Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**

MANUALE OPERATIVO DI ADEGUAMENTO
AL REGOLAMENTO U.E. 679/2016

Il Titolare del trattamento dati adotta il presente documento :

Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**
Sito web	
Attività culturale	**ATTIVITA` CULTURALI, CORSI E ATTIVITA' DI FORMAZIONE E QUALIFICAZIONE PROFESSIONALE SU TUTTO IL TERRITORIO NAZIONALE FINALIZZATI ALLO SCAMBIO E SVILUPPO DI CONOSCENZE SCIENTIFICHE E TECNOLOGICHE NELL'AMBITO DELL'INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.**
Codici ATECO	• **85.52.09 - Altra formazione culturale**
Rappresentante legale	**Bernardo TELLINI**
Codice fiscale	
Contatti	

Report interventi

DATA	**AUDIT**
27/05/2019	CONSEGNA MODULISTICA E MANUALE OPERATIVO

Finalità del documento:
Il presente manuale ha per oggetto l'adeguamento della azienda, descritta in anagrafica e nel corso dello stesso, alle disposizioni relative alla tutela dei dati personali e al loro trattamento, secondo le disposizioni del regolamento U.E. 679/2016.

Contenuto del documento:
Definizioni e principi generali
Guida del Garante alla applicazione del regolamento
Anagrafica Azienda e suo organigramma
Esame dei rischi e degli archivi
Definizioni di carattere generale
Prescrizioni e Istruzioni
Registri dei trattamenti dei dati
Informative e modulistica

Il titolare del trattamento dei dati ATTESTA che il presente manuale, le informative e i registri SONO CONFORMI alle disposizioni di cui al reg. U.E. 679/2016.

Timbro e Firma

Ragione Sociale	SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**

Definizioni
D.lgs 196/2003

Dato personale: è qualunque informazione relativa a un individuo, identificato o identificabile, anche indirettamente.
In un condominio, i dati personali possono essere, ad esempio, il nome e il cognome, il numero di telefono, la mail, l'indirizzo, l'immagine fotografica o un video che ritrae la persona interessata.
Possono esserlo anche altre informazioni quali il numero dell'interno dell'abitazione o la bolletta dei consumi dell'acqua, quando questi sono riconducibili ai singoli condòmini.

Dato identificativo: è il dato personale che permette l'identificazione diretta dell'interessato

Dato sensibile: è qualsiasi informazione che possa rivelare, tra le altre, lo stato di salute e la vita sessuale, ma anche la razza, l'etnia, le convinzioni religiose o politiche di una persona, l'adesione a partiti
o sindacati.

Dato giudiziario: è l'informazione idonea a rivelare provvedimenti in materia di casellari o giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato.

Trattamento dei dati: qualsiasi operazione (raccolta, archiviazione, utilizzo, diffusione, consultazione, aggiornamento, cancellazione) che può essere effettuata utilizzando i dati personali dei vari condomini o di soggetti terzi.

Comunicazione del dato: è l'atto di comunicare dati personali a uno o più soggetti determinati diversi dal diretto interessato, dal responsabile o dall'incaricato del trattamento dei dati.
Nel caso del condominio è la comunicazione di un dato di un condomino o riconducibile anche indirettamente a questo, effettuata ad esempio, ad un fornitore o, laddove non siano stati nominati come incaricati, al portiere oppure non direttamente all'amministratore ma ad un collaboratore di questo.

Diffusione del dato: l'atto di divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti in qualunque forma (ad esempio pubblicandoli su internet), anche mediante la loro messa a disposizione o consultazione.

Titolare del trattamento: è la persona fisica o giuridica o l'organismo al quale spetta decidere le finalità e le modalità del trattamento dei dati personali.

Esercita le potestà decisionali relative all'attività di trattamento e subisce le eventuali sanzioni laddove erogate.
In un condominio, il titolare del trattamento è la compagine condominiale.

Interessato: L'interessato è il soggetto al quale i dati si riferiscono. In ambito condominiale si tratta del proprietario, conduttore e usufruttuario

Responsabile del trattamento dei dati: è la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, compiti di gestione e controllo del trattamento dei dati;
In ambito condominiale tale figura può essere individuata nell'amministratore scelto

dall'assemblea, il quale a sua volta può conferire incarico a soggetti esterni qualificati "Privacy Officer", al fine di adeguarsi alla normativa. Alcuni Privacy Officer o Consulenti Privacy rilasciano l'attestazione di conformità.

Incaricato del trattamento dei dati: sono sempre persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Si tratta normalmente di personale dipendente che, per il ruolo e la posizione che occupa, gestisce alcuni dati personali (es. personale di studio dell'amministratore o personale dipendente del condomino).
Deve essere designato con forma scritta.

Informativa: contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, come circolano i dati e in che modo esercitare i diritti riconosciuti dalla legge.

Consenso: libera manifestazione della volontà con la quale l'interessato accetta un determinato trattamento di dati che lo riguardano, sul quale è stato preventivamente informato (ad esempio dall' amministratore).

Se il trattamento riguarda dati "sensibili" occorre il consenso rilasciato per iscritto dall'interessato, sempre dopo aver ricevuto un'idonea informativa.

Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**

Definizioni
Regolamento UE 2016/679

Dato personale: qualsiasi informazione concernente una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni uniche 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.

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 faccia le o i dati dattiloscopici.

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.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.

Titolare del trattamento: la persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi del trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento.

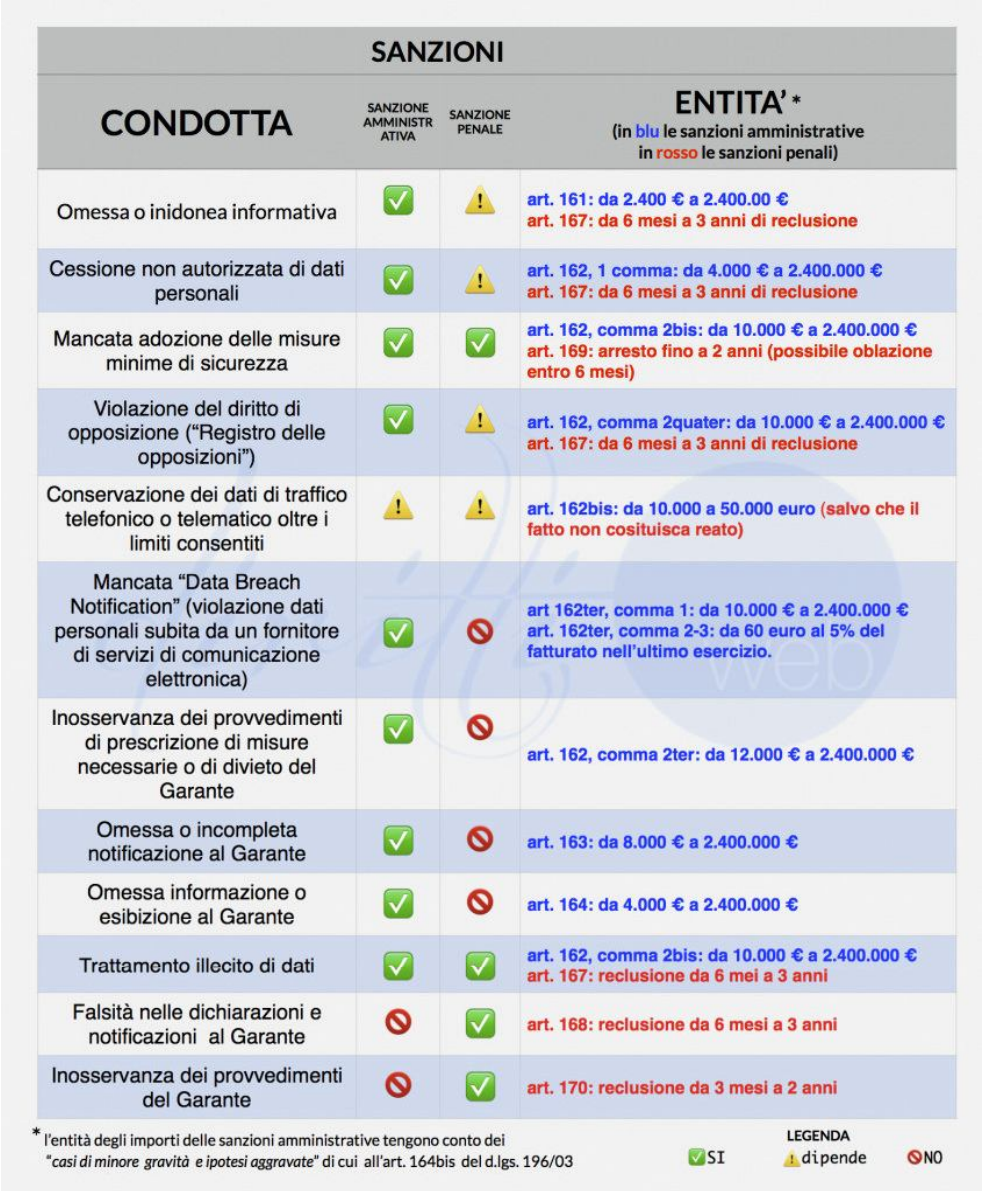
Destinatario: la persona fisica o giuridica, l'autorità pubblica che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**

TABELLA SINOTTICA DI RAFFRONTO TRA IL DLGS 196/03 E IL REGOLAMENTO UE 679/2016

I SOGGETTI	
Titolare; Responsabile Del Trattamento; Incaricato.	Titolare; Responsabile del Trattamento Addetto al Trattamento; Responsabile della Protezione dei Dati.
L'INFORMATIVA	
- Le finalità e le modalità del trattamento; - la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale mancata comunicazione dei dati; - i soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi; - i diritti spettanti agli interessati; - i dati del titolare e l'indicazione di almeno uno dei responsabili eventualmente designati, indicando il sito della rete di comunicazione o di modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili.	- Le finalità e modalità del trattamento e categorie di destinatari; - la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale mancata comunicazione dei dati; - i dati del titolare e del Responsabile della Protezione dei Dati; - l'intenzione del titolare di trasferire i dati ad un Paese terzo; - il periodo di conservazione dei dati o i criteri per determinarlo; - i diritti spettanti agli interessati con specifica indicazione di quello di accesso, rettifica, cancellazione, opposizione, portabilità dei dati trattati; - la possibilità di opporre reclamo presso l'Autorità di controllo; - esistenza di eventuale profilazione.
LE SANZIONI	
- Da art. 161 ad art. 172 del D.lgs. 196/2003.	- Il primo livello sanzionatorio va fino ad un massimo di € 10.000.000 o per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore; - il secondo livello sanzionatorio va fino ad un massimo di € 20.000.000 o per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore.

Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**



SANZIONI

CONDOTTA	SANZIONE AMMINISTRATIVA	SANZIONE PENALE	ENTITA' * (in blu le sanzioni amministrative in rosso le sanzioni penali)
Omessa o inidonea informativa	✅	⚠	art. 161: da 2.400 € a 2.400.00 € art. 167: da 6 mesi a 3 anni di reclusione
Cessione non autorizzata di dati personali	✅	⚠	art. 162, 1 comma: da 4.000 € a 2.400.000 € art. 167: da 6 mesi a 3 anni di reclusione
Mancata adozione delle misure minime di sicurezza	✅	✅	art. 162, comma 2bis: da 10.000 € a 2.400.000 € art. 169: arresto fino a 2 anni (possibile oblazione entro 6 mesi)
Violazione del diritto di opposizione ("Registro delle opposizioni")	✅	⚠	art. 162, comma 2quater: da 10.000 € a 2.400.000 € art. 167: da 6 mesi a 3 anni di reclusione
Conservazione dei dati di traffico telefonico o telematico oltre i limiti consentiti	⚠	⚠	art. 162bis: da 10.000 a 50.000 euro (salvo che il fatto non costituisca reato)
Mancata "Data Breach Notification" (violazione dati personali subita da un fornitore di servizi di comunicazione elettronica)	✅	⛔	art 162ter, comma 1: da 10.000 € a 2.400.000 € art. 162ter, comma 2-3: da 60 euro al 5% del fatturato nell'ultimo esercizio.
Inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto del Garante	✅	⛔	art. 162, comma 2ter: da 12.000 € a 2.400.000 €
Omessa o incompleta notificazione al Garante	✅	⛔	art. 163: da 8.000 € a 2.400.000 €
Omessa informazione o esibizione al Garante	✅	⛔	art. 164: da 4.000 € a 2.400.000 €
Trattamento illecito di dati	✅	✅	art. 162, comma 2bis: da 10.000 € a 2.400.000 € art. 167: reclusione da 6 mei a 3 anni
Falsità nelle dichiarazioni e notificazioni al Garante	⛔	✅	art. 168: reclusione da 6 mesi a 3 anni
Inosservanza dei provvedimenti del Garante	⛔	✅	art. 170: reclusione da 3 mesi a 2 anni

* l'entità degli importi delle sanzioni amministrative tengono conto dei "casi di minore gravità e ipotesi aggravate" di cui all'art. 164bis del d.lgs. 196/03

LEGENDA ✅SI ⚠dipende ⛔NO

Ragione Sociale	SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**

Principi generali

La gestione dei dati personali da parte del condominio deve avvenire nel rispetto della legge, nel senso che deve esser conforme non solo alla disciplina specifica in tema di privacy, ma a tutta la normativa vigente.

I principi con i quali debbono essere trattati e gestiti i dati personali sono i seguenti:

- Principio di liceità-

Il Condominio, e per esso l'amministratore, è tenuto al rispetto della normativa evitando interpretazioni meramente letterali, contrastanti con i principi espressi e affermati "nella "disciplina "sulla protezione dei dati personali.

- Principio di correttezza-

Tutti i dati personali e le modalità del loro trattamento devono essere pertinenti e non eccedenti rispetto alle finalità perseguite.

In ambito condominiale si tratta delle sole informazioni personali pertinenti e necessarie rispetto allo svolgimento delle attività di gestione e amministrazione delle parti comuni e idonee a determinare, secondo le regole del codice civile (artt. 1117 ss. c.c.), le posizioni di dare e avere dei singoli partecipanti siano essi proprietari o usufruttuari, nonché i dati strettamente indispensabili alla convocazione o al funzionamento dell'assemblea.

Il trattamento è lecito soltanto se alla sua base sussiste una ragione che lo giustifica, appunto la finalità (ad es. un rapporto contrattuale). In base al suddetto principio le finalità devono essere determinate, esplicite e legittime e di pertinenza del titolare del trattamento.

-Principio di pertinenza e di non eccedenza-

Il trattamento dei dati dei condomini deve avere finalità esplicite, pertinenti e determinate e deve sempre ricadere al fine di consentire l'applicazione degli artt. 1117 e ss.c.c. e le leggi speciali connesse al funzionamento del sodalizio condominiale

Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	**06211830481**
Codice fiscale	**94126920480**
Sede legale	**Via Giorgio Vasari 4, 00196 Roma - RM**
Contatti	**- Email: IEEE_ITALY@IEEE.ORG**

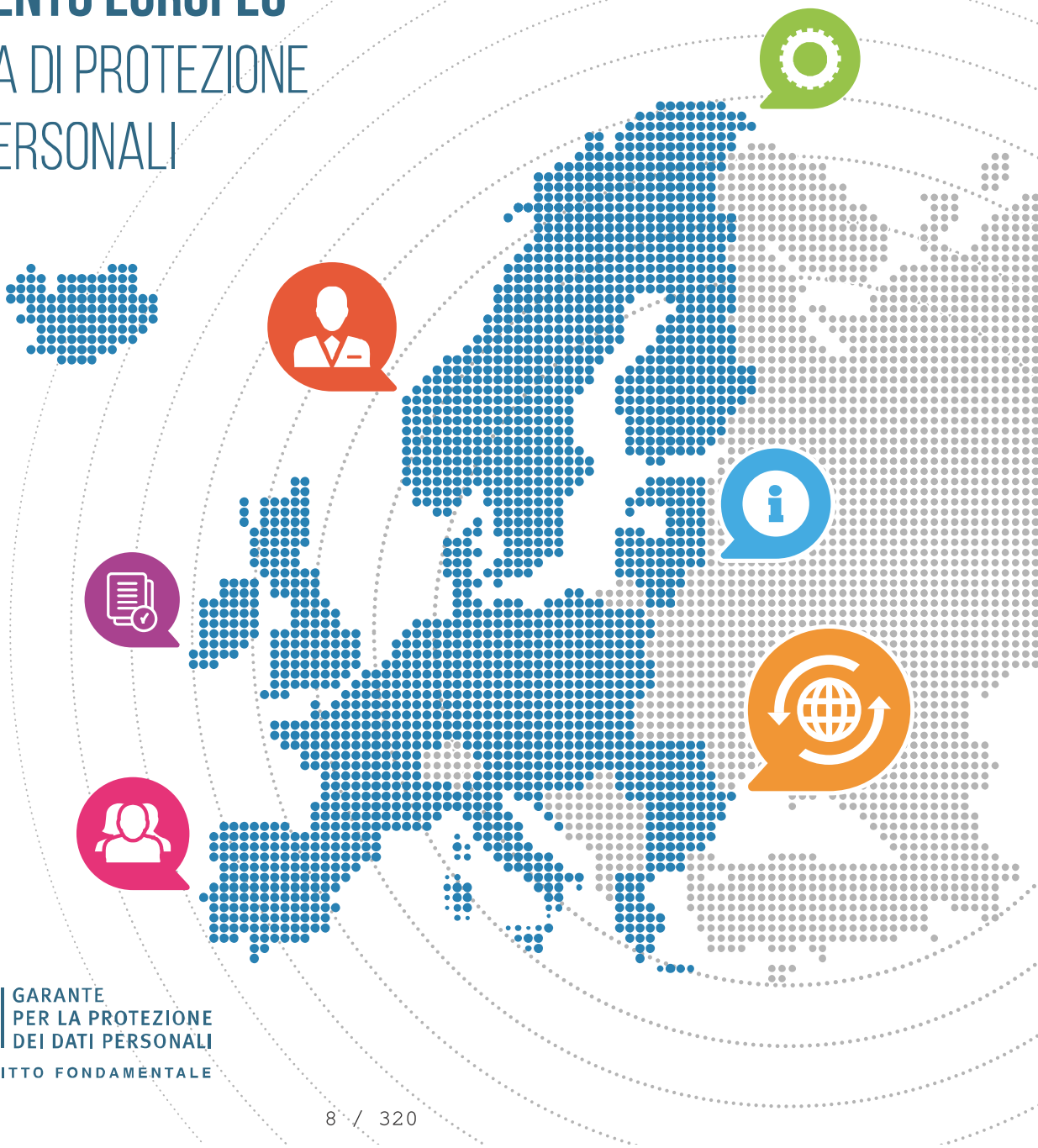
Privacy - principi ed applicabilità

Principio di pertinenza e non eccedenza: L'Amministratore può trattare soltanto le informazioni personali pertinenti e non eccedenti le finalità di gestione e amministrazione delle parti comuni. Es: i dati anagrafici e gli indirizzi dei condòmini (ai fini della convocazione dell'assemblea o per altre comunicazioni), i dati riferiti alle quote millesimali di proprietà, ed eventuali ulteriori dati necessari al calcolo delle spese condominiali.

GUIDA ALL'APPLICAZIONE DEL

REGOLAMENTO EUROPEO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI



1997 2017

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Indice

Fondamenti di liceità del trattamento 4

Informativa 8

Diritti degli interessati 12

Titolare, responsabile, incaricato del trattamento 20

Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili 24

Trasferimenti di dati verso Paesi terzi e organismi internazionali 30

Introduzione

La Guida intende offrire un panorama delle principali problematiche che imprese e soggetti pubblici dovranno tenere presenti in vista della piena applicazione del regolamento, prevista il 25 maggio 2018.

Attraverso raccomandazioni specifiche vengono suggerite alcune azioni che possono essere intraprese sin d'ora perché fondate su disposizioni precise del regolamento che non lasciano spazi a interventi del legislatore nazionale (come invece avviene per altre norme del regolamento, in particolare quelle che disciplinano i trattamenti per finalità di interesse pubblico ovvero in ottemperanza a obblighi di legge).

Vengono, inoltre, segnalate alcune delle principali novità introdotte dal regolamento rispetto alle quali sono suggeriti possibili approcci in modo da arrivare all'appuntamento del 25 maggio 2018 con le idee più chiare.

La presente Guida è soggetta a integrazioni e modifiche alla luce dell'evoluzione della riflessione a livello nazionale ed europeo

Fondamenti di liceità del trattamento

Il regolamento 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 e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003** (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

In particolare:

Consenso

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **deve** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

- **Non** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) **deve** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

- **Il consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

COSA NON CAMBIA

- **Deve** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **non** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).
- **Deve** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Raccomandazioni

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.
In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

COSA CAMBIA

Interesse vitale di un terzo

- Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46).

Interesse legittimo prevalente di un titolare o di un terzo

COSA CAMBIA

- Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **non spetta** all'Autorità ma **è compito dello stesso titolare**; si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto protezione dati.

COSA NON CAMBIA

- L'interesse legittimo del titolare o del terzo deve prevalere 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.

Raccomandazioni

Il regolamento offre alcuni criteri per il bilanciamento in questione (si veda considerando 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (WP217).

Si confermano, inoltre, nella sostanza, i requisiti indicati dall'Autorità nei propri provvedimenti in materia di bilanciamento di interessi (si veda, per esempio, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992 con riguardo ad alcune tipologie di trattamento di dati biometrici; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 con riguardo all'utilizzo della videosorveglianza;http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256 in merito all'utilizzo di sistemi di rilevazione informatica anti-frode; ecc.) con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorità, con eccezione ovviamente delle disposizioni che il regolamento ha espressamente abrogato (per esempio: obbligo di notifica dei trattamenti). I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

Informativa

Contenuti dell'informativa

COSA CAMBIA

- I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **deve sempre** specificare **i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).
- Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.
- Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa

COSA CAMBIA

- Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**non** della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

COSA CAMBIA

- Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
- L'informativa è data, **in linea di principio, per iscritto e preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.
- Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare**

se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

COSA NON CAMBIA

- L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

NOTA: ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Raccomandazioni

È opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018.

Il regolamento supporta chiaramente il concetto di **informativa "stratificata"**, più volte esplicitato dal Garante nei suoi provvedimenti (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/

docweb/1712680 relativo all'utilizzo di un'icona specifica per i sistemi di videosorveglianza con o senza operatore; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675 contenente prescrizioni analoghe rispetto all'utilizzo associato di sistemi biometrici e di videosorveglianza in istituti bancari), in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove **l'utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative.

I titolari potranno, dunque, una volta adeguata l'informativa nei termini sopra indicati, **continuare o iniziare a utilizzare queste modalità** per la prestazione dell' informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione.
Dovranno essere adottate anche le **misure organizzative interne** idonee a garantire il rispetto della tempistica: il termine di 1 mese per l'informativa all'interessato è chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del regolamento menziona in primo luogo che il **termine deve essere "ragionevole"**.

