di competenza.

È fatto divieto di utilizzare la casella di posta per motivi diversi da quelli strettamente legati all'attività lavorativa e/o che esulino dall'espletamento delle mansioni affidate a ciascun Utente.

A titolo esemplificativo, l'Utente **non potrà**:

- inviare o ricevere allegati contenenti foto/filmati, brani musicali (o link a contenuti di tale genere) che non siano legati all'attività prestata;
- inviare o ricevere messaggi personali o per la partecipazione a dibattiti, aste online, forum, mailing list, newsletter, salvo diversa esplicita autorizzazione da parte del Responsabile area/ufficio;
- utilizzare l'indirizzo di posta per inviare messaggi di tipo umanitario, sociale o solidale, salvo diversa esplicita autorizzazione da parte del Responsabile area/ufficio;
- partecipare alle cosiddette catene di "sant'Antonio";
- creare, archiviare o spedire messaggi pubblicitari o promozionali in nessun modo connessi con lo svolgimento della prioria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto;
- inviare o memorizzare messaggi o file di natura oltraggiosa, violenta, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e/o politica;
- inviare le email ricevute e/o i dati attinenti all'attività condotta ad altro indirizzo email privato, nemmeno in periodi di assenza;
- utilizzare la casella di posta Dell'Ente per ragioni e/o finalità personali.

Inoltre, per una corretta fruizione del servizio di posta elettronica Dell'Ente devono essere rispettate le seguenti regole:

- per garantire la sicurezza della rete è necessario prestare particolare attenzione alla posta ricevuta. In caso di mail da mittenti sconosciuti o messaggi insoliti, di dubbia autenticità o di provenienza e/o con contenuti non attinenti all'attività svolta dall'Utente ovvero con contenuti anomali è necessario verificare la sorgente/intestazione del messaggio e, in caso di dubbio, contattare il personale IT. Ciò per evitare di essere infettati da virus/malware e/o di essere vittima di phishing. A seguito della verifica con individuazione di possibili minacce si dovrà procedere alla cancellazione dei messaggi senza aprirli;
- non dovranno essere aperti file con estensioni diverse da quelle comunemente in uso e/o con nomi sospetti o altre anomalie;

- qualora, in allegato ad una mail, vi dovessero essere file eseguibili (.exe) ovvero file di archivio compresso (.zip, .rar, .tar, …) è necessario accertarsi preventivamente del loro contenuto verificando il mittente (eventualmente tramite contatto diretto con lo stesso) e contattando il personale IT;
- è obbligatorio controllare i file ricevuti in allegato alla mail per accertarne la sicurezza contattando il mittente. Inoltre, in casi di dubbio o in ipotesi di cui al punto che precede, rivolgersi sempre al personale IT;
- non bisogna cliccare su link di provenienza dubbia o incerta senza averli verificati con il mittente nonché con il personale IT;
- nell'invio di allegati utilizzare solo formati comuni (.doc, .xls, .pdf, .ppt…) e accertarsi che non vengano superate le dimensioni massime consentite sia per il mittente (dimensioni massime 20 MB) che per il destinatario;
- nel caso in cui fosse necessario inviare allegati "pesanti" è opportuno ricorrere prima alla compressione degli stessi in formato .zip o equivalente. Se anche in tale modo il file risultasse eccessivamente pesante dovrà essere contattato il personale IT;
- la posta elettronica non deve essere utilizzata per ricevere, inviare o memorizzare materiale che violi le norme sul diritto d'autore o sulla proprietà industriale;
- **La casella deve essere mantenuta in ordine, cancellando messaggi e documenti inutili o la cui conservazione non è necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, prediligendo, il salvataggio dell'allegato nelle condivisioni. Inoltre, con cadenza mensile, l'Utente deve provvedere ad archiviare le mail di rilevanza per l'attività del Titolare nelle opportune cartelle del Server Dell'Ente;**
- è possibile utilizzare le funzionalità di "conferma di recapito" e "conferma di lettura";
- nell'eventualità di natura eccezionale che sia necessario inviare messaggi contenenti allegati con dati personali è obbligatorio che tali file vengano preventivamente resi inintelligibili tramite cifratura con apposito software (archiviazione e compressione con password). La password per cifrare il documento andrà comunicata al destinatario della comunicazione attraverso un canale diverso dalla mail e in nessun caso unitamente ai dati criptati stessi. Tali informazioni andranno, inoltre, inviate unicamente a destinatari legittimati a riceverle;
- la diffusione massiva di messaggi di posta elettronica deve essere effettuata unicamente per motivi inerenti al servizio e su autorizzazione del Responsabile dell'ufficio/area. I destinatari dovranno essere inseriti in copia conoscenza nascosta (Ccn);
- è vietato inviare messaggi in nome e per conto di altro soggetto, salvo una sua espressa autorizzazione;
- i messaggi in entrata vengono sistematicamente analizzati per la ricerca di virus e malware e per l'eliminazione di spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico;
- non è consentito salvare sulla propria area di server o sulle risorse condivise in rete file allegati a messaggi di posta di caselle diverse da quelle assegnate all'Utente;
- ogni email inviata dovrà riportare in automatico la nota di cui in calce:

"La presente comunicazione, unitamente alle informazioni in essa contenute e ogni documento o file allegato, è strettamente riservata e può contenere informazioni confidenziali. È rivolta unicamente ai destinatari cui è indirizzata e agli altri soggetti da questi autorizzati a riceverla.
Se non siete i destinatari/autorizzati siete avvisati che qualsiasi azione, copia, comunicazione, divulgazione o simili è vietata e potrebbe essere contro la legge.
Se avete ricevuto questa comunicazione per errore, vi preghiamo di darne immediata notizia al mittente e di distruggere il messaggio originale e ogni file allegato senza farne copia o riprodurne in alcun modo il contenuto.
Il destinatario è responsabile di proteggere i propri sistemi informatici da aggressioni esterne.
Ai sensi del Regolamento UE 679/2016 (GDPR), La informiamo che i nostri sistemi ed archivi comprendono recapiti relativi a persone fisiche, aziende, enti che hanno fornito gli stessi o con i quali sono intercorse precedenti comunicazioni. I dati saranno trattati solo dai nostri incaricati, debitamente autorizzati, e saranno conservati fino all'esaurirsi della finalità per cui sono stati raccolti. L'interessato potrà esercitare i diritti di cui agli Artt. 15 e ss del GDPR scrivendo al titolare del trattamento: RAGIONE SOCIALE, MAIL, PEC. È possibile inoltre presentare un reclamo all'autorità Garante della Privacy ai sensi degli Artt. 77 e ss del GDPR.
Si ricorda che questo indirizzo di posta elettronica non è un indirizzo di posta privato e perciò il suo uso è soggetto a regolamentazione.";

- è opportuno inserire in calce al testo della mail la propria firma accompagnata dall'indicazione della denominazione dell'Ente, dell'ufficio/unità di appartenenza e dei recapiti;
- ogni comunicazione – inviata o ricevuta - che abbia contenuti rilevanti o contenga impegni per l'Ente deve essere visionata o autorizzata dal superiore gerarchico.

Si informano gli Utenti che, in caso di richiesta da parte elle Autorità competenti (Guardia di Finanza, Autorità giudiziaria, …), le mail memorizzate sui server dell'Ente potrebbero essere rese note e consegnate alle stesse.

In caso di assenze programmate (es. ferie o attività di lavoro fuori sede, …) l'Utente dovrà utilizzare il sistema di risposta automatica indicando: la data di inizio del periodo di assenza, la data di ripresa del servizio, l'indicazione di altro Utente (con relativi recapiti) cui potrà essere inviata in copia la corrispondenza.

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e unicamente per improrogabili necessità lavorative, si debba conoscere il contenuto dei messaggi di posta elettronica, l'Utente può delegare un'altra persona (il cosiddetto "fiduciario") a verificare il contenuto dei messaggi ed inoltrare la corrispondenza rilevante all'attività lavorativa all'Ente. La nomina del fiduciario deve avvenire per iscritto.

