Nome del documento / procedura	Sezione:	Livello di riservatezza:
ISTRUZIONI PER I SOGGETTI DESIGNATI AL TRATTAMENTO	**DESIGNAZIONE SOGGETTI AUTORIZZATI**	**Controllato**

Allegato 1

INDICE

ISTRUZIONI PER GLI ADDETTI

1) PREMESSA

L'articolo 29 del Regolamento Europeo 2016/679, stabilisce che:
"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".
Chiunque abbia accesso ai dati personali dovrà obbligatoriamente essere istruito dal Titolare o dal Responsabile del trattamento. Limitatamente ai trattamenti dati e all'ambito di competenza a Lei assegnato nella designazione in qualità di soggetto autorizzato dal titolare del trattamento, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nelle operazioni di trattamento dei dati personali, in conformità alle normative vigenti in materia di trattamento dei dati personali ed in particolare al GDPR.
Il soggetto designato deve essere sempre in grado di comprendere ed avere consapevolezza rispetto al tipo di dato che sta trattando secondo quanto stabilito nelle definizioni dell'articolo 4 e secondo i principi applicabili al trattamento dei dati personali di cui all'articolo 5 e secondo le basi giuridiche dell'art. 6 del GDPR. Le istruzioni sotto riportate fanno riferimento anche alla normativa interna in materia di trattamento di dati personali.
Qualora avesse necessità di chiarimenti, deve fare riferimento al Titolare del Trattamento, e/o al referente designato.

2) CONTESTO NORMATIVO GENERALE DI RIFERIMENTO

Per i trattamenti dati relativi a cittadini ubicati nella UE:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE; di seguito "GDPR" in inglese: General Data Protection Regulation.

- Linee guida e del European Data Protection Board siglato EDPB
Il Comitato europeo per la protezione dei dati (EDPB) o Consiglio europeo per la protezione di dati è un organismo dell'Unione europea che sostituisce il Gruppo dell'articolo 29 per la tutela dei dati dal 25 maggio 2018 ed è incaricato dell'applicazione del nuovo regolamento sulla protezione dei dati (GDPR regolamento 2016/679). È composto dal rappresentante di ciascuna autorità per la protezione dei dati e dal garante europeo della protezione dei dati e dal loro rappresentante. Il comitato contribuirà a garantire che la nuova legislazione sulla protezione dei dati sia applicata in modo corretto in tutta l'UE.

3) NORMATIVA SPECIFICA VIGENTE IN ITALIA:

- D.Lgs. 101/2018 che va a modificare il D.Lgs. 196/2003
Che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

- D.Lgs. 196/2003 così come modificato da D.Lgs. 101/2018
Decreto legge italiano adeguato con il D.Lgs. 101/2018.

- Linee guida e provvedimenti del Garante della Privacy italiano anche precedenti all'applicazione del GDPR
Le linee guida ed i provvedimenti del Garante Privacy italiano sono ad oggi ancora validi e vigenti se non in contrasto con il GDPR, in rif. all'art. 22 del D.Lgs. 101/2018

- Legge n. 300 del 1970 (Statuto dei lavoratori)

- Lavoro trasparente D.Lgs. n. 104/2022
attuazione della Direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019, relativa alle condizioni di lavoro trasparenti e prevedibili, il Legislatore ha emanato nuove norme con lo scopo di rafforzare la tutela dei lavoratori rispetto agli obblighi informativi cui è tenuto il datore di lavoro. Fra gli obblighi informativi occorre annoverare gli obblighi in merito al trattamento dei dati dei lavoratori, per i quali si richiedono alcune integrazioni alle informazioni da rendere ai lavoratori in ottemperanza di tale decreto.

- D.Lgs. 10 marzo 2023, n. 24
Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

- Telelavoro e Smartworking: "lo Smartworking deriva dal telelavoro"

Telelavoro:
La parola stessa indica il lavoro che si svolge a distanza (tele…) rispetto alla sede centrale. Si è diffuso negli anni '70 grazie allo sviluppo delle tecnologie informatiche. I cd teleworkers lavoravano per lo più da casa o in un luogo specifico distaccato/ decentrato. Con l'Accordo Quadro del 2004, il telelavoro segue normative specifiche, come ad esempio l'obbligo – da parte del datore di lavoro – di eseguire ispezioni per sincerarsi del regolare svolgimento del lavoro, con tutto ciò che ne consegue in termini di prestazione, allo stesso modo, performante che di sicurezza.
Lavoro agile / Smartworking
Al netto delle considerazioni già svolte in proposito, la sostanziale differenza rispetto al telelavoro risiede nella non più necessità di "legarsi" ad un luogo fisico fisso (di fatto, poi sempre il medesimo, come potrebbe essere il domicilio) ove lavorare. In smart working si può lavorare da casa, così come in un bar o ristorante, ovvero ancora in un parco o qualunque luogo altro luogo nel quale poter adoperare un pc o uno smartphone, o un tablet, ed avere una connessione WIFI. L'orario viene autodeterminato, purché si raggiunga l'obiettivo prefissato ed il monte ore è gestito dal dipendente (smart workers). A costoro, i meglio noti come "lavoratori agili", è garantita la parità di trattamento: economico e giuridico.