Poiché spetterà al titolare valutare lo **sforzo sproporzionato** richiesto dall'informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del regolamento, sarà utile fare riferimento ai **criteri evidenziati nei provvedimenti** con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione (si veda, in particolare, il provvedimento del 26 novembre 1998 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624; più di recente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423 in tema di esonero dagli obblighi di informativa).

Diritti degli interessati

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

COSA CAMBIA

- **Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese,** estendibile fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego**.

- **Spetta al titolare** valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se così richiede l'interessato** stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa**, **trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

COSA NON CAMBIA

- **Il titolare del trattamento deve agevolare l'esercizio dei diritti** da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo titolare a dover dare riscontro** in caso di esercizio dei diritti (art. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

- **L'esercizio dei diritti è, in linea di principio, gratuito** per l'interessato, ma possono esservi eccezioni (si veda il paragrafo "Cosa cambia"). Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

- Sono ammesse **deroghe ai diritti** riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).
  In questo senso, in via generale, possono continuare a essere applicate **tutte le deroghe previste dall'art. 8, comma 2, del Codice in quanto compatibili** con le disposizioni citate. Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del regolamento.

Raccomandazioni

È opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all'intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso (si vedano varie decisioni relative a ricorsi contenute nel Bollettino dell'Autorità pubblicato qui: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/766652, e più recentemente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1449401 in materia di dati sanitari, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1290018 in materia di dati telematici).

Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, l'Autorità intende valutare l'opportunità di definire linee-guida specifiche (anche sul fondamento delle determinazioni assunte sul punto nel corso degli anni: si veda in particolare la Deliberazione n. 14 del 23 dicembre 2004 - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1104892 , di concerto con le altre autorità Ue, alla luce di quanto prevede l'art. 70 del regolamento con riguardo ai compiti del Board.

Diritto di accesso (art. 15)

COSA CAMBIA

- Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.

- Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Raccomandazioni

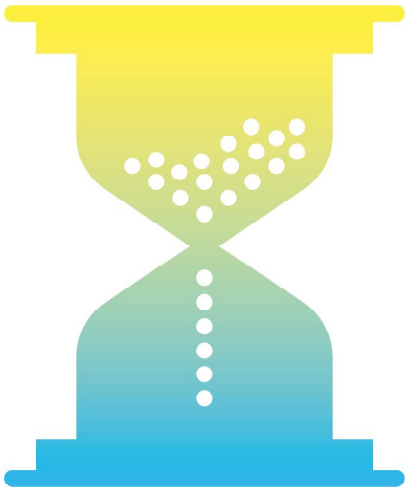
- Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti (si veda "Modalità per l'esercizio dei diritti"), i titolari possono **consentire agli interessati di consultare direttamente, da remoto** e in modo sicuro, i propri dati personali (si veda considerando 68).

Diritto di cancellazione (diritto all'oblio) (art.17)

COSA CAMBIA

- Il diritto cosiddetto "all'oblio" 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).

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



Diritto di limitazione del trattamento (art. 18)

COSA CAMBIA

- 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).

Raccomandazioni

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

Diritto alla portabilità dei dati (art. 20)

COSA CAMBIA

- 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 per maggiori dettagli).

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

Raccomandazioni

Il Gruppo "Articolo 29" ha pubblicato recentemente linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità (http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 con le relative FAQ http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf; versione italiana per adesso disponibile sul sito del Garante: http://www.garanteprivacy.it/garante/document?ID=6058842 con le relative FAQ

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058857).

Al riguardo, si ricordano i numerosi **provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento** fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del Codice (si vedano, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3251012 e, con riguardo all'attività bancaria in generale, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1457247).
Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un **formato interoperabile** secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo "Articolo 29".

Titolare, responsabile, incaricato del trattamento

COSA CAMBIA

Il regolamento:

- disciplina la **contitolarità del trattamento** (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente (rispetto all'art. 29 del Codice) le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti (ex art. 30, paragrafo 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (ex art. 32 regolamento); **la designazione di un RPD-DPO**, nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'Ue dovrà **designare un rappresentante in Italia** quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.

COSA NON CAMBIA

- Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice italiano. Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).

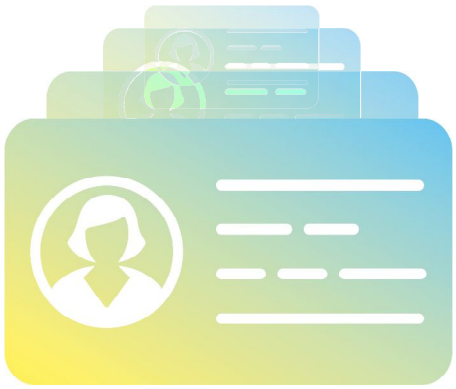
Raccomandazioni

I titolari di trattamento dovrebbero valutare attentamente l'esistenza di eventuali situazioni di contitolarità (si vedano, in proposito, le indicazioni fornite dal Garante in vari provvedimenti, fra cui http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785), essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26, paragrafo 1, del regolamento. Sarà necessario, in particolare, individuare il "punto di contatto per gli interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal regolamento.

I titolari di trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del regolamento. Dovranno essere apportate le necessarie integrazioni o modifiche entro il 25 maggio 2018, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti. La Commissione e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali modello da utilizzare a questo scopo.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4. Il Garante sta valutando i codici deontologici attualmente vigenti per alcune tipologie di trattamento nell'ottica dei requisiti fissati nel regolamento (art. 40), mentre per quanto concerne gli schemi di certificazione occorrerà attendere anche l'intervento del legislatore nazionale che dovrà stabilire alcune modalità di accreditamento dei soggetti certificatori (se diversi dal Garante: si veda art. 43). In ogni caso, il Gruppo "Articolo 29" sta lavorando sui temi e sarà opportuno tenere conto degli sviluppi che interverranno in materia nei prossimi mesi.

Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante (si veda art. 30 del Codice e, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1507921, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1508059 per quanto riguarda la pubblica amministrazione, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953 in materia di tracciamento delle attività bancarie) in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento (si veda art. 24, paragrafo 1, del regolamento).



Approccio basato sul rischio e misure di accountability di titolari e responsabili

COSA CAMBIA

- Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, 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.

- Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** (si veda art. 25), 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) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

- Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento 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); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) 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'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

- Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega **l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano**, come la **notifica preventiva dei trattamenti** all'autorità di controllo e il cosiddetto **prior checking** (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

Si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati recentemente pubblicate dal Gruppo "Articolo 29", disponibili qui: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Nei paragrafi seguenti si richiamano **alcune delle principali novità** in termini di adempimenti da parte di titolari e responsabili del trattamento.

Registro dei trattamenti

COSA CAMBIA

- 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 art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. 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'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Raccomandazioni

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.

I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.
Nello specifico, si richiama l'attenzione sulla sostanziale **coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento**; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.

Misure di sicurezza

COSA CAMBIA

- Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); 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, **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.
Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il

caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Notifica delle violazioni di dati personali

COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – 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). 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 delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento**. Su questo e su tutta la disciplina in materia, il Comitato europeo della protezione dati (si veda art. 70, paragrafo 1, lettere g) e h)) è chiamato a formulare linee-guida specifiche, alle quali sta già lavorando il Gruppo "Articolo 29". Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835) che intende rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il regolamento.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice.
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Responsabile della protezione dei dati

COSA CAMBIA

- Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano art. 38 e 39) in termini che Gruppo "Articolo 29" ha ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubblicazione, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5930287).

Trasferimenti di dati verso Paesi terzi e organismi internazionali

COSA CAMBIA

- In primo luogo, **viene meno il requisito dell'autorizzazione nazionale** (si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice.
  Tuttavia, **l'autorizzazione del Garante sarà ancora necessaria** se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

- Il regolamento consente di ricorrere anche a **codici di condotta ovvero a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che **i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione**, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti.
  Tuttavia (si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2), tali titolari dovranno assumere, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

- Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo**, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda art. 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un **interesse pubblico riconosciuto dal diritto dello Stato membro** del titolare o dal diritto dell'Ue (si veda art. 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

- Il regolamento **fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme**. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del regolamento – ossia, **è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati** (si veda art. 65, paragrafo 1, lettera d)).

COSA NON CAMBIA

- **Il regolamento** (si veda Capo V) **ha confermato l'approccio attualmente vigente** in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

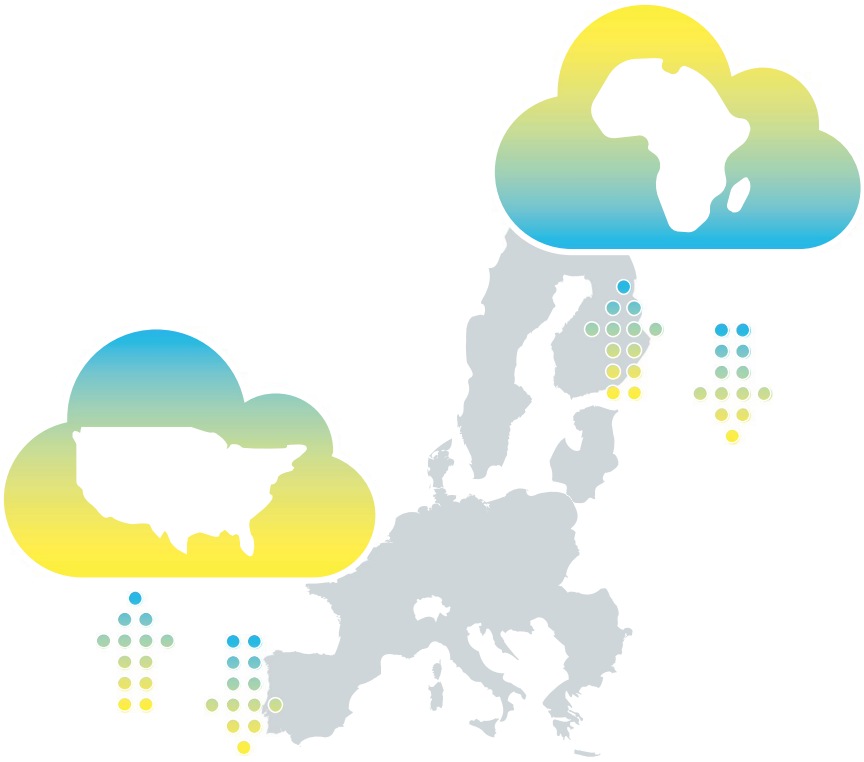
  i. adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (si veda art. 44, comma 1, lettera b), del Codice);

  ii. in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello) (si veda art. 44, comma 1, lettera a) del Codice);

  iii. in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (corrispondenti in parte alle disposizioni dell'art. 43, comma 1, del Codice).

- **Le decisioni di adeguatezza sinora adottate** dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica (si vedano art. 45, paragrafo 9, e art. 96). Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione

(si veda http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1). Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (si veda art. 46, paragrafo 5), sino a loro eventuale modifica.