In ogni caso, in ipotesi di assenza improvvisa o prolungata, l'accesso alla predetta cartella potrà essere effettuato dall'Amministratore di sistema su esplicita e motivata richiesta scritta dell'Ente. In tale ipotesi, l'Ente dovrà informare dell'accesso l'Utente assente.

Nel caso di cessazione del rapporto di lavoro ovvero della collaborazione tra l'Ente e l'Utente, per qualsiasi motivo intervenuta, la mail affidata all'Utente verrà disattivata immediatamente. Il sistema, in ogni caso, potrà generare una risposta automatica informando il mittente della disattivazione e invitando quest'ultimo a rivolgersi ad altro dipendente/funzione Dell'Ente.

Una volta disattivato l'account di posta, copia dei messaggi verrà conservata sul server centrale o sui backup dell'Ente entro i termini previsti dalla retention policy Dell'Ente, salvo che vi siano elementi che inducano l'Ente a ritenere necessario un periodo di conservazione più ampio (ad es. per finalità di difesa in giudizio) anche in seguito ad un eventuale valutazione di impatto ai sensi dell'art. 35 del GDPR.

L'Ente, per il tramite dell'Amministratore di sistema, non controlla in modo sistematico il flusso di comunicazioni mail né è dotata di sistemi di lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, ultronei rispetto a quanto tecnicamente necessario per svolgere il servizio di email.

Tuttavia, l'Ente, per il tramite dell'Amministratore del Sistema, può accedere all'account di posta prendendo visione dei messaggi, salvando o cancellando file come previsto dal presente Regolamento.

Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

USO PERSONALE

L'uso personale di internet o di servizi di web mail privati durante l'orario di lavoro e/o mediante gli Strumenti dell'Ente è consentito solo occasionalmente ed in ipotesi eccezionali e, in ogni caso, con modi, tempi e durata tali da non arrecare pregiudizio all'organizzazione del Titolare o all'attività lavorativa.

SOFTWARE

L'Ente mette a disposizione degli Utenti anche taluni software, per i quali vigono le seguenti regole di comportamento:

- L'Ente acquista le licenze d'uso dei software e dunque è soggetta a limitazioni nel loro utilizzo. Ne consegue che le medesime limitazioni valgono anche nei confronti dei Destinatari;
- I Destinatari non potranno riprodurre i software, salvo ragioni di salvataggio (copie di backup opportunamente documentate);
- All'infuori dei software messi a disposizione dell'Ente, gli Utenti non potranno utilizzarne altri, salvo espressa autorizzazione. Tale divieto vige in particolare per tutti quei software atti ad intercettare, falsificare o alterare il contenuto di documenti informatici (ad es. programmi di password recovery, cracking, sniffing, …);
- La manutenzione dei software verrà svolta da personale autorizzato cui i Destinatari dovranno rivolgersi;
- Qualora l'Utente dovesse venire a conoscenza di qualsivoglia criticità derivante dalla configurazione o da difetti intrinsechi dei software dovrà darne tempestiva comunicazione al personale incaricato;

- Non dovranno essere modificati gli standard di configurazione dei software installati.

ANTIVIRUS

Gli strumenti Dell'Ente, laddove tecnicamente possibile, verranno dotati di software antivirus adeguatamente configurati ed aggiornati. Ogni Utente deve comunque tenere comportamenti tali da minimizzare i rischi di attacchi informatici a danno del sistema informatico Dell'Ente.

Ogni dispositivo di provenienza esterna, per il cui utilizzo l'Utente deve essere già stato autorizzato, nonché i files eseguibili o contenenti software vengono verificati dall'antivirus.

Nel caso in cui l'antivirus rilevasse la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnare il dispositivo e segnalare l'accaduto al proprio responsabile che a sua volta si rivolgerà all'Amministratore di Sistema.

Un'eventuale segnalazione dovrà, inoltre, essere effettuata qualora il Destinatario accerti la non presenza o il mancato aggiornamento dell'antivirus.

SISTEMA DI CRITTOGRAFIA E SCAMBIO DATI

Lo scambio di informazioni di carattere personale con terzi autorizzati da contratti, convenzioni, o a fini lavorativi deve avvenire in modo sicuro e rispettoso della riservatezza dalle informazioni.

UTILIZZO DI TELEFONO FISSO/ CELLULARE/ SMARTPHONE/ TABLET/ FAX

Per quanto riguarda il telefono fisso/ cellulare/ smartphone/ tablet/ fax, non sono consentite comunicazioni a carattere personale o non strettamente inerenti all'attività lavorativa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, non sono consentite chiamate a numeri a pagamento, salvo espressa autorizzazione del proprio referente/responsabile.

Peraltro, per cellulare/smartphone/tablet, strumenti dei quali l'assegnatario sarà responsabile con riferimento al loro utilizzo e alla loro custodia, vigono le seguenti regole di comportamento, oltre a quelle già previste nei paragrafi sopra laddove compatibili (cfr. per es. uso strumenti elettronici, posta elettronica e navigazione Internet):

- proteggere tutti i dati presenti nel dispositivo anche mediante *"pin code"* (o analoghi strumenti), sistemi di blocco automatico dello schermo e cifratura;
- non scaricare/installare applicazioni non preventivamente richieste al proprio referente/responsabile ed autorizzate dall'Ufficio IT.

Rimane inteso che, in ipotesi di comprovato rischio per i dati presenti su cellulari/ smartphone/ tablet (es. furto, smarrimento, …) l'Ente si riserva la facoltà di intervenire anche da remoto sugli stessi. A tale fine, gli strumenti dovranno essere configurati in modo da consentire la ricezione di una richiesta remota di cancellazione dei dati e dei contenuti.

Per tali Strumenti potranno essere effettuati i controlli di cui al presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

UTILIZZO DI SISTEMI DI RIPRODUZIONE

L'uso di sistemi di riproduzione quali stampanti e scanner è consentito esclusivamente per motivi connessi all'esecuzione della prestazione lavorativa/professionale, anche nel rispetto dei principi di economia e di salvaguardia dell'ambiente.

La produzione di copie cartacee o informatiche di documenti, soprattutto se aventi natura riservata o contenenti dati personali, deve essere giustificata da una concreta necessità e l'Utente dovrà presidiare il processo di stampa/scansione al fine di impedire che terzi non autorizzati possano conoscere le sopracitate informazioni. Conseguentemente, sarà cura dell'Utente provvedere a recuperare immediatamente le stampe presso la fotocopiatrice e cancellare i file contenenti dati personali/riservati qualora siano accessibili a soggetti non autorizzati.

Si ricorda di prediligere le stampanti di rete condivise nonché stampare, laddove possibile, in bianco/nero e fronte/retro di modo da ridurre i materiali di consumo ed i costi.

Il loro utilizzo per fini personali può essere ammesso unicamente per ipotesi eccezionali e delimitate temporalmente e quantitativamente senza che ne venga incisa l'attività generale e l'organizzazione dell'apparato del Titolare. In tali ipotesi sarà cura del soggetto interessato circostanziare la richiesta al proprio Responsabile.

SISTEMI IN CLOUD

Utilizzare un servizio in cloud per memorizzare dati può esporre il Titolare a potenziali rischi. Ne consegue che è vietato il loro utilizzo eccettuato il caso in cui sia il Titolare stesso ad approvare taluni sistemi cloud.

ASSISTENZA DEGLI UTENTI E MANUTENZIONE

L'Amministratore di Sistema può accedere ai dispositivi sia direttamente sia attraverso software di accesso remoto per i seguenti motivi:

a. Verificare e risolvere problemi sistemici ed applicativi su segnalazione dell'Utente;
b. Verificare il corretto funzionamento dei singoli dispositivi qualora venissero rilevati problemi nella rete;
c. Evadere richieste di aggiornamento software o manutenzione preventiva;
d. Effettuare i controlli previsti dal presente Regolamento.

Per le ipotesi *a*, *b* e *c*, qualora l'effettuazione dell'intervento renda necessario l'accesso alle aree personali dell'Utente, l'Amministratore dovrà ottenerne il previo consenso. Diversamente, l'intervento tecnico che si limiti ad accedere ad aree non riservate all'Utente potrà effettuarsi senza il consenso di quest'ultimo.