4) FOCUS SUL REGOLAMENTO (UE) 2016/679

Vengono riportate di seguito le definizioni, i riferimenti normativi ed i relativi considerando per una più chiara lettura e comprensione del GDPR. Sono indicati i considerando (es. C1) del GDPR in riferimento ai principi ispiratori del legislatore europeo, che occorrono a completare la comprensione dei concetti.

4.1) Definizioni (Articolo 4);
«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; (C26, C27, C30);
«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;
«Limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro (C67);
«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 (C24, C30, C71-C72);
«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 (C26, C28-C29);
«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 (C15);
«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 (C74);
«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;
«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 (C31);
«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;
«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 (C32, C33);

«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 (C85);
«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 (C34);
«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 (C51);
«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 (C35);
«Stabilimento principale»: (C36, C37):
- 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;
«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 (C80);
«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;
«Gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate (C37, C48);
«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 (C37, C110);
«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
«Autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto (C124):
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;
«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;
«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);
«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.

4.2) Principi applicabili al trattamento di dati personali (Articolo 5):

1. I dati personali sono (C39):
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 del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74);

4.3) Liceità del trattamento - basi giuridiche del trattamento dati - Articolo 6 Reg. UE 2016/679

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40);
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43);
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 (C44);
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (C45);
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (C46);
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 (C45, C46);
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. (C47-C50)
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.
Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX. (C8, C10, C41, C45, C51);
3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: (C8, C10, C41, C45, C51) 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, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), 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. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente 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. 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, 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: (C50)
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; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Qui di seguito vengono precisate due importanti categorie di dati. L'articolo 9 e 10 del GDPR definiscono:

4.4) Trattamento di categorie particolari di dati personali - Articolo 9 Reg. UE 2016/679

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. (C51);
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52);
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 di cui al paragrafo 1;
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; (C55, C56);
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; (C53);
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; (C54);
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), 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. (C53);
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. (C8, C10, C41, C45, C53).

4.5) Trattamento dei dati personali relativi a condanne penali e reati - Articolo 10 Reg. UE 2016/679
Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

ISTRUZIONI OPERATIVE PER LA SICUREZZA ED IL CORRETTO TRATTAMENTO DEI DATI

1) PREMESSA
Nello svolgimento della propria mansione, ogni dipendente/collaboratore che trattata dati personali, siano essi identificativi o rientrino nelle categorie di dati particolari o dati personali relativi a condanne penali e reati, con strumenti elettronici e non, deve adottare le precauzioni sotto riportate.
Oltre alle istruzioni generali che seguono, l'incaricato dovrà attenersi al Regolamento degli strumenti informatici, ove presente. Tale documento riporta infatti indicazioni, procedure e le modalità di controllo sull'attività del lavoratore nonché gli eventuali provvedimenti disciplinari.

2) VERIFICA DELL'ESATTEZZA DEI DATI

L'Organizzazione addotta criteri al fine di monitorare il grado di esattezza dei dati personali trattati, attraverso le fasi di:

– acquisizione dei dati mediante verifica della coerenza dei dati personali
Occorre adottare criteri di verifica della coerenza dei dati personali, ad esempio confrontando l'anno indicato nella data di nascita con il codice fiscale, oppure l'età della persona, oppure verificando la congruenza del codice fiscale, in ogni caso se i dati sono raccolti verbalmente è buona prassi rileggere quanto acquisito per conferma, eventualmente utilizzare lo spelling.

– segnalazione di eventuali errori, modifiche, o problematiche nella raccolta;
Nel caso in cui ravvisi una inesattezza o ad esempio un indirizzo email risulti non corretto (perché viene segnalato un errore in automatico e/o nella mail di ritorno) proceda a correggere l'errore senza ritardo, ove necessario contattando gli interessati.

– rifiuto di raccolta dei dati incompleti o imprecisi;
Qualora i dati siano incompleti o imprecisi e non permettano di effettuare le corrette attività di trattamento dati proceda a rifiutare l'acquisizione parziale o imprecisa, segnalando immediatamente la problematica all'interessato, o al soggetto che ha comunicato i dati.

– verifica o richiesta di conferma dei dati personali trattati qualora sia necessario adottare una decisione che possano ledere i diritti o libertà degli interessati, in presenza di rischio medio e alto del trattamento dati.
Sono adottati criteri ragionevoli per ridurre il rischio di assumere decisioni che possono ledere i diritti degli interessati sulla base di informazioni e dati non esatti, o non aggiornati relativamente ai soggetti interessati. Tali criteri sono trasferiti al personale attraverso le istruzioni ai soggetti designati ed autorizzati al trattamento dei dati.

La formazione del personale ricopre quindi un ruolo principale soprattutto quando i dati devono essere caricati e raccolti manualmente dai vari soggetti designati. In questi casi, infatti, il rischio dell'errore umano assume una concreta possibilità di manifestarsi. L'adozione di istruzioni comportamentali costituiscono idonee misure di controllo che possono facilitare il rispetto del principio di "esattezza" anche a fronte di garantire la c.d. "privacy by design" art. 25 del GDPR.