ANAGRAFICA AZIENDA

Azienda/Organizzazione	**ASSOCIAZIONE SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**

SEDE LEGALE	LEGALE Via Giorgio Vasari 4, 00196 Roma - RM

Data revisione: 20/11/2018

DATI AZIENDA

Ragione Sociale	**SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**
Partita IVA	06211830481
Codice fiscale	94126920480
Sede legale	Via Giorgio Vasari 4, 00196 Roma - RM
Contatti	- Email: IEEE_ITALY@IEEE.ORG
Sito web	
Attività culturale	ATTIVITA` CULTURALI, CORSI E ATTIVITA' DI FORMAZIONE E QUALIFICAZIONE PROFESSIONALE SU TUTTO IL TERRITORIO NAZIONALE FINALIZZATI ALLO SCAMBIO E SVILUPPO DI CONOSCENZE SCIENTIFICHE E TECNOLOGICHE NELL'AMBITO DELL'INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.
Codici ATECO	• 85.52.09 - Altra formazione culturale
Rappresentante legale	Bernardo TELLINI
Codice fiscale	
Contatti	

SEDI

Nome	**LEGALE**
Tipo	- Legale - Amministrativa - Operativa
Indirizzo	Via Giorgio Vasari 4, 00196 Roma - RM

NOMINE

Soggetto	**DIPENDENTE PERSONALE (non presente)**
Contatti	
Nomina	**Persona autorizzata** Sede: LEGALE

Soggetto	**SEVERINI ALESSANDRO**
Contatti	
Nomina	**Responsabile del trattamento esterno** Sede: LEGALE

Soggetto	**TELLINI BERNARDO**
Contatti	
Nomina	**Titolare del trattamento** Sede: LEGALE

PARTNERS

Nominativo	**SEVERINI ALESSANDRO**
Tipo Partner	Partner/fornitore
Partita IVA	
Codice fiscale	
Indirizzo residenza	' -
Contatti	

ARCHIVI INFORMATICI

Nome	**ARCHIVIO DI SEDE**
Tipo Struttura	Interna
Sede	LEGALE (Roma)
Personale con diritti di accesso	TELLINI BERNARDO RAPUANO SERGIO MASSUCCO STEFANO ZIZZO GAETANO FERRARI STEFANO
Note	Cloud Platform PROTETTO DA USER NAME E PASSWORD.
Software utilizzati	- GESTIONALE PROPRIO

ORGANIGRAMMA GDPR

Azienda/Organizzazione	**ASSOCIAZIONE SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**

SEDE LEGALE	LEGALE Via Giorgio Vasari 4, 00196 Roma - RM

Data revisione: 20/11/2018

Di seguito, è riportato l'organigramma con le funzioni nominate per la gestione della protezione del trattamento dati personali:

SEDE LEGALE

Titolare del trattamento:	**TELLINI BERNARDO**	Data nomina: 21/01/2019

Responsabili esterni del trattamento:	**SEVERINI ALESSANDRO**	Data nomina: 25/05/2018

Persone autorizzate:	**TELLINI BERNARDO**	Data nomina: 21/01/2019
	MASSUCCO STEFANO	Data nomina: 21/01/2019
	RAPUANO SERGIO	Data nomina: 21/01/2019
	ZIZZO GAETANO	Data nomina: 21/01/2019
	FERRARI STEFANO	Data nomina: 21/01/2019

VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione	**ASSOCIAZIONE SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**

SEDE LEGALE	LEGALE Via Giorgio Vasari 4, 00196 Roma - RM

Data revisione: 20/11/2018

VALUTAZIONE ARCHIVI INFORMATICI

Di seguito, è riportata la valutazione degli archivi informatici in dotazione all'organizzazione.
L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

RISULTATI

Nome	ARCHIVIO DI SEDE
Tipo Struttura	Interna
Sede	LEGALE (Roma)
Personale con diritti di accesso	BERNARDO TELLINI RAPUANO SERGIO MASSUCCO STEFANO ZIZZO GAETANO FERRARI STEFANO
Note	Cloud Platform PROTETTO DA USER NAME E PASSWORD.
Software utilizzati	• GESTIONALE PROPRIO

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Trascurabili	Accettabile

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Trascurabili	Accettabile

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Trascurabili	Accettabile

PERICOLO
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)

RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Trascurabili	Accettabile

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Trascurabili	Accettabile

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Improbabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• - Viene eseguita opportuna manutenzione. - Sono gestiti i back up - I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili - Sono utilizzati software antivirus e anti intrusione. - Sono definiti i ruoli e le responsabilità. - Esistono procedure per l'individuazione del custode delle password. - E' presenta una politica per la sicurezza e la protezione dei dati. - L'impianto elettrico è certificato ed a norma. - Sono stabiliti programmi di formazione e sensibilizzazione. - Studio protetto da porta blindata - Impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi. - I software utilizzati sono protetti da password • Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati • E' applicata una gestione della password degli utenti • Studio protetto da porta blindata • Sono utilizzati software antivirus e anti intrusione

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

Premessa
1. Utilizzo del Personal Computer
2. Utilizzo della rete
3. Gestione delle Password
4. Utilizzo dei supporti magnetici
5. Utilizzo di PC portatili
6. Uso della posta elettronica
7. Uso della rete Internet e dei relativi servizi
8. Osservanza delle disposizioni in materia di Privacy.
9. Non osservanza della normativa aziendale.
10. Aggiornamento e revisione

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.
Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* della Associazione IEEE.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali.*
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *Responsabile dei sistemi informatici aziendali.*
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento).*

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

Regole per la gestione delle password

- Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale. User-id e password iniziali sono assegnati, dal custode delle password.
- User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti. La User-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome. La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso

al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

- Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
- Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
- Le password di amministratore di tutti i PC che lo prevedono sono assegnate dallo amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
- In caso di manutenzione straordinaria possono essere comunicate, qualora necessario,
- dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le

credenziali di autenticazione di servizio.
Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo; per la definizione/gestione della password devono essere rispettate le seguenti regole:

- la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve contenere lo user-id come parte della password;
- al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
- la nuova password non deve essere simile alla password precedente;
- la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei mesi di inattività;
- la password è segreta e non deve essere comunicata ad altri;
- la password va custodita con diligenza e riservatezza;
- l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia

UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per . **SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS** . deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, ...).
Per la trasmissione di file all'interno di . **SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS** .è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Le presenti prescrizioni disciplinano le modalità di accesso e di uso della rete informatica etelematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

La struttura promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione. Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore.
E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema.

L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer.
Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

Minacce

Minacce a cui sono sottoposte le risorse hardware
Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

Minacce a cui sono sottoposte le risorse connesse in rete
Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:

- all'utilizzo della LAN/Intranet (interne);
- ai punti di contatto con il mondo esterno attraverso Internet (esterne);
- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

Elenco delle minacce

IP spoofing - L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
Packet sniffing - Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.
Port scanning - Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.
Highjacking - Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.
Social engineering - Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.
Buffer overflow - Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;
Spamming - Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.
Password cracking - Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.
Trojan - Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.
Worm - Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano

le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).
Logic bomb - Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.
Malware e MMC (Malicious Mobile Code) - Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.
DOS (Denial of Service) - Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.
DDOS (Distributed Denial of Service) - Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete.
L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti esterne a quella della rete locale LAN. La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

Minacce a cui sono sottoposti i supporti di memorizzazione
Le principali minacce ai supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- attivazione di un sistema di backup con periodicità giornaliera.
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows , di seguito specificate;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per
- controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza giornaliera e la scansione periodica dei supporti di memoria

Regole per la gestione di strumenti elettronico/informatico

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;

- le copie di backup realizzate sono conservate in armadio chiuso a chiave, nell'ufficio amministrativo;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile,

lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screen-saver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi

che supportano la multiutenza;

- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti

file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;

- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la

provenienza, ovvero divieto di “scaricare“ dalla rete internet ogni sorta di file,
eseguibile e non. La decisione di “scaricare” può essere presa solo dal responsabile del trattamento;

- disattivare gli ActiveX e il download dei file per gli utenti del browser Internet

Explorer;

- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il

livello di protezione su “chiedi conferma” (il browser avvisa quando uno script cerca
di eseguire qualche azione);

- attivare la protezione massima per gli utenti del programma di posta Outlook Express
- al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è

visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);

- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso

analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");

- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema

operativo e applicare le patch di sicurezza consigliate;

- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema

operativo, o forniti direttamente dal costruttore del PC);

- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di

backup consentita per legge;

- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk,definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

Incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

- evitare danni diretti alle persone;
- proteggere l'informazione sensibile o proprietaria;
- evitare danni economici;
- limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

- isolare l'area contenente il sistema oggetto dell'incidente;
- isolare il sistema compromesso dalla rete;
- spegnere correttamente il sistema oggetto dell'incidente.
- Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
- documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide. Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

- Eseguire una copia bit to bit degli hard disk del sistema compromesso;
- Se l'incidente riguarda i dati il restore dei dati può avvenire sulla precedente a partire dalle ultime copie di backup ritenute valide;

DIVIETI

E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;

- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare
- operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete,

- programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. Virus,

cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico percontrollare le attività degli utenti, leggere copiare o cancellare file e software di altriutenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

Attività consentite

E' consentito all'amministratore di sistema:
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico percontrollare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, percopiare o rimuovere file e software, solo se rientrante nelle normali attività dimanutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password ;
- rimuovere programmi software, solo se rientrante nelle normali attività dimanutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

ISTRUZIONI OPERATIVE VIDEOSORVEGLIANZA

INDICE

Premessa
1. Definizioni
2. Principi generali
3. Diritti degli interessati
4. Adempimenti applicabili a soggetti pubblici e privati
5. Verifica preliminare
6. Misure di sicurezza
7. Responsabili e incaricati
8. Durata della conservazione dati
9. Soggetti pubblici
10. Soggetti privati
11. Osservanza delle disposizioni in materia di Privacy
12. Non osservanza della normativa aziendale
13. Aggiornamento e revisione

PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali, volte a garantire l'incolumità pubblica e la sicurezza urbana.

L'Azienda SEZIONE ITALIA DELLA IEEE ASSOCIAZIONE ha adottato una procedura interna per il trattamento dei dati personali acquisiti mediante l'uso di sistemi di videosorveglianza, che rispetta i principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e dalla normativa nazionale in vigore.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, si definisce:

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

2. PRINCIPI GENERALI

La videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad

accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
2) protezione della proprietà;
3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
4) acquisizione di prove.
La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati. Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.
L'attività di videosorveglianza dev'essere effettuata nel rispetto del principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite.

3. DIRITTI DEGLI INTERESSATI
Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al regolamento, in particolare il diritto di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.
Dev'essere assicurato il "diritto all'oblio", ovvero il diritto di ogni singolo individuo a richiedere la cancellazione dei propri dati personali. Vi è, infatti, l'obbligo di cancellazione da parte del titolare del trattamento se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori" (articolo 17 Regolamento 2016/679 e normativa nazionale in vigore).

4. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI
Secondo quanto afferma il Garante per la Privacy, un sistema di videosorveglianza è a norma quando rispetta i principi di liceità, necessità, proporzionalità e finalità. Attraverso il sistema di videosorveglianza è consentita:
- la registrazione delle immagini se necessarie ad obblighi di legge o per tutelare un interesse legittimo (liceità);
- le riprese devono limitarsi solamente a ciò che è necessario per raggiungere gli scopi prefissati (necessità);
- l'impianto va impiegato solo in luoghi dove è realmente necessario, limitando le riprese alle sole aree interessate ed escludendo la visuale su quelle circostanti (proporzionalità);
- lo scopo della videosorveglianza deve essere esplicito e legittimo nonché limitato alle finalità di pertinenza dei titolari dei dati (finalità).