Nel caso in cui soggetti terzi (es. fornitori) debbano accedere in teleassistenza ai dispositivi degli utenti, dovrà essere ottenuta per il primo accesso l'autorizzazione dell'Amministratore di Sistema che verificherà le modalità di intervento. Le richieste successive, invece, potranno essere gestite in autonomia dall'Utente purché avvengano con le modalità autorizzate dall'Amministratore.

Rimane inteso che gli interventi in teleassistenza di terzi richiedono sempre la presenza dell'Utente o dell'Amministratore di Sistema per impedire comportamenti non conformi al presente Regolamento.

Inoltre, qualora si rendesse necessario permettere l'accesso da remoto alla rete dell'Ente al personale di imprese fornitrici per l'adempimento di obblighi contrattuali in essere, l'Amministratore di Sistema è autorizzato, previa richiesta scritta da parte del Titolare, a rilasciare i profili autorizzativi. Rimane inteso che, in tali casi, al fornitore verrà data copia del presente Regolamento al quale quest'ultimo dovrà attenersi.

CONTROLLI SUGLI STRUMENTI
(AD INTEGRAZIONE DELL'INFORMATIVA PRIVACY GIA' CONSEGNATA)

L'uso degli Strumenti Dell'Ente, come analiticamente precisato nel Regolamento Dell'Ente sul loro utilizzo, può lasciare traccia di talune informazioni eventualmente contenenti dati personali dell'Utente.

In tale ambito rientrano anche i cosiddetti files di log ossia una serie di informazioni aggregate dei sistemi preposti alla gestione di internet, posta elettronica e rete interna Dell'Ente, che contengono dati relativi alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, data base, …). I files di log contengono tipicamente: data e ora dell'operazione effettuata, utente, tipologia dell'operazione e dati associati alla stessa.

Il Titolare si riserva la facoltà di effettuare controlli, nei limiti di quanto consentito dalle norme legali e contrattuali, sugli Strumenti Dell'Ente per:

1. Verificare l'integrità e la sicurezza dei sistemi;
2. Per la manutenzione degli Strumenti o altri motivi tecnici (es. aggiornamento, sostituzione, implementazione di programmi, …);
3. La tutela del patrimonio, compreso il patrimonio informativo;
4. Constare utilizzi indebiti e/o non conformi degli Strumenti Dell'Ente come definiti nel Regolamento anche su eventuale segnalazione di terzi o dell'Autorità Giudiziaria;
5. Comprovate esigenze produttive o organizzative.

Il datore di lavoro, infatti, può avvalersi, nel rispetto dell'art. 4 co. 3 dello Statuto dei Lavoratori, di sistemi che indirettamente consentono il controllo dei lavoratori purché nel rispetto delle procedure di informazione nei confronti dei lavoratori anche in base alla normativa privacy vigente.

In particolare, verranno rispettati i seguenti principi nel condurre i suddetti controlli:

- Proporzionalità: l'estensione del controllo dovrà avere un carattere adeguato, pertinente e non eccessivo;
- Trasparenza: il presente Regolamento ha il precipuo obbiettivo di informare gli Utenti sui diritti ed i doveri delle parti;
- Pertinenza e non eccedenza: non avverrà alcuna interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori né vi sarà alcun controllo prolungato, costante o indiscriminato.

Si segnala che le informazioni derivanti dai controlli condotti potranno essere utilizzabili a tutti i fini connessi al rapporto di lavoro. Ciò in quanto l'informativa ai lavoratori e il Regolamento sull'uso degli Strumenti Dell'Ente costituiscono idonea informazione circa le modalità d'uso degli Strumenti e dell'effettuazione dei controlli nel rispetto, in ogni caso, della normativa vigente.

Il mancato rispetto o la violazione delle regole contenute nel Regolamento sugli Strumenti Dell'Ente è perseguibile con provvedimenti disciplinari, così come disciplinati dal Ccnl ed altresì con le azioni civili e penali qualora si ravvisino gli estremi per integrare tali responsabilità.

CONTROLLO PER LE FINALITÀ 1,2,3,4

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per le finalità di cui ai punti 1, 2, 3, 4 il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

- I controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Destinatari e su dati aggregati tramite analisi statistiche, anche generali. Si sottolinea come gli stessi non verranno compiuti in modo prolungato, costante o indiscriminato;
- Avviso generico a tutti i dipendenti, o ad una specifica area/reparto, della presenza di comportamenti anomali e richiamo all'esigenza di attenersi ai compiti assegnati e alle istruzioni impartite;
- Dopo almeno 7 giorni ed in caso di persistenza del comportamento anomalo, l'Ente potrà autorizzare l'Amministratore di Sistema ad effettuare il controllo ossia ad accedere alle informazioni contenute negli Strumenti, con possibilità di rilevare siti web visitati, files trattati, software installati, statistiche sull'uso, …;
- Tale attività andrà effettuata in forma anonima;
- Si potrà effettuare un controllo su base individuale unicamente in caso di richiesta da parte dell'Autorità Giudiziaria, quando si verifichi un evento dannoso o una situazione di pericolo imminente ovvero quando i controlli di cui ai punti precedenti non hanno condotto alla risoluzione dell'anomalia;
- L' accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o, in caso di controllo su base individuale, mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso);
- Qualora sussista un grave ed imminente rischio rispetto alle finalità per le quali il controllo è condotto, l'Ente, unitamente all'Amministratore di Sistema, potrà attivarsi per intervenire immediatamente con un controllo su base individuale, senza operare dunque con una gradualità dell'azione di controllo. Rimane inteso che, in tale evenienza, l'Ente e l'Amministratore di Sistema avranno cura di precisare le motivazioni che hanno condotto ad effettuare tale scelta operativa;
- Redazione di un verbale che riassuma i passaggi precedenti e le motivazioni addotte per effettuare l'accesso.

CONTROLLO PER LA FINALITÀ 5

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per la finalità di cui al punto 5, il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

Si precisa che tale tipo di accesso è consentito unicamente quando concorrono i seguenti presupposti:

- assenza improvvisa o prolungata del dipendente; e
- improrogabili necessità legate all'attività lavorativa.

In tali ipotesi il Titolare si atterrà alla seguente procedura:

- Il Responsabile Area/ Ufficio ove è/era inquadrato l'Utente dovrà redigere documento scritto che comprovi le necessità produttive e/o organizzative e delimiti, per quanto possibile, la natura e specie delle risorse coinvolte;
- L'Interessato è messo in grado di delegare (cfr. modulo allegato) un altro soggetto operante all'interno della Struttura del datore di lavoro (fiduciario). Tale soggetto si occuperà di verificare il contenuto delle risorse coinvolte e di inoltrare all'Ente quello ritenuto rilevante per i fini di cui alla richiesta;
- La nomina del fiduciario deve avvenire per iscritto e la richiesta di accedere alla casella di posta dovrà essere effettuata dal Responsabile dell'ufficio/area del soggetto assente mediante richiesta scritta indirizzata al fiduciario;
- Nel caso in cui il lavoratore non abbia provveduto a indicare alcun Fiduciario, ovvero quest'ultimo non sia a sua volta reperibile, verrà dato incarico all'Amministratore di Sistema affinché acceda alle risorse informative necessarie. Tale accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso).
- Dell'accesso, inoltre, verrà redatto un verbale che verrà controfirmato dall'Amministratore di Sistema e dal fiduciario ed inviato al soggetto assente.

CONSERVAZIONE DEI DATI

I Dati relativi ai files di log verranno conservati per un periodo di 6 mesi. Nel caso in cui l'esercizio del diritto di difesa o una specifica richiesta dell'Autorità dovesse rendere necessario un prolungamento del tempo di conservazione, esso verrà effettuato limitatamente al soddisfacimento di tali necessità.

Il contenuto dei dispositivi di memorizzazione degli strumenti Dell'Ente, delle cartelle del server, degli account di posta elettronica, saranno conservati sul server centrale/backup secondo la politica Dell'Ente.