Istruzioni specifiche sono rilasciate al personale designato per la gestione dei diritti degli interessati di cui agli art. da 15 a 22 del GDPR.

3) AFFIDAMENTO AI SOGGETTI AUTORIZZATI DI DOCUMENTI CONTENENTI DATI PERSONALI E MODALITÀ DA OSSERVARE PER LA CUSTODIA DEGLI STESSI

3.1) TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del referente in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare. Al di fuori delle autorizzazioni ricevute non è possibile prendere visione di nessun documento. Una volta presi in carico, gli atti e i documenti contenenti dati personali, non devono essere lasciati incustoditi senza controllo ed a tempo indefinito nei locali ove si svolge il trattamento. Provvedere in qualche modo a controllarli e custodirli, per poi riporli negli archivi al termine delle operazioni affidate.
In caso di affidamento di atti e documenti contenenti categorie particolari di dati personali e dati personali relativi a condanne penali e reati, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione.
A tale fine, è quindi necessario dotarsi di cassetti e/o contenitori muniti di serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti le categorie dei dati sopra citati prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa). In mancanza di tali strumenti sollecitare il referente del titolare e/o il Titolare affinché provveda.

Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento. Qualora si debbano utilizzare anche nei giorni successivi i documenti potranno essere riposti in tali cassetti al termine della giornata lavorativa. Al termine del trattamento dovranno invece essere riposti nell'archivio.

Distruzione dei documenti

Qualora sia necessario disfarsi di documenti cartacei riportanti dati personali è necessario provvedere alla distruzione di tali documenti prima di conferirli negli appositi contenitori per i rifiuti cartacei. Occorre assicurarsi che dopo l'operazione di distruzione dei documenti non sia più possibile risalire ai dati personali contenuti originariamente. A tal fine è suggerita l'adozione di appositi distruggi documenti.

Stampanti

E' fatto d'obbligo assicurarsi che i documenti prodotti dalle stampanti aziendali, sia presso il proprio ufficio, che presso aree comuni, siano presidiati fino alla completa esecuzione della stampa, così da non permettere ad altri soggetti non autorizzati la presa visione, o l'asportazione. Se necessario è suggerito dotarsi di opportune misure tecniche ed organizzative atte ad impedire la stampa dei documenti senza la presenza dell'operatore, ad esempio mediante impostazione di codice di autorizzazione individuale per la stampa.

Nello svolgimento della propria mansione, ogni dipendente/collaboratore che trattata dati personali, siano essi identificativi o particolari, o relativi a condanne con strumenti elettronici, deve adottare anche le precauzioni sotto riportate.

3.2) I SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto: tali strumenti vanno custoditi in modo appropriato e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni disciplinari, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali.

In questo contesto l'azienda potrà per necessità di sicurezza aziendale o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione. Per ulteriori informazioni fare riferimento al Regolamento aziendale per l'utilizzo degli strumenti elettronici se presente e/o alle disposizioni del datore di lavoro.

3.3) UTILIZZO DEL PERSONAL COMPUTER

E' consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal referente.

Non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri.

Non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.).

I Personal Computer "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.

3.4) UTILIZZO DI INTERNET – REGOLE GENERALI

Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate.

Non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge.

Non è consentito navigare in siti che possano consentire una profilazione dell'individuo. In particolare con la navigazione in alcuni siti si potranno evincere palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali.

Non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto.

Non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal Titolare o dal Responsabile.

Non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer.

E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

Non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames).
Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

4) UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA
Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:
-Non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
-Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
-La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente riservati";
-Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list. Tale partecipazione può avvenire solo previa autorizzazione da parte del referente e/o del Titolare sulla base delle procedure aziendali;
Nel caso esista un dominio di proprietà aziendale (es.: nomeazienda.it) al quale sia collegato un servizio di posta e la relativa casella (es.: rossi@nomeazienda.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini aziendali salvo diversa ed esplicita autorizzazione o specifiche disposizioni dell'organizzazione.

5) MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD
Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione. Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto. Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Incaricato.
Nel caso in cui sia prevista la figura del custode delle copie credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa (meglio se sigillata) all'incaricato od al responsabile addetto alla loro custodia. Fare riferimento al Titolare od al referente per i dettagli operativi della procedura. Elaborare le password seguendo le istruzioni sotto riportate.

5.1) SCELTA DELLE PASSWORD
Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

5.2) COSA NON FARE
NON dica a nessuno la sua password. Ricordi che lo scopo principale per cui usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.
NON scriva la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
Quando immette la password NON faccia sbirciare a nessuno quello che sta battendo sulla tastiera.
NON scelga password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
NON creda che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
NON usi il suo nome utente. È la password più semplice da individuare.
NON usi password che possano in qualche modo essere legate a lei come, ad esempio, il suo nome, quello di sua moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

5.3) COSA FARE OBBLIGATORIAMENTE
La password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica.
L'incaricato deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema.
La password deve essere modificata dall'incaricato almeno ogni 6 mesi.
Se il trattamento riguarda categorie particolari di dati personali e dati personali relativi a condanne penali e reati la password deve essere modificata almeno ogni tre mesi.