Il principio generale in materia stabilisce che chiunque installi un sistema di videosorveglianza deve provvedere a segnalarne la presenza, facendo in modo che qualunque soggetto si avvicini all'area interessata dalle riprese sia avvisato della presenza di telecamere già prima di entrare nel loro raggio di azione.

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.
Il supporto con l'informativa:
• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata, poi rinvii a un testo completo contenente tutti gli elementi, accessibile anche con strumenti informatici e telematici.
Il Titolare del trattamento ha l'obbligo di effettuare la valutazione dell'impatto sulla protezione dei dati personali (DPIA), nel caso in cui la sorveglianza è sistematica su larga scala di una zona accessibile al pubblico (articolo 35 Regolamento 2016/679 e normativa nazionale in vigore).

5. VERIFICA PRELIMINARE
Le riprese effettuate per fini di sicurezza e tutela dell'ordine pubblico, con particolare riferimento alla prevenzione di reati o atti di vandalismo e alla sicurezza sul lavoro, costituiscono un'eccezione, e non necessitano dell'obbligo di segnalazione.
Normalmente, per installare un sistema di videosorveglianza, non è necessario l'assenso da parte del Garante della privacy; fanno però eccezione tutti i casi in cui sussiste il rischio di ledere i diritti e le libertà fondamentali o la dignità degli individui ripresi.
Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.
Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso.
La conservazione delle immagini deve avere una durata prestabilita e non eccedente le 24 ore; in situazioni particolari, nelle quali sussiste un elevato fattore di rischio, la durata massima si estende ad una settimana. Nel caso si necessita di una conservazione dei dati più lunga sarà invece necessaria la verifica preliminare del Garante.
Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

Esclusione della verifica preliminare
Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:
a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;
b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti.
Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso.
È regola generale che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.
Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza, deve essere preventivamente notificato a questa Autorità.

6. MISURE DI SICUREZZA

Il titolare del trattamento dei dati ha l'obbligo di prendere le misure di sicurezza minime onde evitare la distruzione, la perdita, l'accesso abusivo alle immagini, nonché il loro utilizzo per scopi incoerenti con le finalità previste.
In particolare, i dati raccolti mediante sistemi di videosorveglianza, devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).
È inevitabile che, in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati, le misure minime di sicurezza possano variare anche significativamente.

È tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:
a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini, devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;
f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

7. RESPONSABILI E INCARICATI

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini. Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento.

8. DURATA DELLA CONSERVAZIONE DATI

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario.

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario a raggiungere la finalità perseguita.

Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento deve stabilire un termine per la cancellazione o per la verifica periodica.

Generalmente la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che si ritiene non debba comunque superare la settimana.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del GARANTE, e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

9. SOGGETTI PUBBLICI

I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati.

Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di

videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa che:
• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria. Al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.
Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.
In ogni caso, si ribadisce l'auspicio che, l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.
Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti.
Avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e da enti territoriali
Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.
Questa Autorità ha già individuato un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale.
In particolare:
a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;
b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e

rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.
Il titolare del trattamento è tenuto a richiedere una verifica preliminare all'Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

10. SOGGETTI PRIVATI

L'installazione di sistemi di videosorveglianza viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Regolamento GDPR non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l'adozione di cautele a tutela dei terzi. In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all'interno di condomini e loro pertinenze (quali posti auto e *box*).
Benché non trovi applicazione la disciplina del Regolamento GDPR, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l'angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l'accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l'abitazione di altri condomini.

11. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

12. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

13. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

Rappresentante Legale

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per **"Violazione di dati**" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.

- **Rischio elevato**: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

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

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

Premessa
1. Definizioni
2. Adempimenti
3. Modalità di svolgimento delle operazioni
4. Istruzioni per l'uso degli strumenti informatici
5. Gestione strumenti elettronici (pc fissi e portatili)
6. Gestione username e password
7. Installazione di hardware e software
8. Gestione posta elettronica aziendale
9. Gestione del salvataggio dei dati
10. Gestione dei supporti rimovibili
11. Gestione protezione dai virus informatici
12. Istruzioni per l'uso degli strumenti "non elettronici"
13. distruzione delle copie cartacee
14. Misure di sicurezza
15. Prescrizioni per gli incaricati

1 Addetti alla manutenzione

2 Osservanza delle disposizioni in materia di Privacy.
3 Non osservanza della normativa aziendale.
4 Aggiornamento e revisione

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Associazione SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERING, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Azienda.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo

come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 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;
- 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.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:
- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:
- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Azienda di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

4. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a) Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.
Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:
• prima della riconsegna, rimuovere eventuali file ivi elaborati;
• quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
• tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.
Ciascun incaricato deve scegliere le password in base ai seguenti criteri:
• devono essere lunghe almeno otto caratteri;
• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
• non deve essere uguali alle precedenti.
Per la corretta gestione della password è necessario:
• Almeno ogni 3 mesi è obbligatorio cambiare la password;
• Ogni password ricevuta va modificata al primo utilizzo;
• La password venga conservata in un luogo sicuro;
• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
• Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.
Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

d) Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza della Associazione e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:
• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
• l'indirizzo del destinatario sia stato correttamente digitato,
• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

e) Gestione del salvataggio dei dati

• Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

• Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

f) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD

riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

5. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

h) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

i) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;

• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

j) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:
• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
• i supporti devono essere archiviati in ambiente ad accesso controllato;
• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

6. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta

elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

8. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

9. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Data

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

A seguito del recepimento della direttiva 2009/136/Ce ad opera del decreto legislativo 28 maggio 2012, n. 69, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante e, in alcuni casi, al contraente o ad altre persone interessate, le violazioni dei dati personali (Data breach) che detengono nell'ambito delle proprie strutture.

Titolare che effettua la comunicazione

Denominazione o ragione sociale: ……

Provincia……Comune……

Cap. …… Indirizzo ……

Nome persona fisica addetta alla comunicazione……

Cognome persona fisica addetta alla comunicazione……

Funzione rivestita……

Indirizzo Email/PEC per eventuali comunicazioni……

Recapito telefonico per eventuali comunicazioni……

Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

☐ Nuova comunicazione

☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

☐ Ritiro precedente comunicazione

Breve descrizione del trattamento di dati personali

Quando si è verificata la violazione di dati personali?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

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)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati personali?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono coinvolti nella violazione ?

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

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

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?

Quale canale è utilizzato per la comunicazione ai contraenti (o alle persone interessate)?

Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione coinvolge contraenti (o altre figure interessate) che si trovano in altri Paesi UE?

☐ Sì

☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

☐ No

☐ Sì

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: **databreach.pa@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

Denominazione o ragione sociale:

……

Provincia……**Comune**……

Cap. …… **Indirizzo** ……

Nome persona fisica addetta alla comunicazione……

Cognome persona fisica addetta alla comunicazione……

Funzione rivestita……

Indirizzo Email/PEC per eventuali comunicazioni……

Recapito telefonico per eventuali comunicazioni……

Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

☐ Nuova comunicazione

☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

☐ Ritiro precedente comunicazione

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione di dati personali?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

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)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati personali?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono coinvolti nella violazione?

☐ Dati anagrafici/codice fiscale

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

☐ Dati relativi a minori

☐ 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

☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale

☐ Dati giudiziari

☐ Copia per immagine su supporto informatico di documenti analogici

☐ Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?

Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 4 giugno 2015 "*Linee guida in materia di dossier sanitario*"**, i titolari di trattamento dei dati personali effettuati mediante il *dossier* sanitario sono tenuti a comunicare al Garante all'indirizzo: **databreach.dossier@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle proprie strutture (*cfr. punto 7.1. delle predette Linee guida*).

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Titolare del trattamento del dossier sanitario

Denominazione o ragione sociale: ……

Provincia……Comune……

Cap. …… Indirizzo ……

Nome persona fisica addetta alla comunicazione……

Cognome persona fisica addetta alla comunicazione……

Funzione rivestita……

Indirizzo PEC e/o EMAIL per eventuali comunicazioni……

Recapito telefonico per eventuali comunicazioni……

Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

……

……

……

Breve descrizione della violazione dei dati personali trattati mediante il *dossier* sanitario

Quando si è verificata la violazione dei dati personali trattati mediante il *dossier* sanitario?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

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)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Computer

☐ Rete

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Documento cartaceo

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati mediante il *dossier* sanitario?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici

☐ Indirizzo di posta elettronica

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

☐ Dati idonei a rivelare lo stato di salute

☐ Dati relativi a minori

☐ Dati sanitari relativi a persone sieropositive, a donne che si sono sottoposte a un'interruzione volontaria di gravidanza, a vittime di atti di violenza sessuale o di pedofilia, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, a donne che hanno deciso di partorire in anonimato, i dati riferiti ai servizi offerti dai consultori familiari

☐ Copie per immagine su supporto informatico di documenti analogici

☐ Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati personali trattati mediante il *dossier* sanitario (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

VIOLAZIONE DI DATI BIOMETRICI

MODELLO DI COMUNICAZIONE AL GARANTE

A seguito del Provvedimento del 12 novembre 2014, i titolari di trattamento di dati biometrici sono tenuti a comunicare al Garante le violazioni di tali dati (*data breach*) che si verificano nell'ambito dei propri sistemi.

La comunicazione deve essere effettuata in base al presente modello, allegando eventualmente ulteriore documentazione ritenuta utile.

Titolare del trattamento di dati biometrici

Denominazione o ragione sociale: ……

Provincia……Comune……

Cap. …… Indirizzo ……

Nome persona fisica addetta alla comunicazione……

Cognome persona fisica addetta alla comunicazione……

Funzione rivestita……

Indirizzo Email/PEC per eventuali comunicazioni……

Recapito telefonico per eventuali comunicazioni……

Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

☐ Nuova comunicazione

☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

Breve descrizione del trattamento di dati biometrici (finalità, caratteristiche biometriche utilizzate…)

Breve descrizione della violazione di dati biometrici

Quando si è verificata la violazione di dati biometrici?

☐ Il……

☐ Tra il…… e il ……

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

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)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati biometrici?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Altri dati coinvolti nella violazione

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

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

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

La violazione coinvolge interessati che si trovano in altri Paesi UE?

☐ Sì

☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

☐ No

☐ Sì

All’attenzione di
(indicare il titolare del trattamento)

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….
nato/a a……il……, esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

- ☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
- ☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell’art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

1 le finalità del trattamento;

2 le categorie di dati personali trattate;

3 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;

4 il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

5 l’origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);

6 l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);

cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a)…;

b)….;

c)…;

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

contesta l'esattezza dei dati personali;

il trattamento dei dati è illecito;

i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

3.Portabilità dei dati

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: .....):*

tutti i dati personali forniti al titolare;

un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____

_____

_____

_____

_____

_____

_____

5. Opposizione al trattamento per fini di marketing diretto

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta:

Via/Piazza
Comune Provincia Codice postale

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

(Luogo e data)

(Firma)

IEEE – SEDE PER L'ITALIA
INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI
(ART. 13 e 14 DEL REG. U.E. 679 / 2016)

I dati personali dell'utente sono utilizzati da SEZIONE ITALIA DELLA IEEE ASSOCIAZIONE, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1) La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:
   - Mista - elettronica e cartacea

   con le seguenti finalità:
   - Corsi e attività di formazione
   - Gestione e amministrazione della associazione e attività connesse

Consenso al trattamento di dati particolari:

☐ accetto ☐ non accetto

I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto associativo e istituzionale in essere.