ISTRUZIONI IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO O DI COLLABORAZIONE

In caso di cessazione del rapporto di lavoro/collaborazione ovvero in tutti i casi in cui l'utente è chiamato a riconsegnare gli strumenti, la restituzione dovrà avvenire senza eliminare alcun dato Dell'Ente e mantenendo il dato stesso leggibile. Rimane inteso che, prima della riconsegna, il destinatario dovrà provvedere a eliminare qualsiasi dato personale a sé riferibile.

I dati Dell'Ente sopracitati non potranno essere conservati, duplicati, comunicati o diffusi dal Destinatario. Viceversa, gli stessi, verranno conservati in base alla policy Dell'Ente da parte dell'Ente.

SOCIAL MEDIA

L'eventuale utilizzo di canali social da parte dell'Ente verrà gestito e organizzato esclusivamente da quest'ultima sulla base di apposito Regolamento.

Ciò non toglie che, pur nel rispetto della libertà di espressione dei singoli utenti che collaborino con l'Ente, si debba considerare che gli stessi potrebbero essere identificati dai fruitori dei social quali soggetti alle dipendenze di codesta Ente. Ne consegue che gli Utenti sono chiamati a osservare un comportamento corretto e rispettoso.

Nello specifico, il personale ed i collaboratori sono chiamati ad attenersi alle seguenti regole:

- qualora volessero rendere pubblico il loro rapporto alle dipendenze dell'Ente sarà necessario che il soggetto indichi nel proprio profilo che le opinioni espresse all'interno del social sono puramente personali e non impegnano in alcun modo l'Ente;
- non possono essere divulgate, mediante i canali social, informazioni riservate, quali la corrispondenza interna, informazioni di terze parti (a titolo esemplificativo non esaustivo istituzioni, utenti, etc…) o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati e/o comunicati formalmente alle parti;
- possono essere liberamente condivisi sui profili personali i contenuti (od un rimando agli stessi) pubblicati nella pagina istituzionale dell'Ente;
- fermo restando il corretto esercizio delle libertà sindacali e del diritto di critica, non devono essere diffusi o trasmessi messaggi o dichiarazioni ingiuriose, minatorie o offensive nei confronti dell'Ente;
- non possono essere postati contenuti multimediali che riprendano i locali dell'Ente, il personale o i clienti dell'Ente senza l'esplicita autorizzazione delle persone coinvolte;
- deve essere rispettata la riservatezza dei colleghi evitando, conseguentemente, di pubblicare riferimenti alle attività lavorative svolte, salvo l'ipotesi in cui le stesse non siano di dominio pubblico.

L'interazione con i canali social in ogni caso è severamente vietata durante l'orario lavorativo.

DISPOSITIVI PERSONALI

L'utilizzo di dispositivi personali da parte dei dipendenti e dei collaboratori per rendere la prestazione oggetto di accordo con l'Ente dovrà essere preventivamente autorizzato nonché preceduto da una preventiva valutazione dello strumento da parte dell'Amministratore di Sistema. Quest'ultimo dovrà esaminare il dispositivo al fine di accertare la presenza di idonee misure di sicurezza.

Rimane inteso che tale verifica andrà condotta alla presenza dell'Utente. Per facilitare, in ogni caso, tali operazioni, all'Utente verrà fornita una lista di requisiti minimi di cui il dispositivo dovrà essere dotato.

SANZIONI

Il mancato rispetto o la violazione delle regole contenute nel Regolamento sugli Strumenti Dell'Ente è perseguibile con provvedimenti disciplinari, così come disciplinati dal Ccnl ed altresì con le azioni civili e penali qualora si ravvisino gli estremi per integrare tali responsabilità.

NORME FINALI

Il presente Regolamento entrerà in vigore con la Sua approvazione da parte dell'organo competente e farà parte integrante del Regolamento Privacy dell'Ente.

Con la sua entrata in vigore tutte le disposizioni precedentemente adottate in materia si intendono sostituite, qualora incompatibili o difformi, da quanto previsto dal Regolamento.

Esso verrà pubblicato sul sito istituzionale dell'Ente e sul portale per le comunicazioni con il personale. Inoltre, esso verrà affisso nei luoghi di lavoro ai sensi dell'art. 7 dello Statuto dei Lavoratori.

Tutti gli Utenti possono proporre integrazioni/modifiche motivate al presente Regolamento.

ALLEGATO 1: Informativa privacy per gli utenti degli strumenti Dell'Ente

Informativa privacy per gli Utenti degli Strumenti Dell'Ente

Egregio Sig.re / Gentile Sig.ra, ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR), il trattamento dei Suoi dati personali sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti. Pertanto, è gradito fornirle le seguenti informazioni.

Titolare del Trattamento

C.R.A. S. Scalabrin, con sede in Via IV Martiri n. 73 – Arzignano (Vi), tel. 0444-670683, e-mail segreteria@crascalabrin.it, PEC segreteria@pec.crascalabrin.it nella persona del Suo Legale Rappresentante pro tempore

Responsabile della Protezione dei Dati (DPO)

Tel. 049-0998416, e-mail dpo@robyone.net, PEC dpo.robyone@ronepec.it

Tipologia di dati raccolti

Dati personali relativi all'utilizzo del sistema informativo e degli Strumenti Dell'Ente.

Finalità

1. *Gestire e garantire l'utilizzo e la funzionalità degli Strumenti Dell'Ente assegnati;*
2. *Effettuare i controlli di cui al Regolamento sugli Strumenti Dell'Ente con lo scopo di garantire l'integrità e la sicurezza dei sistemi, la manutenzione degli Strumenti, la tutelare del patrimonio Dell'Ente, compreso il patrimonio informativo; di constare utilizzi indebiti e/o non conformi degli Strumenti Dell'Ente; di soddisfare comprovate esigenze produttive e organizzative.*

Base giuridica

Per le finalità sopracitate il trattamento è necessario al fine di eseguire un contratto di cui l'Utente è parte nonché per il perseguimento del legittimo interesse del Titolare o di Terzi, a condizione che non prevalgano interessi, diritti o libertà fondamentali dell'interessato (art. 6, parag. 1, lett. b) e f) del GDPR).

Destinatari dei dati

I dati potranno essere comunicati alle seguenti categorie di soggetti: soggetti incaricati della gestione del personale nell'ambito di rapporti di assistenza e consulenza; soggetti incaricati della tenuta dei dati informatici, della manutenzione hardware/software; soggetti che forniscono servizi per la gestione del sistema informativo del Titolare e delle reti di telecomunicazioni; legali incaricati della tutela del Titolare; autorità competenti per adempimenti di obblighi derivanti dalla legge e/o da disposizioni di organi pubblici, in particolare l'autorità giudiziaria nell'esercizio dei propri compiti giurisdizionali.

Conservazione

I dati del dipendente verranno conservati per il tempo minimo necessario alla loro funzione, nel rispetto del principio di minimizzazione del trattamento dei dati imposto dall'art. 5 par. 1 lett. c del GDPR. I Dati relativi ai files di log verranno conservati per un periodo di 6 mesi.

Obbligatorietà fornitura dei dati, motivazione e conseguenze mancata comunicazione

Il conferimento dei dati è obbligatorio. In mancanza non sarà possibile l'utilizzo degli strumenti assegnati.

Modalità di trattamento

I dati saranno trattati da persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare. Eventuali trattamenti da effettuare in esterno, per attività specifiche non eseguibili all'interno, vengono affidati a soggetti di comprovata affidabilità all'uopo nominati.

Diritti degli interessati

In qualsiasi momento, l'interessato esercitare il diritto di opposizione al trattamento dei dati che lo riguardano (art. 21 del GDPR).

Inoltre, lo stesso potrà avere accesso ai propri dati personali (art. 15 del GDPR), ottenerne la rettifica o la cancellazione, la limitazione del trattamento (art. 16, 17 e 18 del GDPR), la portabilità (art. 20 del GDPR).