5.4) CONSIGLI PRATICI PER L'UTILIZZO DELLE PASSWORD
Utilizzare più di una parola e creare password lunghe.
A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare. Inoltre

è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un ottima protezione contro possibili violazioni.
Utilizzare numeri e simboli al posto di caratteri
Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:
Caratteri minuscoli: a, b, c,...
Caratteri maiuscoli: A, B, C,...
Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?
Non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare. Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

5.5) INDICAZIONI SULLE PASSWORD DALL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

www.garanteprivacy.it/flash

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network*, ecc.).

Consigli flash

X TUTELARE

la tua privacy

con buone password

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che anche gli altri profili che ti appartengono possano essere violati.

3 CONSERVA CON CURA LE PASSWORD

- **Non conservare mai** le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet*.
- **Evita di condividere** le password via e-mail, sms, *social network*, *instant messaging*, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

4 PROVA AD USARE SOFTWARE «GESTORI DI PASSWORD»

Si tratta di programmi specializzati che **generano password sicure** e **consentono di appuntare sul pc tutte le password salvandole in un database cifrato sicuro.**
Ce ne sono di vario tipo, gratuiti o a pagamento.

Ti suggeriamo di consultare anche le altre schede informative che trovi su www.garanteprivacy.it/flash **e le nostre campagne di comunicazione** «Social privacy», «Fatti smart» **e** «Connetti la testa».
Se hai dubbi e domande, puoi contattare l'URP del Garante: www.garanteprivacy.it/home/urp

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

6) OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI MENTRE È IN CORSO UNA SESSIONE DI LAVORO

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:
- Incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
- Accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.
Non si devono invece mai verificare situazioni in cui lo strumento elettronico venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un incaricato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave. E' possibile installare strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password. Verifichi con i Responsabili o con il Titolare le possibilità di abilitazione dello strumento.

7) PROCEDURE E MODALITÀ DI UTILIZZO DEGLI STRUMENTI E DEI PROGRAMMI ATTI A PROTEGGERE I SISTEMI INFORMATIVI
In collaborazione con i Responsabili o con il Titolare, che possono installare dove previsti degli automatismi in grado di sostituirsi all'incaricato, prevedere di:
Aggiornare con cadenza almeno mensile gli antivirus installati sulla propria postazione PC. Si consigliano ovviamente cadenza più serrate;
Installare le Patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dati personali, con cadenza annuale che diviene semestrale in caso di trattamenti di dai sensibili o giudiziari.

8) FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE:
- Riutilizzo di dispositivi esterni già adoperati in precedenza, o da terzi;
- Uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
- Collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- Collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- File attached di posta elettronica (allegati)

9) LINEE GUIDA PER LA PREVENZIONE DEI VIRUS E ALTRI PROGRAMMI MALEVOLI
Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido. Come prevenire i virus:

- Usi soltanto programmi provenienti da fonti fidate
Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzi programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.
- Si assicuri che il suo software antivirus sia aggiornato
La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Si informi attraverso il Portale della privacy sugli obblighi di legge in tema di aggiornamento degli antivirus e applichi, se possibile, una frequenza di aggiornamento mensile (più idonea di quella prevista dalla legge).
- Si assicuri che il suo PC sia stato controllato dall'antivirus
Almeno una volta alla settimana e provveda a lanciare una scansione dell'intero sistema con il suo software antivirus. Se questo software lo prevede, scheduli anche in questo caso la programmazione della scansione in maniera tale da non doversi ricordare di lanciarla e lasciando che il programma la esegua in automatico. Si consulti con i Responsabili o con il Titolare per le informazioni necessarie.
- Non apra, utilizzi o diffonda messaggi di provenienza dubbia
Se riceve messaggi che avvisano di un nuovo virus pericolosissimo, lo ignori: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).
- Non partecipi a "catene di S. Antonio" o simili
Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente

le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare al termine del proprio accesso.
- Eviti la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
- Non utilizzi i server di rete come stazioni di lavoro;
- Non aggiunga mai dati o file a memorie di massa removibili a meno che non siano proteggibili in scrittura e con sistema di accesso controllato;
- E' buona norma assicurarsi di non far partire accidentalmente il computer con una chiavetta USB inserita, o un CD, DVD. Infatti se il dischetto fosse infettato, il virus si trasferirebbe nel computer e potrebbe espandersi ad altri files.

10) OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI
Anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra incaricati, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

11) CYBERSECURITY DALL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

11.1) SOCIAL ENGINEERING
Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati. Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

11.2) E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere

con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore. Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima.

11.3) RAMSONWARE DALL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Attenzione al ransomware. Il programma che prende "in ostaggio" il tuo dispositivo

L'emergenza sanitaria da **Covid2019** - che porta molte più persone e per molto più tempo ad essere connesse online e ad utilizzare dispositivi digitali - sembra essere affiancata da un pericoloso "contagio digitale", alimentato da malintenzionati che diffondono software "malevoli" per varie finalità illecite. Una delle attività più diffuse e dannose è attualmente il cosiddetto ransomware.

Cos'e' il ransomware?

Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, "ransom") da pagare per "liberarli".
La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All'utente viene minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.
Ci sono due tipi principali di ransomware:

- i cryptor (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);
- i blocker (che bloccano l'accesso al dispositivo infettato).

Come si diffonde?
Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

- sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);
- contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli.

In altri casi, il ransomware può essere scaricato sul dispositivo quando l'utente:

- clicca **link o banner pubblicitari su siti web** (un canale molto usato è rappresentato dai siti per adulti) o social network
- naviga su **siti web creati ad hoc o "compromessi"** da hacker per diventare veicolo del contagio ransomware.

Il ransomware può essere diffuso da malintenzionati anche attraverso **software e app** (giochi, utilità per il PC, persino falsi anti-virus), offerti gratuitamente per invogliare gli utenti al download e infettare così i loro dispositivi.
E' bene ricordare che **ogni dispositivo "infettato" ne può "contagiare" altri**. Il ransomware può diffondersi sfruttando, ad esempio, le sincronizzazioni tra dispositivi, i sistemi di condivisione in cloud, oppure può impossessarsi della rubrica dei contatti e utilizzarla per spedire automaticamente ad altre persone messaggi contenenti link e allegati che diventano veicolo del ransomware.

Come difendersi?
La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.) e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ognora il contenuto.
Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze. Ad esempio:

- non aprire mai **allegati con estensioni "strane"** (ad esempio, allegati con estensione ".exe" sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare **software da siti sospetti** (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);
- **scaricare preferibilmente app e programmi da market ufficiali**, i cui gestori effettuano controlli sui prodotti e dove è eventualmente possibile leggere i commenti di altri utenti che contengono avvisi sui potenziali rischi;
- se si usa un pc, si può **passare la freccia del mouse su eventuali link o banner pubblicitari** ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso nella finestra del browser, si può vedere l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).

E' inoltre utile:

- installare su tutti i dispositivi un **antivirus con estensioni anti-malware**;
- **mantenere costantemente aggiornati** il sistema operativo oltre che i software e le app che vengono utilizzati più spesso;
- utilizzare dei sistemi di **backup** che salvino (anche in maniera automatica) una copia dei dati (sono disponibili soluzioni anche libere e gratuite per tutti i sistemi operativi). Con un corretto backup, in caso di necessità, si potranno così ripristinare i dati contenuti nel dispositivo, quantomeno fino all'ultimo salvataggio.

Come liberarsi dal ransomware?
Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in "liste di pagatori" potenzialmente soggetti a periodici attacchi ransomware.
La soluzione consigliata è quella di rivolgersi a **tecnici specializzati** capaci di sbloccare il dispositivo.
Un'alternativa efficace è quella di **formattare il dispositivo**: ma in questo caso, oltre ad eliminare il malware, si perdono tutti i dati in esso contenuti. Per questo è fondamentale (come suggerito) effettuare backup periodici dei contenuti (che è sempre una buona prassi) in modo da non perderli in caso di incidenti (es: danneggiamento del dispositivo, ecc.) o attacchi informatici che necessitano di interventi di ripristino.

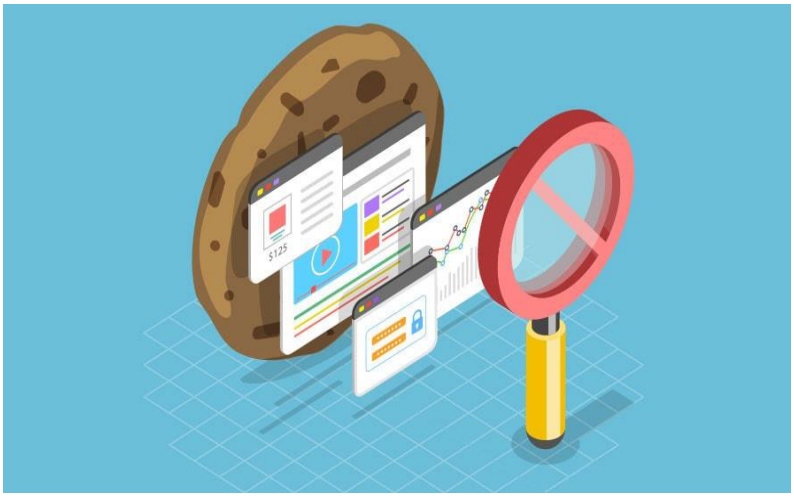
11.4) DEEPFAKE – IL FALSO CHE TI <<RUBA>> LA FACCIA E LA PRIVACY
I deepfake sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

11.5) PHISHING: ATTENZIONE AI <<PESCATORI>> DI DATI PERSONALI

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente

11.6) LINEE GUIDA SULL'UTILIZZO DI COOKIE E DI ALTRI STRUMENTI DI TRACCIAMENTO

I cookie sono di regola stringhe di testo che i siti web (cd. publisher o "prima parte") visitati dall'utente ovvero siti o web server diversi (cd. "terze parti") posizionano ed archiviano – direttamente, nel caso dei publisher e indirettamente, cioè per il tramite di questi ultimi, nel caso delle "terze parti" - all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo.