La informiamo altresì che durante le attività potrebbero essere realizzate delle riprese audio video o dei rilievi fotografici che saranno utilizzate esclusivamente per finalità promozionale e divulgative anche mediante pubblicazione sui portali istituzionale e sui canali social istituzionali di IEE-ITALY SECTION.
Per partecipare all'evento è richiesto il consenso all'uso delle riprese audio/video per le finalità sopra descritte. In accordo con la politica degli eventi IEEE, che impone alcune restrizioni sull'uso di contenuti multimediali durante i suoi eventi, un partecipante è autorizzato a utilizzare fotocamere portatili e/o smartphone per scattare fotografie e acquisire immagini digitali per uso personale e non commerciale, a condizione di non determinare interruzioni.
Le fotografie non possono essere pubblicate, vendute, riprodotte, trasmesse, distribuite o altrimenti sfruttate commercialmente in alcun modo. La Sezione IEEE Italia declina ogni responsabilità per l'acquisizione della vostra immagine in qualsiasi formato multimediale da parte di altri partecipanti all'evento.

BASE GIURIDICA

2) Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti. L'associazione tratta i dati facoltativi degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di interessati: Consulenti e liberi professionisti anche in forma associata - Imprese e Ordini Professionali - Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le seguenti categorie di persone autorizzate e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati: responsabili dell'organizzazione degli eventi; Bernardo TELLINI - Rappresentante legale; Stefano MASSUCCO – Vice-Presidente; Sergio RAPUANO - Tesoriere; Gaetano ZIZZO - Segretario; Stefano FERRARI - Gestore dati informatici.

TRASFERIMENTO DATI PERSONALI PRESSO PAESI TERZI

Denominazione attività	Paese
Attività di formazione della associazione e gestione degli iscritti	Stati Uniti

STRUTTURE INFORMATICHE

IEEE – SEDE PER L'ITALIA
INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI
(ART. 13 e 14 DEL REG. U.E. 679 / 2016)

Denominazione attività	**Attività di formazione della associazione e gestione degli iscritti**
Strutture informatiche	ARCHIVIO DI SEDE
Tipo Struttura	Interna
Sede	LEGALE (Roma)

PRINCIPI SUL TRATTAMENTO DEI DATI
(ARTT. 6 E SEGUENTI DEL REG.U.E. 679/2016)

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, 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»);

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, 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»).

2. Il titolare del trattamento è competente per il rispetto dei suddetti e in grado di comprovarlo («responsabilizzazione»).

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) 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;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) 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;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, quando è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
La base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX del regolamento
. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 del regolamento , al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del regolamento;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

Il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.
1. 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.

Quanto sopra non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto ;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai

sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) 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;

h) 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, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h) del regolamento , se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

PERIODO DI CONSERVAZIONE

3) I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento del rapporto commerciale e contabile.
I dati di chi non acquista o usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con dei rappresentanti dell'associazione, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di promozione commerciale o ricerca di mercato.
Il periodo di conservazione dei dati è: ANNI CINQUE

DIRITTI DELL'INTERESSATO

4) Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:

- richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso);

- conoscerne l'origine;
- riceverne comunicazione intelligibile;
- avere informazioni circa la logica, le modalità e le finalità del trattamento;
- richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti;
- nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
- il diritto di presentare un reclamo all'Autorità di controllo.

Come e quando l'Interessato può opporsi al trattamento dei propri dati personali? (Art. 21 GDPR) .

Per motivi relativi alla situazione particolare dell'Interessato, lo stesso può opporsi in ogni momento al trattamento dei propri dati personali se esso è fondato sul legittimo interesse o se avviene per attività di promozione commerciale, inviando la richiesta al Titolare all'indirizzo comunicato al momento del perfezionamento del rapporto su cui si basa il trattamento stesso.

L'Interessato ha diritto alla cancellazione dei propri dati personali se non esiste un motivo legittimo prevalente del Titolare rispetto a quello che ha dato origine alla richiesta, e comunque nel caso in cui l'Interessato si sia opposto al trattamento per attività di promozione commerciale.

A chi può proporre reclamo l'Interessato? (Art. 15 GDPR)

Fatta salva ogni altra azione in sede amministrativa o giudiziale, l'Interessato può presentare un reclamo all'autorità di controllo competente sul territorio Italiano (Autorità Garante per la protezione dei dati personali) ovvero a quella che svolge i suoi compiti ed esercita i suoi poteri nello Stato membro dove è avvenuta la violazione del GDPR.

Titolare del trattamento dei Suoi dati personali è SEZIONE ITALIA DELLA IEEE
p.iva 06211830481, c.f. 94126920480
Email: IEEE_ITALY@IEEE.ORG
Responsabile : BERNARDO TELLINI

****

Il/I sottoscritto/i (1) in calce identificato/i dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 ed esprime il consenso al trattamento ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.
L'eventuale rifiuto nel consentire il trattamento dei dati potrebbe comportare l'impossibilità di usufruire del servizio richiesto dall'utente.

Data _____ Firma _____

_____
Consenso al trattamento dei dati particolari

[ ] Accetto [ ] Non Accetto

IEEE ITALY SECTION
PRIVACY POLICY

The personal data of the user are used by IEEE ITALY SECTION, which is the holder for the treatment, in compliance with the principles of protection of personal data established by the GDPR 2016/679 Regulation.

MODALITIES AND PURPOSES OF DATA PROCESSING

1) We inform you that the data will be processed with the support of the following means:

- Mixed - electronic and paper

with the following purposes:

- Courses and training activities
- Management and administration of the association and related activities

The data will be kept for the time necessary to achieve the purpose for which they were collected.

We also inform you that the activities could be subject to audio/video capturing in order to document and display the event experience. This material can be used for promotional and dissemination purposes, also through publication on the institutional portals and on the IEEE ITALY SECTION institutional social channels.
By attending the event, you acknowledge to the use of the audio-video footage for the above mentioned purposes.
In agreement with the IEEE events policy, which imposes certain restrictions on the use of multimedia at its events, an attendee is permitted to use hand-held cameras and/or smart phones to take photographs and capture digital images for personal, non-commercial use, provided the photography is not disruptive. Photographs may not be published, sold, reproduced, transmitted, distributed or otherwise commercially exploited in any manner whatsoever.
IEEE Italy Section disclaims all liability for the capture of your image in any multimedia format by other attendees at the event.

LEGAL BASIS

2) The provision of data is mandatory for all that is required by legal and contractual obligations and therefore any refusal to supply them in whole or in part may give rise to the impossibility of providing the services requested. The association deals with the users' optional data on the basis of their consent, that is through the explicit approval of this privacy policy and in relation to the methods and purposes described below.

CATEGORIES OF RECIPIENTS

Without prejudice to the communications carried out in compliance with legal

and contractual obligations, all data collected and processed may be communicated exclusively for the purposes specified above to the following categories of stakeholders: Consultants and freelancers also in partnership; Businesses and Professional Associations.
Furthermore, the following categories of authorized persons and/or internal and external managers identified in writing and to whom specific written instructions have been provided regarding the processing of data can be involved in the processing of your data: responsible for organizing the events ; Legal representative; Treasurer; Secretary; Information Management Coordinator.

TRANSFER PERSONAL DATA TO THIRD COUNTRIES

Activity description	**Country**
IEEE training activities and management of membership	United States

INFORMATION STRUCTURES

Activity description	IEEE training activities and management of membership
IT structures	Office archive
Structure type	Internal
Registered office	Rome

CONSERVATION PERIOD

3) The mandatory data for contractual and accounting purposes are kept for the time necessary to carry out the commercial and accounting relationship.
The data of those who do not buy or use products / services, even if they have had a previous contact with representatives of the association, will be immediately canceled or processed anonymously, where their conservation is not otherwise justified, unless it has been validly acquired the informed consent of the interested parties regarding a subsequent commercial promotion or market research activity.

The data retention period is: Five years.

RIGHTS OF THE DATA SUBJECT

According to European Regulation 679/2016 (GDPR) and national legislation, the interested party may, in accordance with the procedures and within the limits established by current legislation, exercise the following rights:

- Request confirmation of the existence of personal data concerning him / her (right of access);
- Know its origin;
- Receive intelligible communication;
- To have information about the logic, the methods and the purposes of the processing;
- Request the updating, correction, integration, cancellation, transformation into anonymous form, blocking of data processed in violation of the law, including those no longer necessary for the pursuit of the purposes for which they were collected;
- In cases of consent-based processing, receive their data provided to the holder, in a structured and readable form by a data processor and in a format commonly used by an electronic device;
- The right to lodge a complaint with the Control Authority.

How and when can the data subject oppose the processing of personal data? (Article 21 GDPR).

For reasons relating to the particular situation of the interested party, the same may oppose at any time the processing of their personal data if it is based on legitimate interest or if it takes place for business promotion, by sending the request to the Owner at the time communicated the improvement of the relationship on which the treatment itself is based.

The interested party has the right to cancel his/her personal data if there is no legitimate overriding reason for the Data Controller than the one giving rise to the request, and in any case in case the Data Subject opposes the processing for commercial promotion activities.

To whom can the interested party submit a complaint? (Article 15 GDPR)

Without prejudice to any other action in administrative or judicial proceedings, the interested party may lodge a complaint with the competent supervisory authority on the Italian territory (Authority for the protection of personal data) or the one carrying out its duties and exercising its powers in the Member State where the GDPR violation took place.

The data controller of your personal data is:
IEEE ITALY SECTION
p.iva 06211830481, c.f. 94126920480
mail: IEEE_ITALY@IEEE.ORG
Legal representative: IEEE Italy Section Chair

****

MODELLO COMUNICAZIONE AL GARANTE DEI DATI DELL'RPD AI SENSI DELL'ART. 37, PAR. 1, LETT. *A*) E PAR. 7, DEL RGPD

DATI DEL TITOLARE/RESPONSABILE DEL TRATTAMENTO

Denominazione ente: SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

Codice Fiscale /P.Iva: 94126920480 / 06211830481

Via / Piazza: Via Giorgio Vasari N. civico: 4

Città: Roma Cap: 00196 Provincia: RM

Email: IEEE_ITALY@IEEE.ORG Pec: pec@pec.ieeesezioneitalia.it

Sito istituzionale http://sites.ieee.org/italy

DATI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Lettera di incarico

Roma, 28/05/2019

Oggetto: Lettera di nomina di amministratore di sistema

Il sottoscritto Bernardo TELLINI, in qualità di rappresentante legale della SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, con sede legale in Via Giorgio Vasari 4, 00196 Roma (RM), titolare del trattamento dei dati ai sensi del Regolamento UE 2016/679 e della normativa nazionale in vigore, affida al Sig. Bernardo TELLINI per la sede LEGALE, Via Giorgio Vasari 4, 00196 Roma RM, dalla data del 28/05/2019 alla data del 28/05/2020, l'incarico di amministratore di sistema con i seguenti compiti:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up secondo i criteri stabiliti dal Titolare/Responsabile del Trattamento dei dati;
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;
- fare in modo che sia prevista la disattivazione dei “codici identificati personali” (User-ID), in caso di perdita della qualità che consentiva all’utente o incaricato l’accesso all’elaboratore, oppure nel caso di mancato utilizzo dei “codici identificativi personali” (User-ID) per oltre 6 mesi;
- gestire le password di root o di amministratore di sistema
- collaborare con il responsabile del trattamento dei dati personali;
- collaborare con il custode delle password;
- informare titolare e responsabili sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

L’amministratore di sistema testé incaricato dichiara di essere a conoscenza di quanto stabilito dal Regolamento UE 2016/679 e normativa nazionale in vigore, e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme.