Lei potrà esercitare i sopradescritti diritti contattando il Titolare o il Responsabile della Protezione dei Dati.

Potrà, infine, proporre reclamo all'autorità di controllo (Garante Privacy) (artt. 15, par. 1, lett. f , e 77 del GDPR).

ALLEGATO 2: Informativa sui controlli

Informativa sui controlli sugli Strumenti Dell'Ente utilizzati per rendere la prestazione.

L'uso degli Strumenti Dell'Ente, come analiticamente precisato nel Regolamento Dell'Ente sul loro utilizzo, può lasciare traccia di talune informazioni eventualmente contenenti dati personali dell'Utente.

In tale ambito rientrano anche i cosiddetti files di log ossia una serie di informazioni aggregate dei sistemi preposti alla gestione di internet, posta elettronica e rete interna Dell'Ente, che contengono dati relativi alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, data base, …). I files di log contengono tipicamente: data e ora dell'operazione effettuata, utente, tipologia dell'operazione e dati associati alla stessa.

Il Titolare si riserva la facoltà di effettuare controlli, nei limiti di quanto consentito dalle norme legali e contrattuali, sugli Strumenti Dell'Ente per:

1. *Verificare l'integrità e la sicurezza dei sistemi;*
2. *Per la manutenzione degli Strumenti o altri motivi tecnici (es. aggiornamento, sostituzione, implementazione di programmi, …);*
3. *La tutela del patrimonio, compreso il patrimonio informativo;*
4. *Constare utilizzi indebiti e/o non conformi degli Strumenti Dell'Ente come definiti nel Regolamento anche su eventuale segnalazione di terzi o dell'Autorità Giudiziaria;*
5. *Comprovate esigenze produttive o organizzative.*

Il datore di lavoro, infatti, può avvalersi, nel rispetto dell'art. 4 co. 3 dello Statuto dei Lavoratori, di sistemi che indirettamente consentono il controllo dei lavoratori purché nel rispetto delle procedure di informazione nei confronti dei lavoratori anche in base alla normativa privacy vigente.

In particolare, verranno rispettati i seguenti principi nel condurre i suddetti controlli:

- *Proporzionalità: l'estensione del controllo dovrà avere un carattere adeguato, pertinente e non eccessivo;*
- *Trasparenza: il presente Regolamento ha il precipuo obbiettivo di informare gli utenti sui diritti ed i doveri delle parti;*
- *Pertinenza e non eccedenza: non avverrà alcuna interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori né vi sarà alcun controllo prolungato, costante o indiscriminato.*

Si segnala che le informazioni derivanti dai controlli condotti potranno essere utilizzabili a tutti i fini connessi al rapporto di lavoro. Ciò in quanto l'informativa ai lavoratori e il Regolamento sull'uso degli Strumenti Dell'Ente costituiscono idonea informazione circa le modalità d'uso degli Strumenti e dell'effettuazione dei controlli nel rispetto, in ogni caso, della normativa vigente.

Il mancato rispetto o la violazione delle regole contenute nel Regolamento sugli Strumenti Dell'Ente è perseguibile con provvedimenti disciplinari, così come disciplinati dal Ccnl ed altresì con le azioni civili e penali qualora si ravvisino gli estremi per integrare tali responsabilità.

<u>CONTROLLO PER LE FINALITÀ 1,2,3,4</u>

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per le finalità di cui ai punti 1, 2, 3, 4 il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

- *I controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Destinatari e su dati aggregati tramite analisi statistiche, anche generali. Si sottolinea come gli stessi non verranno compiuti in modo prolungato, costante o indiscriminato;*
- *Avviso generico a tutti i dipendenti, o ad una specifica area/reparto, della presenza di comportamenti anomali e richiamo all'esigenza di attenersi ai compiti assegnati e alle istruzioni impartite;*
- *Dopo almeno 7 giorni ed in caso di persistenza del comportamento anomalo, l'Ente potrà autorizzare l'Amministratore di Sistema ad effettuare il controllo ossia ad accedere alle informazioni contenute negli Strumenti, con possibilità di rilevare siti web visitati, files trattati, software installati, statistiche sull'uso, …*
- *Tale attività andrà effettuata in forma anonima;*
- *Si potrà effettuare un controllo su base individuale unicamente in caso di richiesta da parte dell'Autorità Giudiziaria, quando si verifichi un evento dannoso o una situazione di pericolo imminente ovvero quando i controlli di cui ai punti precedenti non hanno condotto alla risoluzione dell'anomalia;*
- *L' accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o, in caso di controllo su base individuale, mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso);*
- *Qualora sussista un grave ed imminente rischio rispetto alle finalità per le quali il controllo è condotto, l'Ente, unitamente all'Amministratore di Sistema, potrà attivarsi per intervenire immediatamente con un controllo su base individuale, senza operare dunque con una gradualità dell'azione di controllo. Rimane inteso che, in tale evenienza, l'Ente e l'Amministratore di Sistema avranno cura di precisare le motivazioni che hanno condotto ad effettuare tale scelta operativa;*
- *Redazione di un verbale che riassuma i passaggi precedenti e le motivazioni addotte per effettuare l'accesso.*

CONTROLLO PER LA FINALITÀ 5

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per la finalità di cui al punto 5, il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

Si precisa che tale tipo di accesso è consentito unicamente quando concorrono i seguenti presupposti:

- *assenza improvvisa o prolungata del dipendente; e*
- *improrogabili necessità legate all'attività lavorativa.*

In tali ipotesi il Titolare si atterrà alla seguente procedura:

- *Il Responsabile Area/ Ufficio ove è/era inquadrato l'Utente dovrà redigere documento scritto che comprovi le necessità produttive e/o organizzative e delimiti, per quanto possibile, la natura e specie delle risorse coinvolte;*
- *L'Interessato è messo in grado di delegare (cfr. modulo allegato) un altro soggetto operante all'interno della Struttura del datore di lavoro (fiduciario). Tale soggetto si occuperà di verificare il contenuto delle risorse coinvolte e di inoltrare all'Ente quello ritenuto rilevante per i fini di cui alla richiesta;*

- *La nomina del fiduciario deve avvenire per iscritto e la richiesta di accedere alla casella di posta dovrà essere effettuata dal Responsabile dell'ufficio/area del soggetto assente mediante richiesta scritta indirizzata al fiduciario;*
- *Nel caso in cui il lavoratore non abbia provveduto a indicare alcun Fiduciario, ovvero quest'ultimo non sia a sua volta reperibile, verrà dato incarico all'Amministratore di Sistema affinché acceda alle risorse informative necessarie. Tale accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso).*
- *Dell'accesso, inoltre, verrà redatto un verbale che verrà controfirmato.*

ALLEGATO 3: Modulo Nomina Fiduciario

Nomina di soggetto fiduciario

Il/La sottoscritto/a _____ codice fiscale _____ in qualità di utente di _____

DELEGA

in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, i seguenti soggetti

nome e cognome _____ codice fiscale _____

nome e cognome _____ codice fiscale _____

nome e cognome _____ codice fiscale _____

a verificare il contenuto degli strumenti Dell'Ente da me utilizzati e ad inoltrare all'Ente quello ritenuto rilevante ai fini di cui alla richiesta.

Data _____

Firma _____

SOCIAL MEDIA POLICY

Il presente disciplinare riporta la *Policy* che il C.R.A. S. SCALABRIN (di seguito l'Ente) adotta sui *social media* dove è presente.

L'Ente ritiene che il *web* ed i nuovi *media* siano dei validi strumenti al fine di rendere maggiormente partecipata la comunicazione con gli utenti ed i destinatari dei servizi, informandoli sulle iniziative, sulle attività e sui progetti dell'Ente. Rappresentano dunque validi supporti ai canali comunicativi tradizionali per la loro capacità di garantire una maggior diffusività delle informazioni che l'Ente condivide con gli utenti.

Inoltre, attraverso l'utilizzo dei *social network* viene favorita la partecipazione, il confronto e il dialogo tra l'Ente ed i propri interlocutori.