12) CYBERSECURITY DALL'ENISA PER LA SICUREZZA INFORMATICA DURANTE L'ACQUISTO E LA VENDITA ONLINE

L'Agenzia dell'Unione europea per la cybersicurezza (ENISA) è attiva dal 2004 sul fronte della sicurezza informatica in Europa. L'ENISA collabora con l'Unione europea (UE) e i suoi Stati membri, di concerto con il settore privato e i cittadini europei, al fine di formulare consigli e raccomandazioni sulle buone pratiche in materia di sicurezza delle informazioni. Assiste inoltre gli Stati membri dell'UE nell'attuazione della legislazione dell'Unione in materia e lavora per migliorare la resilienza delle infrastrutture critiche informatizzate e di rete in Europa. L'ENISA si adopera per potenziare l'attuale livello di competenza degli Stati membri dell'UE, sostenendo lo sviluppo di comunità transfrontaliere impegnate a migliorare la sicurezza delle reti e delle informazioni in tutta l'UE. Dal 2019 è attiva nel predisporre schemi di certificazione della cybersicurezza. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

L'Agenzia dell'UE per la sicurezza informatica ha sviluppato 10 suggerimenti per PMI e cittadini per garantire la sicurezza durante l'acquisto e la vendita online.
Suggerimenti per la sicurezza informatica durante l'acquisto e la vendita online
L'epidemia di Covid-19 ha portato a un aumento dell'e-commerce poiché le persone cercano online per acquistare qualsiasi cosa, dai libri ai generi alimentari. Un lato positivo di questo è la crescita della trasformazione digitale, in particolare delle piccole imprese, che hanno bisogno di una presenza online per sopravvivere.

Per i cittadini: acquisti online in sicurezza informatica

1. Connessione sicura: presta attenzione al sigillo di sicurezza di ogni sito web che stai navigando cercando la presenza del lucchetto verde nella barra degli indirizzi. Ciò significa in generale che la connessione viene stabilita su un canale protetto.
2. Fai attenzione alle e-mail di phishing Covid-19 e ai siti Web falsi : c'è stato un aumento nella registrazione dei domini, che contengono la parola "Corona", che viene utilizzata dai criminali informatici per offrire truffe. Diffidare di qualsiasi messaggio di posta elettronica che chiede di controllare o rinnovare le proprie credenziali anche se sembra provenire da una fonte attendibile. In tutti i casi, prova a verificare l'autenticità della richiesta con altri mezzi, non fare clic su collegamenti sospetti o aprire allegati sospetti. Fai attenzione alle e-mail che pretendono di essere una fattura per un acquisto che in realtà non è stato effettuato.
3. Frode nei pagamenti : controlla regolarmente i tuoi conti online e gli estratti conto bancari e segnala qualsiasi attività sospetta alla tua banca. Se pensi di essere stato vittima di un attacco, contatta la tua banca. Se possibile, attiva l'autenticazione a due fattori per i pagamenti.
4. Sistemi aggiornati : assicurati che il tuo sistema (sistema operativo e applicazioni utilizzate) sia aggiornato e assicurati che antivirus e antimalware siano installati e completamente aggiornati .
5. Proteggi la tua privacy: pensaci due volte quando ti vengono richiesti i dati e leggi le politiche sulla privacy. Se è necessario creare un account con un fornitore, utilizzare password complesse che non possono essere facilmente previste e utilizzare un gestore di password. Evita di condividere informazioni personali con persone che non conosci sui social media. Prendi in considerazione l'utilizzo di strumenti per la privacy, come anti-tracking e strumenti di messaggistica sicura, per la tua protezione online e mobile.

Per le PMI: vendita online cyber sicura

1. Proteggi il tuo sito web per i clienti : è fondamentale che tu abbia la giusta sicurezza per proteggere sia la tua azienda ma anche i tuoi clienti, ad esempio utilizza connessioni https e abilita l'autenticazione a 2 fattori ove possibile. Inoltre è importante testare la sicurezza del sito web e garantire un supporto adeguato ai clienti in caso di problemi.
2. Proteggi le tue risorse: proprio come qualsiasi altra risorsa aziendale, le informazioni devono essere gestite e protette strategicamente. La sicurezza delle informazioni è la protezione delle informazioni all'interno di un'azienda, inclusi i sistemi e l'hardware utilizzati per archiviare, elaborare e trasmettere queste informazioni. Assicurati che sia in atto una politica di sicurezza, insieme a tutte le misure di sicurezza tecniche e organizzative necessarie.
3. Memorizza le password in modo sicuro: se i clienti devono creare account per acquistare dal tuo sito web, assicurati che tutte le password siano archiviate in modo sicuro. Assicurati che i dati dei tuoi clienti siano protetti secondo le regole del settore. Ove possibile, assicurati che i dati sensibili non siano leggibili, potrebbero essere applicate soluzioni come hash con chiave o salati.
4. Garantire la conformità ai requisiti di protezione dei dati: quando si elaborano i dati personali dei clienti, assicurarsi di rispettare il quadro giuridico sulla protezione dei dati. Visita il sito web della tua autorità nazionale per la protezione dei dati per ulteriori informazioni.
5. Monitorare e prevenire gli incidenti : disporre di una politica di risposta agli incidenti di sicurezza e assicurarsi che siano adottate misure per la prevenzione, il monitoraggio e la risposta agli incidenti di sicurezza, comprese le violazioni dei dati personali.