Per accettazione dell'incarico
L'amministratore di sistema
TELLINI BERNARDO

_____
(firma)

Il titolare del trattamento
TELLINI BERNARDO

_____
(firma)

Roma, 28/05/2019

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il sottoscritto Bernardo TELLINI, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

Alessandro SEVERINI Responsabile esterno del trattamento dei dati per la sede LEGALE, Via Giorgio Vasari 4, 00196 Roma RM, dalla data del 28/05/2019 alla data del 28/05/2020, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	CONSULENZA FISCALE
DURATA DEL TRATTAMENTO	• I dati personali saranno conservati per la sola durata del mandato, salvi gli obblighi di legge su termini maggiori
DESCRIZIONE DEI TRATTAMENTI	ADEMPIMENTI FISCALI E PREVIDENZIALI
FINALITÀ	• Accertamento e riscossione di tasse e imposte • ADEMPIMENTI CON GLI ENTI PREVIDENZIALI • Adempimento di obblighi fiscali o contabili • CONSULENZA FISCALE • ELABORAZIONE E TENUTA DELLE SCRITTURE CONTABILI E SOCIETARIE • REDAZIONE CONTRATTI • REDAZIONE MODELLI UNICI-770-DICHIARAZIONI VARIE
TIPO DI DATI PERSONALI	• Beni mobili • Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) • Elementi del patrimonio • Particolari (sensibili) • Personali • Stati di salute
CATEGORIE DI INTERESSATI	• Clienti ed utenti • Consulenti

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTO COME PARTNER

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come partner:

LEGALE
REGISTRO DEI TRATTAMENTI DEI DATI DEL TITOLARE

- Attività di formazione della associazione e gestione degli iscritti

ATTIVITA` CULTURALI, CORSI E ATTIVITA` DI FORMAZIONE E QUALIFICAZIONE PROFESSIONALE NELL'AMBITO DELLA INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE SU TUTTO IL TERRITORIO NAZIONALE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.

- Blocco
- Cancellazione
- Comunicazione
- Conservazione
- Consultazione
- Diffusione
- Distribuzione
- Elaborazione
- Interconnessione
- Modifica
- Organizzazione
- Raccolta
- Raffronto

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI
in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE
Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

- i dati devono essere raccolti solo per scopi:

- determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
- espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
- compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

<u>COMPITI PARTICOLARI DEL RESPONSABILE</u>
Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;

b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:

- il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati;
- se del caso, i trasferimenti di dati personali verso Paesi terzi;
- descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;

c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;

e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;

f) adempiere agli obblighi di sicurezza, quali:
   - adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
   - assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
   - testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;

h) su scelta del titolare del trattamento, cancellare o restituirgli 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 degli Stati membri preveda la conservazione dei dati;

i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;

j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;

l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.

m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;

n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(ALESSANDRO SEVERINI)

_____
(firma)

Il titolare del trattamento
TELLINI BERNARDO

_____
(firma)

Lettera di incarico

Oggetto: Lettera di nomina quale persona autorizzata al trattamento dati

Il sottoscritto Bernardo TELLINI, titolare del trattamento dei dati dello/a SEZIONE ITALIA DELLA IEEE ASSOCIAZIONE, con sede legale in Via Giorgio Vasari 4, 00196 Roma (RM), **conferisce** al Sig./Sig.ra ……(ruolo: ……..). l'**incarico** di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del *titolare/responsabile*.

ELENCO ATTIVITA' DI TRATTAMENTO

- Attività di formazione della associazione e gestione degli iscritti

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal *titolare/responsabile*;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
  a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del *titolare/responsabile*;
  b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni;
  c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;

- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;

- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Roma, ……

Per conoscenza ed accettazione
Persona autorizzata al trattamento dati

(nome e cognome) ……

_____
(firma)

Il titolare del trattamento
BERNARDO TELLINI

_____
(firma)

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI
ai sensi dell'art. 30 del GDPR 2016/679

Azienda/Organizzazione	**ASSOCIAZIONE SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**

REGISTRO	REGISTRO DEI TRATTAMENTI DEI DATI DEL TITOLARE

SEDE	LEGALE Via Giorgio Vasari 4, 00196 Roma - RM

Data revisione: 20/11/2018

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	TELLINI
	Nome	BERNARDO
	E-mail	
	PEC	
	N° telefono	

RESPONSABILE DEL TRATTAMENTO DEI DATI	Cognome	TELLINI
	Nome	BERNARDO
	E-mail	
	PEC	
	N° telefono	

TRATTAMENTO: Attività di formazione della associazione e gestione degli iscritti

Struttura	• Amministrazione • Sede legale • Sede operativa

Personale coinvolto	
Persone autorizzate	TELLINI BERNARDO
Clienti / Fornitori	
Altro/ descrizioni degli archivi	

Processo di trattamento	
Descrizione	ATTIVITA` CULTURALI, CORSI E ATTIVITA' DI FORMAZIONE E QUALIFICAZIONE PROFESSIONALE SU TUTTO IL TERRITORIO NAZIONALE FINALIZZATI ALLO SCAMBIO E SVILUPPO DI CONOSCENZE SCIENTIFICHE E TECNOLOGICHE NELL'AMBITO DELL'INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.
Finalità del trattamento	GESTIONE DEI FORNITORI (CONTRATTI, ORDINI, ARRIVI, FATTURE) GESTIONE DELLA CLIENTELA (CONTRATTI, ORDINI, SPEDIZIONI E FATTURE). ATTIVITA` CULTURALI, CORSI E ATTIVITA' DI FORMAZIONE E QUALIFICAZIONE PROFESSIONALE SU TUTTO IL TERRITORIO NAZIONALE, FINALIZZATI ALLOSCAMBIO E SVILUPPO DI CONOSCENZE SCIENTIFICHE E TECNOLOGICHE NELL'AMBITO DELL'INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.
Tipo di dati personali	Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Giudiziari Particolari (sensibili) Personali Elementi del patrimonio Riprese audio video / foto

Categorie di interessati	Docenti Soci associati ed iscritti Consulenti e liberi professionisti, anche in forma associata Clienti ed utenti Professionisti
Categorie di destinatari	Responsabili esterni Responsabili interni AGENZIE DEL TERRITORIO, DELLE ENTRATE E DEL DEMANIO Associazioni ed enti locali Banche e istituti di credito Autorità di vigilanza e controllo Clienti ed utenti Enti previdenziali ed assistenziali Camere di commercio, industria, artigianato ed agricoltura FORNITORI DI BENI E SERVIZI Istituzione di formazione professionale Ordini e collegi professionali Soggetti che svolgono attività di archiviazione della documentazione Società e imprese
Informativa	Si
Consenso	Non necessario
Profilazione	Non necessario
Dati particolari	Si
Frequenza trattamento	Giornaliero
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e saranno conservati in modalita` ristretta per i soli adempimenti fiscali per cinque anni.
Trasferimento dati (paesi terzi)	Si - Stati Uniti;
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Archiviazione	struttura cartacea ben custodita in stanza chiusa e non liberamente accessibile Archivio cartaceo custodito in armadio con serratura Anagrafico contabile Allievi con dati personali e particolari
Strutture informatiche di archiviazione	

ARCHIVIO DI SEDE	Cloud platform
Sede di riferimento	Sede Legale
Personale con diritti di accesso	
Note	Nel corso degli eventi formativi potrebbero essere effettuate delle riprese audio video o dei rilievi fotografici. Il trattamento di questi dati viene effettuato con le stesse condizioni di sicurezza e per le stesse finalità, anche promozionali dell'evento, attraverso la diffusione sul sito web o sui canali social della Associazione.
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Improbabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Riusciamo a gestire le misure di sicurezza tecniche e organizzative in accordo alla gpdr appoggiandosi a google drive o servizi cloud possibilmente messi a diposizione dalla IEEE, senza dover far riferimento a una sede (da cui, certificazione di impianti a norma, strutture a norma, porta blindata e quant'altro che potrebbe rendere piu` complessa la gestione della sicurezza dei dati)

Viene eseguita opportuna manutenzione
- Sono gestiti i back up
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Sono utilizzati software antivirus e anti intrusione
- Sono definiti i ruoli e le responsabilità
- Esistono procedure per l'individuazione del custode delle password
- E' presente una politica per la sicurezza e la protezione dei dati
- L'impianto elettrico è certificato ed a norma
- Sono stabiliti programmi di formazione e sensibilizzazione
- Studio protetto da porta blindata
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- I software utilizzati sono protetti da password
- - Viene eseguita opportuna manutenzione. - Sono gestiti i back up - I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili - Sono utilizzati software antivirus e anti intrusione. - Sono definiti i ruoli e le responsabilità. -

Esistono procedure per l'individuazione del custode delle password. - E' presenta una politica per la sicurezza e la protezione dei dati. - L'impianto elettrico è certificato ed a norma. - Sono stabiliti programmi di formazione e sensibilizzazione. - Studio protetto da porta blindata - Impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi. - I software utilizzati sono protetti da password

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- È applicata una gestione della password degli utenti

F.to Il Titolare / Il responsabile [] esterno del Trattamento dei dati

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Azienda/Organizzazione	**ASSOCIAZIONE SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**

REGISTRO	REGISTRO DEL TRATTAMENTO DEI DATI DEL RESPONSABILE ESTERNO (CONSULENZA FISCALE)

SEDE	LEGALE Via Giorgio Vasari 4, 00196 Roma - RM

Data revisione: 20/11/2018

Il registro delle attività di trattamento del Responsabile è stato elaborato in base alle disposizioni dell'art.30 e contiene tutte le attività di trattamento svolte da SEVERINI ALESSANDRO in qualità di Responsabile esterno del trattamento dati personali.

Il registro è tenuto in forma scritta, anche in formato elettronico ed è revisionato annualmente o tutte le volte che occorrono modifiche alle attività di trattamento.

Su richiesta, il titolare del trattamento o il responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Ai sensi dell'art. 30 comma 2 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del responsabile del trattamento, del titolare del trattamento del trattamento per conto del quale agisce;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Responsabile trattamento esterno	Cognome	SEVERINI
	Nome	ALESSANDRO
	E-mail	
	PEC	
	N° telefono	

Titolare trattamento dati	Cognome	TELLINI
	Nome	BERNARDO
	E-mail	
	PEC	
	N° telefono	

Le attività di trattamento che il Responsabile del trattamento svolge per conto dei Titolari sono le seguenti:

- ATTIVITA' DEL COMMERCIALISTA E ESPERTO CONTABILE

TRATTAMENTO: ATTIVITA' DEL COMMERCIALISTA E ESPERTO CONTABILE

Processo di trattamento	
Finalità del trattamento	Accertamento e riscossione di tasse e imposte Adempimento di obblighi fiscali o contabili ELABORAZIONE E TENUTA DELLE SCRITTURE CONTABILI E SOCIETARIE REDAZIONE DEL BILANCIO CONSULENZA FISCALE REDAZIONE MODELLI UNICI-770-DICHIARAZIONI VARIE REDAZIONE CONTRATTI
Tipo di dati personali	Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Codice fiscale Personali Elementi del patrimonio

	Giudiziari Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati relativi all'attività economica e commerciale
Tipologie di trattamenti	Comunicazione Conservazione Consultazione Elaborazione Organizzazione Raccolta
Trasferimento dati (paesi terzi)	No

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- E' applicata una gestione della password degli utenti - E' presenta una politica per la sicurezza e la protezione dei dati - I software utilizzati sono protetti da password - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - L'impianto elettrico è certificato ed a norma - Studio protetto da porta blindata

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Azienda/Organizzazione	**ASSOCIAZIONE SEZIONE ITALIA DELL'INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS**

