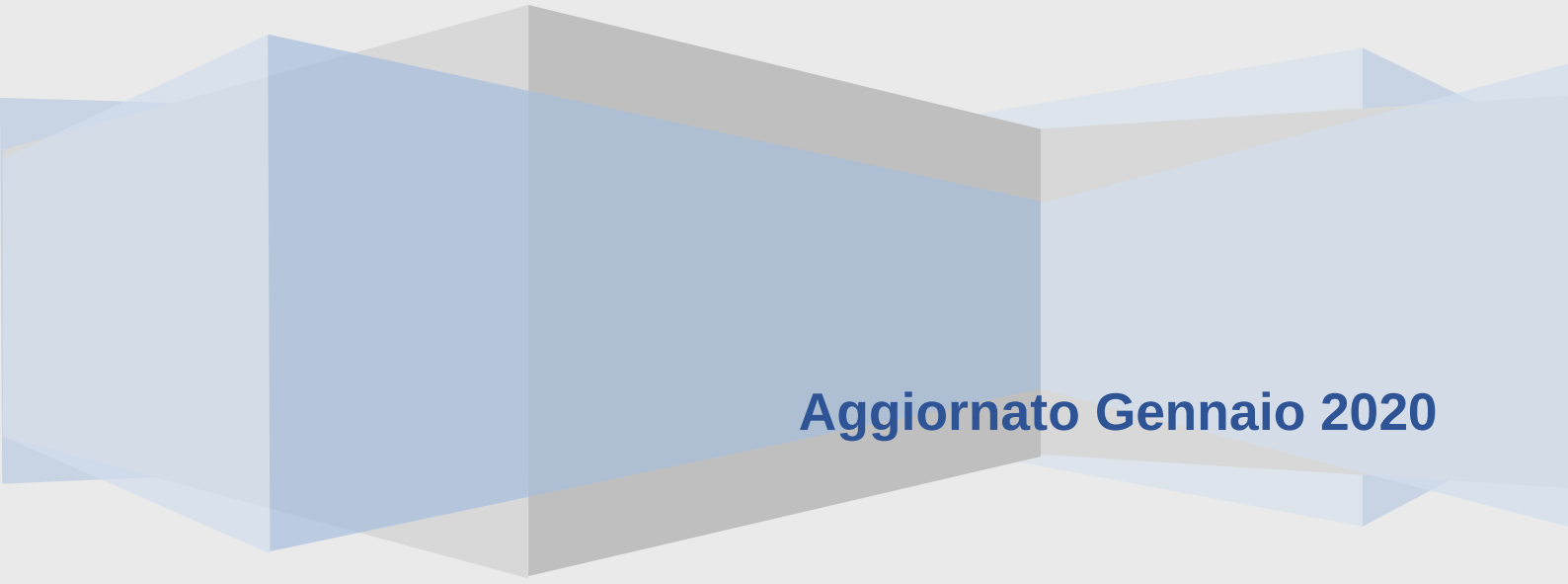
ISTRUZIONI OPERATIVE

PER GLI INCARICATI DEL TRATTAMENTO



Aggiornato Gennaio 2020

INDICE

1. PREMESSA

Il presente documento illustra le “linee guida” a cui i dipendenti incaricati del trattamento dei dati personali devono attenersi nel corso dello svolgimento delle proprie mansioni in conformità a quanto previsto dal Decreto Legislativo 10 Agosto 2018, n. 101 "*Codice in materia di protezione dei dati personali*" (di seguito Codice che recepisce il nuovo regolamento Europeo sul trattamento dei dati personali 679/2016 (di seguito Regolamento).

L’inosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale per l’incaricato e per l’istituto per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

Tale documento si applica, indistintamente, a tutti gli Incaricati "interni" che si trovano ad operare sui dati personali di cui l’I.C. Via Cassia Km 18.700 è Titolare.