13) REGOLE DA RISPETTARE PER LA SALVAGUARDIA DEL PATRIMONIO INFORMATIVO

Non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
Limitatevi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato.
Diffidate di messaggi provenienti da fonte non conosciuta.
Non aprite messaggi provenienti da fonte non conosciuta contenenti allegati.
Non aprite messaggi contenenti allegati sospetti
Non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome.
Non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta.
Non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità.
In caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il referente o il Titolare.

14) PROCEDURE PER IL SALVATAGGIO DEI DATI

Gli incaricati sono tenuti a fare riferimento alla politica interna di back up per le istruzioni specifiche di salvataggio. Se è nominato l'incaricato delle copie di back up, egli sarà il referente per tali operazioni.

15) CUSTODIA ED UTILIZZO DEI SUPPORTI RIMUOVIBILI, CONTENENTI DATI PERSONALI

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. dischetti, chiavette usb, hd removibili, etc), contenenti dati sensibili o giudiziari, nei seguenti termini:

- I supporti rimovibili contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

16) DOVERE DI AGGIORNARSI, UTILIZZANDO IL MATERIALE E GLI STRUMENTI FORNITI DALL'ORGANIZZAZIONE, ATTINENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

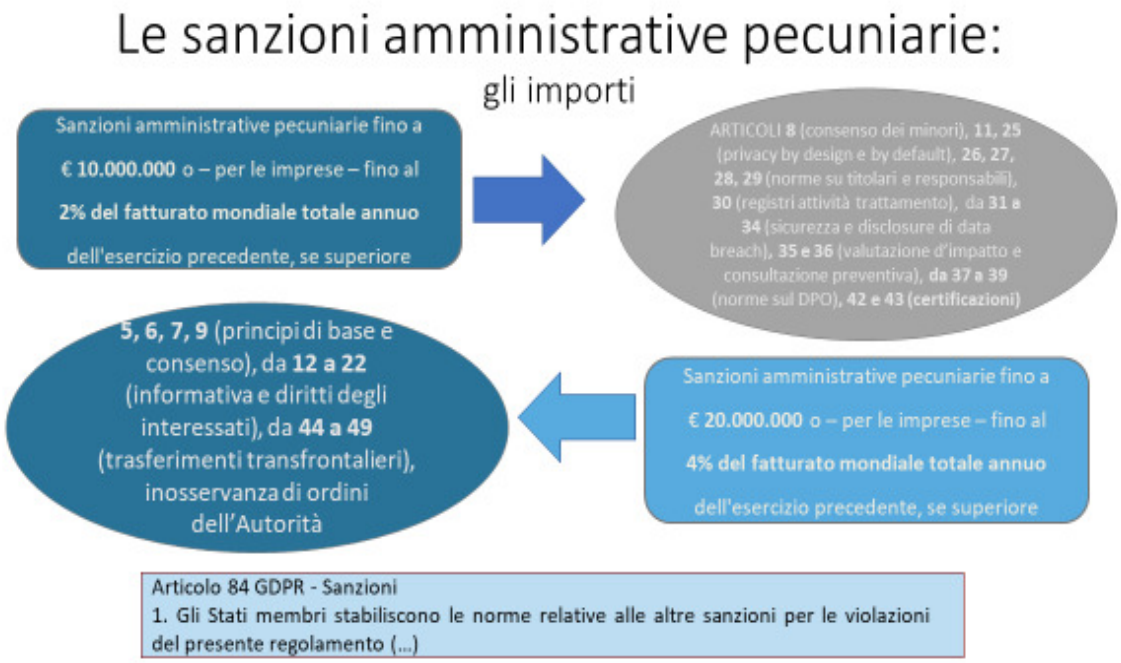
Qualora non siano già stati adottati, pretendere dal titolare che vengano forniti strumenti per la formazione sulla privacy. In particolare relativamente a:
- Profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività e conseguenti responsabilità che ne derivano;
- Rischi che incombono sui dati;
- Misure disponibili per prevenire eventi dannosi;
- Modalità per aggiornarsi sulle misure minime di sicurezza, adottate dall'Organizzazione.