TITOLARE	TELLINI BERNARDO

SEDE	LEGALE Via Giorgio Vasari 4, 00196 Roma - RM

Data revisione: 20/11/2018

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – valutazione del rischio normalizzato

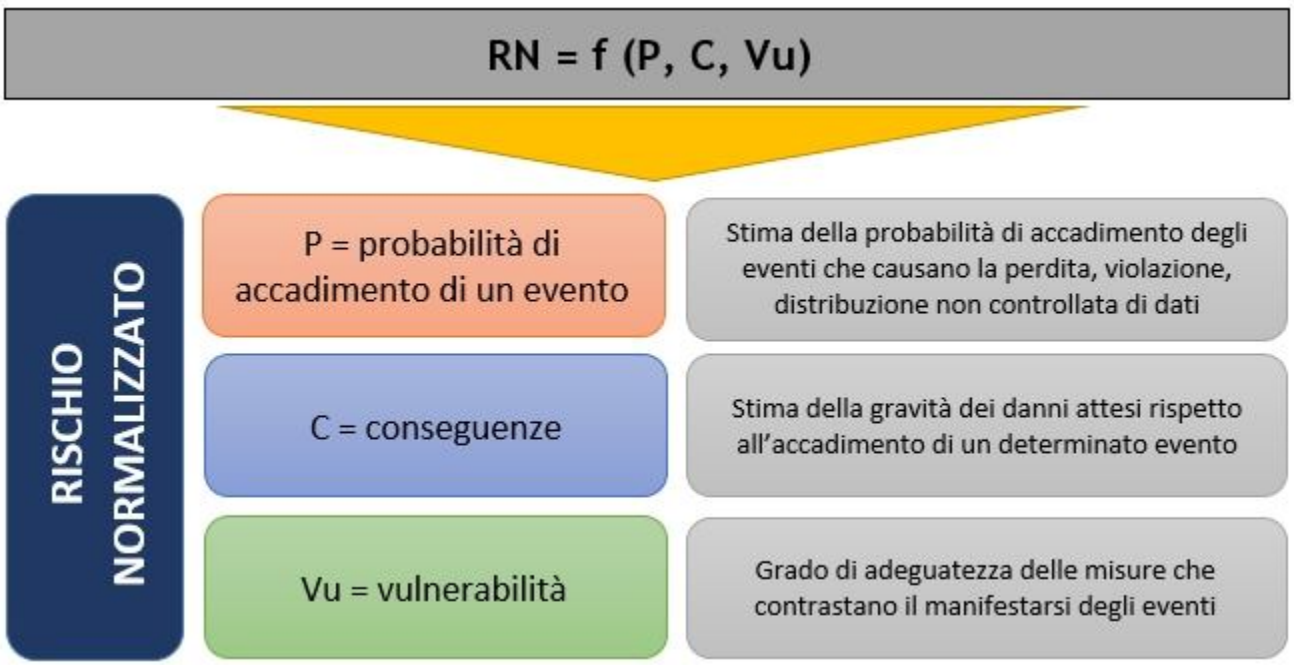
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

P = probabilità
C = conseguenze generate dall'evento



V = vulnerabilità rispetto al grado di adeguatezza delle misure

In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	**Valori di riferimento**
Molto basso	*(1 ≤ **Ri** ≤ 2)*
Basso	*(3 ≤ **Ri** ≤ 4)*
Rilevante	*(6 ≤ **Ri** ≤ 9)*
Alto	*(12 ≤ **Ri** ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	**Adeguate**	**0,25**
2	**Parzialmente adeguate**	**0,5**
3	**Inadeguate**	**1**

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	1 < ***RN*** ≤ 2	3 ≤ ***RN*** ≤ 4	6 ≤ ***RN*** ≤ 9	12 ≤ ***RN*** ≤ 16
	0,5	0,5 < ***RN*** ≤ *1*	1,5 ≤ ***RN*** ≤ 2	3 < ***RN*** ≤ 5	6 ≤ ***RN*** ≤ 8
	0,25	0,25 ≤ ***RN*** ≤ 0,5	0,75 ≤ ***RN*** ≤ 1	1,5 ≤ ***RN*** < 3	3 ≤ ***RN*** ≤ 4
		1 ≤ ***Ri*** ≤ 2	3 ≤ ***Ri*** ≤ 4	6 ≤ ***Ri*** ≤ 9	12 ≤ ***Ri*** ≤ 16
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	0,25 ≤ ***RN*** ≤ 1
Basso	1 < ***RN*** < 3
Rilevante	3 ≤ ***RN*** ≤ 9
Alto	12 ≤ ***RN*** ≤ 16

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Attività di formazione della associazione e gestione degli iscritti
- ATTIVITA' DEL COMMERCIALISTA E ESPERTO CONTABILE

Attività di formazione della associazione e gestione degli iscritti

Struttura	• Amministrazione • Sede legale • Sede operativa

Personale coinvolto	
Titolare del trattamento	Bernardo TELLINI
Persone autorizzate	
Partners - Responsabili esterni	SEVERINI ALESSANDRO • Blocco • Cancellazione • Comunicazione • Conservazione • Consultazione • Diffusione • Distribuzione • Elaborazione • Interconnessione • Modifica • Organizzazione • Raccolta • Raffronto
	Vanno inseriti anche gli altri officer - chiedere?
Altro	

Processo di trattamento	
Descrizione	ATTIVITA` CULTURALI, CORSI E ATTIVITA' DI FORMAZIONE E QUALIFICAZIONE PROFESSIONALE, SU TUTTO IL TERRITORIO NAZIONALE, FINALIZZATI ALLOSCAMBIO E SVILUPPO DI CONOSCENZE SCIENTIFICHE E TECNOLOGICHE NELL'AMBITO DELL'INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.?? ATTIVITA` CULTURALI, CORSI E ATTIVITA' DI

	FORMAZIONE E QUALIFICAZIONE PROFESSIONALE, SU TUTTO IL TERRITORIO NAZIONALE, FINALIZZATI ALLOSCAMBIO E SVILUPPO DI CONOSCENZE SCIENTIFICHE E TECNOLOGICHE NELL'AMBITO DELL'INGEGNERIA ELETTRICA, ELETTRONICA E DELL'INFORMAZIONE, ASSEGNAZIONE DI PREMI, RICONOSCIMENTI, BORSE DI STUDIO.
Fonte dei dati personali	Forniti da terzi Raccolti direttamente Raccolti tramite sito web
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Consenso Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso Contratto
Finalità del trattamento	Gestione dei fornitori (contratti, ordini, arrivi, fatture) Gestione della clientela (contratti, ordini, spedizioni e fatture) Trattamento giuridico ed economico del personale Corsi e attività di formazione
Tipo di dati personali	Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae Dati relativi a situazioni personali Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Giudiziari Particolari (sensibili) Personali Elementi del patrimonio Riprese audio video / foto DATI DEL PERSONALE DIPENDENTE
Categorie di interessati	Docenti Soci associati ed iscritti Consulenti e liberi professionisti, anche in forma associata Clienti ed utenti Consulenti Professionisti
Categorie di destinatari	Responsabili esterni Responsabili interni AGENZIE DEL TERRITORIO, DELLE ENTRATE E DEL DEMANIO Associazioni ed enti locali Banche e istituti di credito Autorità di vigilanza e controllo Clienti ed utenti Enti previdenziali ed assistenziali Camere di commercio, industria, artigianato ed agricoltura

	FORNITORI DI BENI E SERVIZI Istituzione di formazione professionale Ordini e collegi professionali Soggetti che svolgono attività di archiviazione della documentazione Società e imprese
Informativa	Si
Profilazione	Non necessario
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Settimanale
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Si - Stati Uniti;
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
ARCHIVIO DI SEDE	Struttura interna
Sede di riferimento	LEGALE
Personale con diritti di accesso	Eventuali officer
Software utilizzati	- GESTIONALE PROPRIO
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Improbabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Viene eseguita opportuna manutenzione
- Sono gestiti i back up
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Sono utilizzati software antivirus e anti intrusione
- Sono definiti i ruoli e le responsabilità
- Esistono procedure per l'individuazione del custode delle password
- E' presenta una politica per la sicurezza e la protezione dei dati
- L'impianto elettrico è certificato ed a norma
- Sono stabiliti programmi di formazione e sensibilizzazione
- Studio protetto da porta blindata
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- I software utulizzati sono protetti da password
- - Viene eseguita opportuna manutenzione. - Sono gestiti i back up - I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili - Sono utilizzati software antivirus e anti intrusione. - Sono definiti i ruoli e le responsabilità. - Esistono procedure per l'individuazione del custode delle password. - E' presenta una politica per la sicurezza e la protezione dei dati. - L'impianto elettrico è certificato ed a norma. - Sono stabiliti programmi di formazione e sensibilizzazione. - Studio protetto da porta blindata - Impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi. - I software utulizzati sono protetti da

password
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- E' applicata una gestione della password degli utenti

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
- Viene eseguita opportuna manutenzione. - Sono gestiti i back up - I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili - Sono utilizzati software antivirus e anti intrusione. - Sono definiti i ruoli e le responsabilità. - Esistono procedure per l'individuazione del custode delle password. - E' presenta una politica per la sicurezza e la protezione dei dati. - L'impianto elettrico è certificato ed a norma. - Sono stabiliti programmi di formazione e sensibilizzazione. - Studio protetto da porta blindata - Impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi. - I software utulizzati sono protetti da password		
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
E' applicata una gestione	• Problemi tecnici (Anomalie e	

della password degli utenti	malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Esistono procedure per l'individuazione del custode delle password	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
I software utulizzati sono protetti da password		
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
L'impianto elettrico è	• Interruzione servizi (sbalzi di	

certificato ed a norma	tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	
Sono stabiliti programmi di formazione e sensibilizzazione	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Sono utilizzati software antivirus e anti intrusione	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
Studio protetto da porta blindata		
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	

Nessuna valutazione DPIA

ATTIVITA' DEL COMMERCIALISTA E ESPERTO CONTABILE

Processo di trattamento	
Descrizione	STRUTTURA PER LA GESTIONE DELLA ATTIVITA' DEI SERVIZI FORNITI DA REVISORI CONTABILI-PERITI-CONSULENTI-ALTRI SOGGETTI
Finalità del trattamento	Accertamento e riscossione di tasse e imposte ADEMPIMENTI CON GLI ENTI PREVIDENZIALI Adempimento di obblighi fiscali o contabili ELABORAZIONE E TENUTA DELLE SCRITTURE CONTABILI E SOCIETARIE REDAZIONE DEL BILANCIO CONSULENZA FISCALE REDAZIONE MODELLI UNICI-770-DICHIARAZIONI VARIE REDAZIONE CONTRATTI
Tipo di dati personali	Beni, proprietà, possessi (proprietà, possessi e locazioni; beni e servizi forniti o ottenuti) Personali Elementi del patrimonio Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Tipologia di trattamento	Comunicazione Conservazione
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Improbabile	Trascurabili	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- E' applicata una gestione della password degli utenti - E' presenta una politica per la sicurezza e la protezione dei dati - I software utulizzati sono protetti da password - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - L'impianto elettrico è certificato ed a norma - Studio protetto da porta blindata

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
E' applicata una gestione	• Problemi tecnici (Anomalie e	

della password degli utenti	malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
E' presenta una politica per la sicurezza e la protezione dei dati	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
I software utulizzati sono protetti da password		
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	
Studio protetto da porta blindata		

Nessuna valutazione DPIA