2. DEFINIZIONI

Ai fini del presente regolamento s'intende per:

1) «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;
=> Motivo: 26, 27, 28, 29, 38,

2) «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; , , ,

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
=> Articolo: 18
=> Motivo: 67

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
=> Motivo: 30, 91

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
=> Motivo: 26, 28, 29

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

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
=> Articolo: 26

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
=> Articolo: 28

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
=> Motivo: 31, , ,

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

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
=> Articolo: 6, 7, 8
=> Motivo: 32, 33, 38, 42, 43

12) «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;
=> Articolo: 33, 34
=> Motivo: 85, 86, 86, 87, 88, ,

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
=> Motivo: 34

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
=> Motivo: 91

15) «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;
=> Articolo: 9
=> Motivo: 35, 91

16) «stabilimento principale»: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
=> Articolo: 56
=> Motivo: 36, 124

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
=> Motivo: 80

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
=> Articolo: 26
=> Motivo: 37, 48, 150

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro; ,

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. LINEE GUIDA

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Incaricato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

3.1. ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività;
- utilizzata, laddove possibile, in modo esclusivo da un solo utente;
- protetta, evitando che terzi possano accedere ai dati che si sta trattando.

Occorre, inoltre, precisare che spetta all'Incaricato:

- non utilizzare in istituto risorse informatiche private senza specifica autorizzazione;
- non installare alcun software senza preventiva autorizzazione e di dubbia provenienza;
- non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate;
- richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo max.10 minuti di inattività;
- non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);
- non lasciare incustoditi cellulari e palmari;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

3.2. GESTIONE DELLE PASSWORD

Per una corretta gestione delle password, ciascun Incaricato deve aver cura di:

- cambiarla almeno ogni 90 giorni, o immediatamente nei casi in cui sia compromessa;
- comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito;
- usare sia lettere che numeri e almeno un carattere maiuscolo e/o uno speciale (ad es. $! £ ? @ % -> <);
- non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc.,
- mantenerla riservata e non divulgarla a terzi (Salvo specifica richiesta da parte della titolarità);
- non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi, né lasciarla memorizzata sul proprio PC;
- non comunicarla mai per telefono salvo gravi necessità.

3.3. ANTIVIRUS

I Personal Computer (PC) in dotazione agli utenti, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.
Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;
- chiudere correttamente i programmi in uso;
- non aprire, se si lavora in rete, files sospetti e di dubbia provenienza;
- non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate;
- verificare con l'ausilio del programma antivirus in dotazione ogni supporto dati (Pennette USB, HD Esterni), prima dell'esecuzione dei file in esso contenuti;
- non utilizzare, CD-Rom, Pennette USB, HD Esterni di provenienza incerta;
- non utilizzare Pennette USB, HD Esterni già utilizzati su PC su cui è noto che si sono verificati malfunzionamenti;
- porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;
- non modificare le configurazioni impostate sul proprio PC;
- spegnere il PC al termine della giornata di lavoro;

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'Incaricato:

a. sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto;
b. contatti immediatamente l'Area IT o le figure responsabili;
c. chiuda il sistema e le relative applicazioni.

3.4. SALVATAGGIO DEI DATI

Tutti i dati al termine della giornata lavorativa vanno salvati sul cloud dell'istituto.

Quando, per varie ragioni, non fosse possibile il salvataggio centralizzato dei dati sul cloud dell'istituto, l'incaricato dovrà procedere, con cadenza almeno settimanale, all'effettuazione di copie di sicurezza dei dati personali oggetto del trattamento.

Nel caso in cui per le copie di Back-Up o per la conservazione di qualunque altro dato siano utilizzati supporti informatici quali, Cd-Rom, Dvd-Rom, Pen Driver, ecc., gli Incaricati devono osservare le seguenti misure di sicurezza al fine di salvaguardare la riservatezza delle informazioni in essi contenuti:

- conservarli in un luogo sicuro al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- etichettarli riportando la chiara indicazione dei dati in esso contenuti;
- distruggerli o renderli inutilizzabili quando non più necessari;
- cancellare i dati precedentemente registrati prima di riutilizzarli. Se l'operazione non è tecnicamente eseguibile distruggere i supporti.

3.5. PROTEZIONE DEI PC PORTATILI

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa.

Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

- conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'Istituto;

- avvertire tempestivamente l'Area IT o le figure responsabili, che darà le opportune indicazioni, in caso di furto di un PC portatile;
- essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;
- operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

3.6. INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno all'Istituto.

In particolare, occorre osservare le seguenti regole:

- navigare solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- non scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
- evitare di registrarsi a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
- non utilizzare funzioni di instant messaging salvo autorizzazione preventiva;
- non aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);
- non rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto;
- non utilizzare la posta elettronica per comunicare informazioni riservate, dati personali o dati critici, senza garantirne l'opportuna protezione;
- accertarsi sempre che i destinatari siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;
- essere consapevoli che posta elettronica e navigazione Internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi.