In questi spazi e con queste attività Ente intende perseguire le proprie finalità istituzionali. In particolar modo, le pagine social nascono come strumento per permettere a familiari ed affetti degli ospiti di condividere, anche solo da lontano, la quotidianità dei propri cari accorciando virtualmente le distanze. Inoltre, le pagine social sono utilizzate quale mezzo per aggiornare i follower circa le novità e le offerte dell'Ente.

Al fine di perseguire le finalità sopraindicate il presente documento contiene anche:

- la SOCIAL MEDIA POLICY ESTERNA che racchiude le informazioni rivolte agli utenti/interessati circa le finalità, le tipologie di contenuti ed i comportamenti consentiti sulle pagine/profili istituzionali.
- la SOCIAL MEDIA POLICY INTERNA che individua, invece, le principali norme di comportamento che i dipendenti e collaboratori di Ente sono tenuti ad osservare nel momento in cui accedono ai *social network* con l'*account* istituzionale ovvero con i propri *account* personali.

DENOMINAZIONE DELLE PAGINE ISTITUZIONALI E DESCRIZIONE

La denominazione della pagina ufficiale è Centro Residenziale Anziani "S.Scalabrin".

Ove i *social media* lo permettano, l'account istituzionali riporterà la descrizione dell'Ente e dei servizi dallo stesso forniti. Nello specifico, verrà inserita la descrizione sotto riportata unitamente alla *Social Media Policy Esterna*. Inoltre, ove possibile verranno riportati anche i recapiti della struttura:

Descrizione: Il Centro Residenziale Anziani "S. Scalabrin" è una istituzione Pubblica di Assistenza e Beneficenza (I.P.A.B.) ed è costituito con lo scopo di operare nel campo dei servizi sociali con attenzione specifica nell'assistenza socio sanitaria dell'ospite anziano e/o disabile con la realizzazione di centri di servizio residenziale.

- Indirizzo Via IV Martiri n. 73 – 36071 Arzignano (Vi)
- Tel. 0444-670683
- Sito *web www.crascalabrin.it*
- Email segreteria@crascalabrin.it
- Link alla *Social Media Policy Esterna*

I NOSTRI ACCOUNT

L'Ente è presente su Facebook.

I suddetti profili sono gestiti dal Servizio Educativo.

Facebook

La pagina ufficiale dell'Ente è https://www.facebook.com/people/Centro-Residenziale-Anziani-SScalabrin/100054581913769/ .

Su Facebook è possibile condividere e commentare i contenuti pubblicati nel rispetto delle regole stabilite nella presente *Social Media Policy*. È possibile interagire con lo Staff, sia pubblicamente che tramite messaggi privati.

Non è utilizzato alcun meccanismo di pubblicazione automatica dei contenuti.

Sulla pagina potranno essere pubblicati: foto, video, articoli, comunicati stampa, notizie; dichiarazioni di referenti della Struttura, dichiarazioni di soggetti che collaborano con la Struttura e/o prendono parte ad attività, iniziative o progetti di cui alle finalità; comunicazioni provenienti da istituzioni pubbliche o da soggetti che perseguono interessi pubblici.

La decisione di seguire altre pagine non implica alcuna approvazione dei contenuti dalle medesime pubblicati.

Ciascun utente si assume la responsabilità del proprio comportamento sul social e si esprime a titolo personale.

I profili del personale sono gestiti in totale autonomia dallo stesso che se ne assume anche la relativa responsabilità.

SOCIAL MEDIA POLICY ESTERNA

La *Social Media Policy Esterna* contiene le informazioni rivolte agli utenti/interessati circa le finalità, le tipologie di contenuti ed i comportamenti consentiti sulle pagine/profili istituzionali.

Essa verrà resa pubblica sia nella pagina dei singoli canali *social* (ove possibile) sia nel sito *web* istituzionale dell'Ente.

COSA POSTIAMO?

I contenuti pubblicati sui *social media* attengono ai servizi, alle iniziative, alle attività ed ai progetti di Ente. I medesimi altresì possono comprendere informazioni di pubblico interesse ed utilità ricollegabili alle attività dell'Ente realizzate dalle istituzioni di riferimento o da soggetti terzi, previa verifica dell'attendibilità degli stessi.

In ogni caso, i sopracitati canali comunicativi potranno essere utilizzati quali terreno di dialogo e confronto con gli utenti del *web* affinché questi ultimi possano interagire con l'Ente inviando commenti, richieste domande e/o suggerimenti.

Sarà possibile per l'Ente pubblicare anche fotografie, video ed altri contenuti multimediali.

Si segnala, infine, che i contenuti pubblicitari presenti a margine delle pagine istituzionali non è controllata dall'Ente bensì dagli amministratori dei *social media*.

COSA NON POSTIAMO?

- Informazioni su tematiche oggetto di controversie legali o affermazioni che potrebbero essere utilizzate contro l'Ente;
- Informazioni riservate, come la corrispondenza interna, informazioni di terze parti (a titolo esemplificativo non esaustivo istituzioni, utenti, etc…) o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati e/o comunicati formalmente alle parti;
- Informazioni confidenziali e riservate;
- Informazioni di esclusivo interesse dei singoli.

MODERAZIONE

I canali *social* vengono moderati in orari di ufficio dal lunedì al venerdì salvo che la moderazione, per eventi o circostanze contingenti, avvenga in giorni e orari diversi.

Ogni richiesta viene monitorata e presa in carico. Peraltro, qualora le richieste provengano per il tramite di messaggi privati il primo riscontro sarà automatizzato ed avrà il seguente tenore "Il suo messaggio verrà preso in carico dal personale preposto che Le risponderà non appena possibile".

I riscontri da parte dell'Ente varieranno in base alla tipologia di richieste. In ogni caso, il fine dei medesimi sarà rispondere, ove possibile, ovvero indirizzare l'utente verso il pertinente ufficio/organo. Peraltro, l'Ente potrà inserire *link* a documenti o pagine *web* che forniscano adeguato supporto alla richiesta dell'utenza.

È necessario precisare, tuttavia, che per reclami o segnalazioni specifiche, l'Ente invita gli utenti ad indirizzare gli stessi all'Ufficio Amministrativo.

La pubblicazione dei *post* (contenenti o meno foto, video e/o tag) da parte degli utenti di Facebook sulla pagina dell'Ente non avviene in forma immediata e diretta. Soltanto dopo l'approvazione del post da parte dell'Ente, infatti, il post di terzi potrà trovare pubblicazione.

NETIQUETTE

L'Ente si impegna a gestire gli spazi di comunicazione dei *social media* attenendosi alle regole della *"netiquette"* delle quali chiede il rispetto anche da parte degli utenti esterni:

1. tutti hanno diritto di intervenire esprimendo liberamente la propria opinione purché la stessa venga espressa con misura e continenza, nel rispetto dell'opinione altrui e sia fondata, quanto più possibile, su dati verificabili;
2. requisito essenziale degli argomenti sui *social* è rappresentato dall'attinenza alle finalità rispetto alle quali gli *account* istituzionali sono stati aperti;
3. non è possibile utilizzare i canali telematici per affrontare casi personali o casistiche inerenti al singolo;
4. ogni discussione è legata ad un tema/argomento circostanziato. Pertanto gli utenti dovranno rispettare l'attinenza al medesimo.

NON SONO TOLLERATI:

1. contenuti discriminatori e/o offensivi nei confronti dei moderatori o di (gruppi di) utenti, enti, associazioni, aziende in ordine a genere, etnia, lingua, religione, opinioni politiche, condizioni personali o sociali, orientamento sessuale ed età;
2. insulti, turpiloqui, minacce o atteggiamenti che ledano la dignità personale, i diritti delle minoranze e dei minori, i principi di libertà e uguaglianza;
3. immagini/video o altri contenuti multimediali laddove permettano l'identificazione dei soggetti ritratti.