3.7. TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

- chiedere il nome del chiamante e la motivazione della richiesta;
- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
- verificare che il numero dichiarato corrisponda a quello del chiamante;
- procedere immediatamente a richiamare la persona che ha richiesto l'informazione, con ciò accertandosi della identità dichiarata in precedenza.

Quando il dato deve essere inviato a mezzo posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;
- nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;
- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

4. ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L'accesso a tutti i locali dell'Istituto deve essere consentito solo a personale preventivamente autorizzato dalla Titolarità.

5. CONTROLLI DA PARTE DELLA TITOLARITA'

Con il presente capitolo portiamo all'attenzione degli incaricati la possibilità di questo Istituto di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà dell'Istituto in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli dell'Istituto stesso.

6. RIFERIMENTI NORMATIVI

Linee guida del garante per posta elettronica e internet.
Con questa delibera (Deliberazione n.13 del 1/03/2007 – pubblicata sulla G.U. n.58 del 10 marzo 2007) il Garante pone particolare attenzione all'utilizzo dello strumento tecnologico di proprietà del azienda/istituto/ente/ etc. per usi personali da parte del dipendente. Sottolinea alle azienda/istituto/ente/ etc. la necessità di segnalare chiaramente ai propri dipendenti la possibilità da parte loro del controllo, da parte di appositi incaricati, degli strumenti tecnologici dati a loro in dotazione per l'espletamento dell'attività lavorativa. Tali controlli devono essere mirati alla preservazione della sicurezza dell'azienda/istituto/ente/ etc. stesso non a ledere i diritti di privacy del singolo. In conclusione l'azienda/istituto/ente/ etc. può controllare i propri strumenti tecnologici a condizione di aver avvertito i propri dipendenti di questa possibilità e avendo chiaramente indicato (come nei capitoli precedenti è stato fatto) che gli stessi possono essere utilizzati solo a fini Lavorativi.

Tribunale di Torino, Sezione Distaccata di Chiasso, Sentenza 20 Giugno 2006 (dep. 15/07/2006), n.143.
Questa sentenza, ratificata anche dalla Corte di Cassazione, ha visto assolvere l'imputato dalle accuse che gli erano state mosse. Nei fatti, il PM si era espresso a favore di una sentenza di condanna per la Ditta XXX che, tramite suoi incaricati, aveva acceduto presso la postazione informatica di un dipendente senza il consenso dello stesso. Il Giudice ha ritenuto che l'accesso agli strumenti informatici aziendali da parte della Ditta non costituisse reato, purché i dipendenti fossero stati preventivamente ed adeguatamente informati circa la possibilità che ciò potesse verificarsi.

Art.84 Regolamento Europeo 679/2016 "Sanzioni"
1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.
2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

Articolo 29 Regolamento Europeo 679/2016 "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento"
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

7. ATTIVITÀ ISPETTIVA E PROCEDURE SANZIONATORIE

Si ricorda che il Codice e il Regolamento in argomento comporta, per chi lo disattende, sanzioni civili e penali, ma anche provvedimenti da parte dell'Autorità Garante che, ove ravvisasse ipotesi di trattamenti illeciti o non conformi, può disporre ispezioni di verifica ed imporre anche il blocco dei trattamenti.

L'Istituto nel corso degli anni si è dotata di strumenti tecnologici al fine di migliorare la produttività e la sicurezza. La circostanza ha richiesto l'individuazione di figure che avessero capacità manutentive per i nuovi strumenti tecnologici. Oggi sono presenti incaricati interni e società esterne che compiono attività di manutenzione Hardware e Software. Tutti i soggetti coinvolti hanno ricevuto specifiche indicazioni circa il comportamento deontologico da adottare nell'ordinaria e straordinaria manutenzione

Si informa, infine, che il Titolare ed il Responsabile, in esecuzione degli obblighi derivanti dal Codice, possono disporre verifiche periodiche sull'osservanza delle presenti disposizioni.

Redatto in collaborazione con:	DPO
Approvato ed emanato da:	Refertante della Titolarità

Ultima pagina del documento