4. dati personali (caselle email, numeri di telefono, numeri di conto corrente, indirizzi) di colui che pubblica il contenuto o di terzi. In tali evenienze, essi verranno rimossi dalle pagine istituzionali.
5. interventi espressi con linguaggio inappropriato, minaccioso, volgare, licenzioso e/o contrario alla pubblica decenza;
6. argomenti e/o contenuti osceni, pornografici, che istigano alla violenza, denigratori, illegali, ingannevoli o che comunque offendono la morale e la sensibilità;
7. contenuti che violino il diritto d'autore;
8. pubblicità di prodotti e/o servizi di terzi;
9. argomenti propagandistici o politici;
10. contenuti catalogabili quali *spam*;
11. non pertinenti rispetto alla discussione in atto.

Qualora un contenuto/intervento dovesse rappresentare una violazione delle sopradescritte regole, lo stesso verrà **rimosso dall'Amministratore delle pagine/profili nonché sarà oggetto di segnalazione al gestore del *social media* (e, se del caso, alle competenti Autorità)**.

L'Ente si riserva, inoltre, la facoltà in tali cosi di bloccare e/o "bannare" l'utente in modo da impedire ulteriori interventi.

PRIVACY

Anche le piattaforme *social* in uso presso l'Ente hanno accesso alle informazioni che vengono condivise sui profili istituzionali.

Il trattamento dei dati da parte dell'Ente, in ogni caso, avviene in conformità al Regolamento UE 2016/679 ed al D.Lgs. n. 196/2003 (Codice Privacy) come novellato dal D.Lgs. 101/2018. Per maggiori informazioni si rinvia all'Informativa privacy presente al seguente link https://www.crascalabrin.it/altra-documentazione-e-modulistica/

CONTATTI

Gli utenti possono inviare eventuali segnalazioni (ad esempio abusi o violazioni del *copyright*) a: segreteria@crascalabrin.it.

SOCIAL MEDIA POLICY INTERNA

Il personale dell'Ente ed i collaboratori dello stesso (e/o i fornitori esterni della gestione dei *social media*) possono utilizzare le pagine istituzionali sia mediante un uso diretto dell'*account* istituzionale in rappresentanza dell'Ente sia mediante l'instaurazione di interazione tra i loro *account* personali e le pagine dell'Ente.

Il presente documento si rendere necessario per disciplinare suddette interazioni con le pagine istituzionali in quanto un utilizzo scorretto dei canali *social* può comportare diverse conseguenze quali, a titolo esemplificativo:

- la lesione dell'immagine e la reputazione dell'Ente;
- la sospensione o cancellazione del profilo istituzionali;
- danni diretti come richieste di risarcimento danni (es. violazione diritto d'autore) o denunce per diffamazione.

Al fine di disciplinare le modalità di uso degli *account* dell'Ente, in entrambe le ipotesi sopracitate, vengono qui individuate le norme di comportamento cui i soggetti sopraindicati dovranno attenersi.

RESPONSABILITA' DEI PROFILI ISTITUZIONALI

La registrazione ed apertura delle pagine istituzionali viene effettuata dalla Direzione.

Tale Ufficio, peraltro, gestisce le abilitazioni del personale (ovvero dei fornitori esterni) delegato alla gestione e pubblicazione di contenuti all'interno dei social come da apposita nomina rilasciata dall'Ente.

PUBBLICAZIONE E STILE COMUNICATIVO

I contenuti che verranno pubblicati dovranno riferirsi (anche per il tramite di semplici link alla pagina *web* istituzionale):

- alla promozione delle attività, dei servizi e dei progetti organizzati dall'Ente;
- ad argomenti di attualità che siano specificamente ricollegabili alle attività, ai servizi ed ai progetti organizzati dall'Ente.

NON dovranno, invece, essere pubblicati dati personali (di colui che pubblica o di qualsivoglia altro soggetto), materiali Dell'Ente o informazioni riservate o protette da *copyright* quand'anche ricollegabili alle attività sopracitate. Rimane inteso che, qualora la pubblicazione di tali dati fosse necessaria, dovrà preventivamente essere raccolto il consenso dell'interessato.

NON dovranno essere pubblicate immagini/video o altri contenuti multimediali laddove permettano l'identificazione dei soggetti ritratti. Resta ferma la possibilità che tali contenuti multimediali possano essere pubblicati - anche qualora il soggetto ritratto sia identificabile - nei casi in cui sia stato ottenuto il preventivo consenso scritto da parte dell'interessato conformemente a quanto previsto nel GDPR 679/2016.

È opportuno peraltro sottolineare che i *social* si inseriscono nel complessivo panorama comunicativo dell'Ente e dunque la loro gestione deve essere improntata al rispetto dei principi di:

- **costante aggiornamento**, affinché le informazioni contenute nelle pagine siano attuali e non riportino contenuti che possano ingenerare confusione nell'utenza;
- **chiarezza e trasparenza**;
- **coerenza dello stile espositivo** delle comunicazioni *social* rispetto a quanto avviene sui canali tradizionali dell'Ente;
- **rispetto, cura e attenzione nei confronti delle esigenze manifestate dall'utenza**;
- **professionalità**, in quanto i contenuti pubblicati rientrano pur sempre all'interno delle attività di un soggetto che agisce nella sua veste di attore istituzionale.
- Stabiliti dalla *"**netiquette**"* presente nella *Social Media Policy Esterna*.

Inoltre, il personale/collaboratore/fornitore che pubblica nelle pagine istituzionali dovrà adeguarsi allo stile comunicativo proprio del *social media* adottato. A titolo esemplificativo:

- Twitter prevede la pubblicazione di messaggi telegrafici, coincisi e d'impatto;
- Linkedin è caratterizzato da uno stile maggiormente istituzionale ed indirizzato a rivolgersi al modo del lavoro ed ai professionisti del settore;
- Facebook è la piattaforma maggiormente vicina all'utenza e caratterizzata dalla partecipazione ed interazione diretta.

Per quanto concerne la gestione di richieste provenienti dall'utenza si invita il personale/collaboratore/fornitore:

- a ricorrere alla messaggistica privata ovvero a segnalare i contatti dell'ufficio competente cui reiterare la richiesta, qualora nell'area pubblica del *social* l'utenza dovesse pubblicare richieste di rilevanza puramente soggettiva;
- ad inviare all'Ufficio Amministrativo eventuali richieste di informazioni non pertinenti al messaggio diffuso, segnalazioni o reclami, anche se pervenuti attraverso messaggi privati.

USO PRIVATO DEI SOCIAL NETWORK

Nell'utilizzo dei propri account personali, i dipendenti ed i collaboratori della struttura devono considerare come gli stessi possono essere identificati comunque dall'utenza quali soggetti alle dipendenze della struttura. Conseguentemente, essi sono tenuti ad osservare un comportamento corretto e rispettoso.

Nello specifico, il personale ed i collaboratori sono chiamati ad attenersi alle seguenti regole:

- qualora volessero rendere pubblico il loro rapporto alle dipendenze dell'Ente sarà necessario che il soggetto indichi nel proprio profilo che le opinioni espresse all'interno del *social* sono puramente personali e non impegnano in alcun modo l'Ente;
- non possono essere divulgate mediante i canali *social* informazioni riservate, quali la corrispondenza interna, informazioni di terze parti (a titolo esemplificativo non esaustivo istituzioni, utenti, etc…) o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati e/o comunicati formalmente alle parti;
- possono essere liberamente condivisi sui profili personali i contenuti (od un rimando agli stessi) pubblicati nella pagina istituzionale dell'Ente;
- fermo restando il corretto esercizio delle libertà sindacali e del diritto di critica, non devono essere diffusi o trasmessi messaggi o dichiarazioni ingiuriose, minatorie o offensive nei confronti dell'Ente;
- non possono essere postati contenuti multimediali che riprendano i locali dell'Ente, il personale o gli ospiti/utenti dell'Ente senza l'esplicita autorizzazione delle persone coinvolte;
- deve essere rispettata la riservatezza dei colleghi evitando, conseguentemente, di pubblicare riferimenti alle attività lavorative svolte, salvo l'ipotesi in cui le stesse non siano di dominio pubblico.

La violazione di tali regole di comportamento, oltre alle eventuali responsabilità sul piano civilistico o penale, comporterà l'irrogazione di una sanzione disciplinare determinata in base alla gravità della violazione.

POLICY SULL'USO DI WHATSAPP

Il presente disciplinare riporta la *Policy* che Ente adotta su Whatsapp.

L'Ente ha ritenuto utile attivare sui numeri di telefono Dell'Ente l'applicazione di messaggistica istantanea Whatsapp Business per comunicare con facilità con i propri utenti.

Al fine di perseguire le finalità sopraindicate il presente documento contiene anche:

- la POLICY ESTERNA che racchiude le informazioni rivolte agli utenti/interessati circa le finalità, le tipologie di contenuti ed i comportamenti consentiti.
- la POLICY INTERNA che individua, invece, le principali norme di comportamento che i dipendenti e collaboratori di Ente sono tenuti ad osservare nel momento in cui utilizzano l'applicazione.

DENOMINAZIONE DEL "PROFILO DELL'ENTE" E DESCRIZIONE

Il C.R.A. S. Scalabrin detiene due numeri di telefono Dell'Ente legati all'applicazione e gestiti in particolare da:

- Numero 3895647796 Servizio Educativo
- Numero 3488940123 Ufficio Amministrativo

Le informazioni dell'attività svolta riporteranno il testo di cui sotto nonché un rimando all'informativa privacy e alla Policy Esterna: "Gentile Utente, la informiamo che proseguendo nelle richieste ci conferirà dei dati che codesto Ente acquisirà unicamente per fornirle le risposte di cui necessita. Il prosieguo di tale conversazione implicherà un suo consenso al trattamento ai sensi della vigente normativa privacy. L'informativa estesa sarà reperibile al seguente link https://www.crascalabrin.it/altra-documentazione-e-modulistica/."

Inoltre, ove possibile verranno riportati anche i seguenti recapiti:

- Indirizzo Via IV Martiri n. 73 – 36071 Arzignano (Vi)
- Tel. 0444-670683
- Sito web www.crascalabrin.it
- Email segreteria@crascalabrin.it
- Link alla Social Media Policy Esterna

La gestione dell'applicazione è affidata a personale debitamente autorizzato.

POLICY ESTERNA

La *Policy Esterna* contiene le informazioni circa le finalità, le tipologie di contenuti ed i comportamenti consentiti mediante l'applicazione di messaggistica.

CONTENUTO DEI MESSAGGI

I contenuti dei messaggi hanno come fine il mantenimento di un contatto con l'interessato al fine di gestire le sue richieste.

MODERAZIONE

L'applicazione viene gestita dal personale debitamente autorizzato.

Ogni richiesta viene monitorata e presa in carico dall'operatore che si assicura di avere ricevuto l'autorizzazione all'utilizzo dello strumento da parte dell'interessato.

È necessario precisare, tuttavia, che eventuali reclami o segnalazioni specifiche, l'Ente invita gli utenti ad indirizzare gli stessi all'Ufficio Amministrativo.

NETIQUETTE

Nell'uso dell'applicazione di messaggistica dovranno essere seguite le seguenti regole.

NON SONO TOLLERATI:

12. contenuti discriminatori e/o offensivi nei confronti dei moderatori o di (gruppi di) utenti, enti, associazioni, aziende in ordine a genere, etnia, lingua, religione, opinioni politiche, condizioni personali o sociali, orientamento sessuale ed età;
13. insulti, turpiloqui, minacce o atteggiamenti che ledano la dignità personale, i diritti delle minoranze e dei minori, i principi di libertà e uguaglianza;
14. immagini/video o altri contenuti multimediali non pertinenti alle finalità sopracitate;
15. invio di dati personali che non siano pertinenti alle finalità sopracitate o che riguardino un soggetto terzo che non ha autorizzato l'utente a comunicare tali dati.
16. interventi espressi con linguaggio inappropriato, minaccioso, volgare, licenzioso e/o contrario alla pubblica decenza;
17. argomenti e/o contenuti osceni, pornografici, che istigano alla violenza, denigratori, illegali, ingannevoli o che comunque offendono la morale e la sensibilità;

18. contenuti che violino il diritto d'autore;
19. pubblicità di prodotti e/o servizi di terzi;
20. argomenti propagandistici o politici;
21. contenuti catalogabili quali *spam*;
22. non pertinenti rispetto ai servizi/attività dell'Ente.

Qualora un contenuto dovesse rappresentare una violazione delle sopradescritte regole, lo stesso verrà **rimosso dal personale incaricato nonché sarà oggetto di segnalazione al gestore (e, se del caso, alle competenti Autorità)**.

L'Ente si riserva, inoltre, la facoltà in tali cosi di bloccare e/o "bannare" l'utente in modo da impedire ulteriori interventi.

PRIVACY

Il trattamento dei dati da parte dell'Ente, in ogni caso, avviene in conformità al Regolamento UE 2016/679 ed al D.Lgs. n. 196/2003 (Codice Privacy) come novellato dal D.Lgs. 101/2018. Per maggiori informazioni si rinvia all'Informativa privacy presente al seguente link https://www.crascalabrin.it/altra-documentazione-e-modulistica/

CONTATTI

Gli utenti possono inviare eventuali segnalazioni a: segreteria@crascalabrin.it.

POLICY INTERNA

Il personale dell'Ente ed i collaboratori dello stesso (e/o i fornitori esterni) possono utilizzare l'applicazione di messaggistica mediante i dispositivi messi a disposizione dall'Ente o dallo stesso autorizzati.

Il presente documento si rendere necessario per disciplinare suddette interazioni in quanto un utilizzo scorretto può comportare diverse conseguenze quali, a titolo esemplificativo:

- la lesione dell'immagine e la reputazione dell'Ente;
- la sospensione o cancellazione del "profilo";
- danni diretti come richieste di risarcimento danni o denunce.

Al fine di disciplinare le modalità di uso vengono qui individuate le norme di comportamento cui i soggetti sopraindicati dovranno attenersi.

RESPONSABILITA' DELL'APPLICAZIONE

L'applicazione viene attivata dall'Ufficio Amministrativo.

Tale Ufficio, peraltro, gestisce le abilitazioni del personale (ovvero dei fornitori esterni) delegato alla gestione della messaggistica come da apposita nomina rilasciata dall'Ente.

RISPOSTE E STILE COMUNICATIVO

I contenuti che verranno condivisi con gli utenti dovranno riferirsi a quelli preventivamente segnalati dal Titolare tramite i responsabili di area.
All'utente NON dovranno essere fornite risposte con materiali Dell'Ente o informazioni riservate o protette da *copyright* quand'anche ricollegabili alle attività sopracitate.
Gli incaricati dovranno condividere con gli utenti immagini/video o altri contenuti multimediali unicamente quando le persone ritratte non sono riconoscibili oppure hanno espresso il loro consenso in merito a tale comunicazione.

È opportuno, peraltro, sottolineare che l'applicazione di messaggistica rappresenta uno dei canali comunicativi dell'Ente e dunque la sua gestione deve essere improntata al rispetto dei principi di:

- **costante aggiornamento**, affinché le informazioni fornite siano attuali e non riportino contenuti che possano ingenerare confusione nell'utenza;
- **chiarezza e trasparenza**;
- **coerenza dello stile espositivo** delle comunicazioni rispetto a quanto avviene sui canali tradizionali dell'Ente;
- **rispetto, cura e attenzione nei confronti delle esigenze manifestate dall'utenza**;
- **professionalità**, in quanto i contenuti pubblicati rientrano pur sempre all'interno delle attività di un soggetto che agisce nella sua veste di attore istituzionale.
- Stabiliti dalla *"**netiquette**"* presente nella *Policy Esterna*.

Qualora dovessero pervenire messaggi non attinenti al servizio prestato, il personale dovrà invitare l'utente a rivolgersi al soggetto competente ad esaminare la richiesta.

Qualora gli utenti dovessero inviare reclami, segnalazioni o contenuti non appropriati, il personale dovrà confrontarsi con l'Ufficio Amministrativo al fine di convenire sulle modalità di gestione di quanto ricevuto.