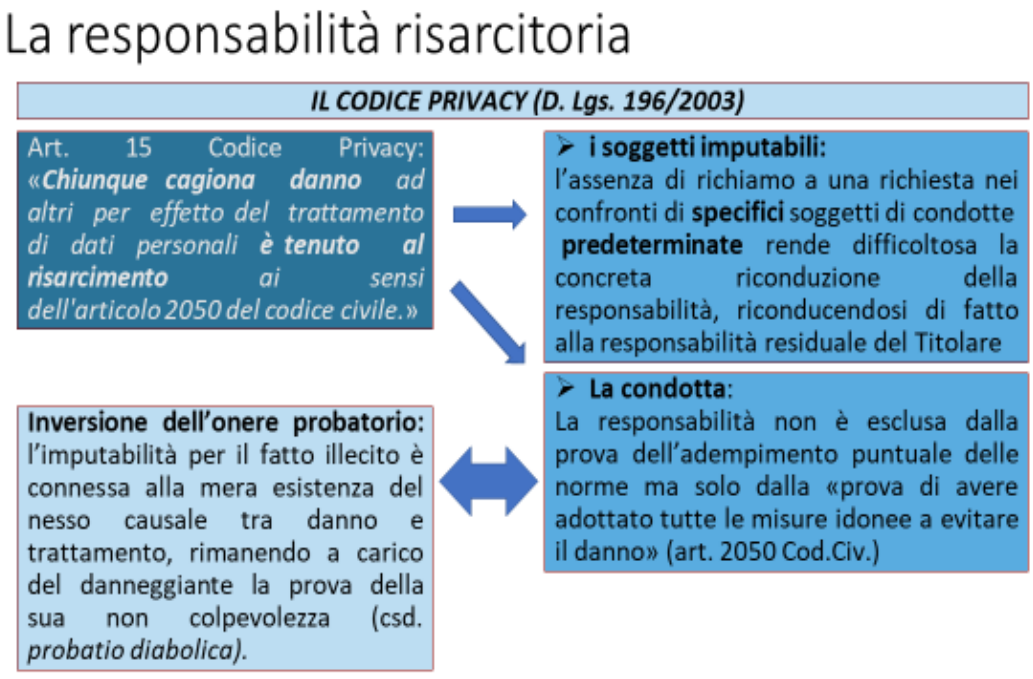
17) RIESAME ED AGGIORNAMENTO DELLE POLITICHE

Le politiche per il trattamento dei dati e per la sicurezza dei dati sono verificate in termini di pertinenza e aggiornamento all'attuali allo stato dell'arte tecnico, e confermate od aggiornate almeno una volta all'anno.

Le politiche sono revisionate a seguito di un cambiamento sostanziale del business che comporta differenti trattamenti dati, introduzione di nuove tecnologie, incidenti di sicurezza che richiedono la revisione delle misure tecniche ed organizzative, o per altre motivazioni descritte per ciascun aggiornamento.

18) SLIDE SULLE SANZIONI DEL GDPR E SULLA RESPONSABILITÀ





Nome del documento / procedura	Sezione:	Livello di riservatezza:
ISTRUZIONI PER I SOGGETTI DESIGNATI AL TRATTAMENTO	**DESIGNAZIONE SOGGETTI AUTORIZZATI**	**Controllato**

LA RESPONSABILITÀ RISARCITORIA

IL GDPR (Regolamento UE 679/2016)

Art. 82, comma 1 GDPR:
Chiunque subisca un danno materiale o immateriale ***causato da una violazione*** del presente regolamento ha il diritto di ottenere il risarcimento del danno dal ***titolare del trattamento o dal responsabile*** del trattamento»

I soggetti imputabili: art. 82, co 3: «Il Titolare del trattamento o il Responsabile del trattamento è esonerato dalla responsabilità (...) se dimostra che l'evento dannoso non gli è in alcun modo imputabile.»

- **La condotta:**

è sempre necessaria la prova di avere adottato tutte le misure idonee a evitare il danno» (cfr. art. 2050 Cod.Civ.), prova fondata sull'esistenza, delle logiche e della coerenza con i fini di sicurezza e protezione dei dati, dei passaggi (analisi, progetti, azioni) che hanno caratterizzato la costruzione del proprio personale percorso di conformità alle norme.

Imputazione:
-Specifica: collegata alla ***non conformità*** del trattamento a specifiche norme del GDPR.
-Soggettiva: riconducibile a ***specifici soggetti, formalmente individuati***, cui è imputabile la violazione specifica che ha causato il danno.
-Solidale: Titolare e Responsabile rispondono in solido per l'ammontare del danno (art. 82, co. 4).

Tenendo conto dello stato dell'arte e dei costi di attuazione, il Titolare del trattamento e il Responsabile:
- mettono in atto misure tecniche e organizzative adeguate (...) volte ad attuare in modo efficace i principi di protezione dei dati (...)» (*Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita).*
- mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio» (*Art. 32 - Sicurezza del trattamento).*

Le responsabilita' per la violazione del gdpr.

Formalizzazione dei ruoli

Il titolare del trattamento assume responsabilità per qualsiasi trattamento che effettua direttamente o che altri effettuino per suo conto, ma a ciascuno degli attori è riconosciuta anche responsabilità autonoma

TITOLARE

Contratto o altro atto giuridicamente vincolante, scritto, contenente obblighi e garanzie di conformità al Regolamento: contratto individuale o basato su clausole contrattuali tipo

SUB-RESPONSABILE ← RESPONSABILE → SUB-RESPONSABILE

SUB-RESPONSABILE

SUB-RESPONSABILE

- Autorizzazione ***scritta*** del Titolare.
- Atto giuridicamente vincolante contenente gli stessi obblighi e garanzie di conformità al regolamento contenuti nella nomina rilasciata dal Titolare

Impianto sanzionatorio

2% del fatturato
(od € 10.000.000,00)

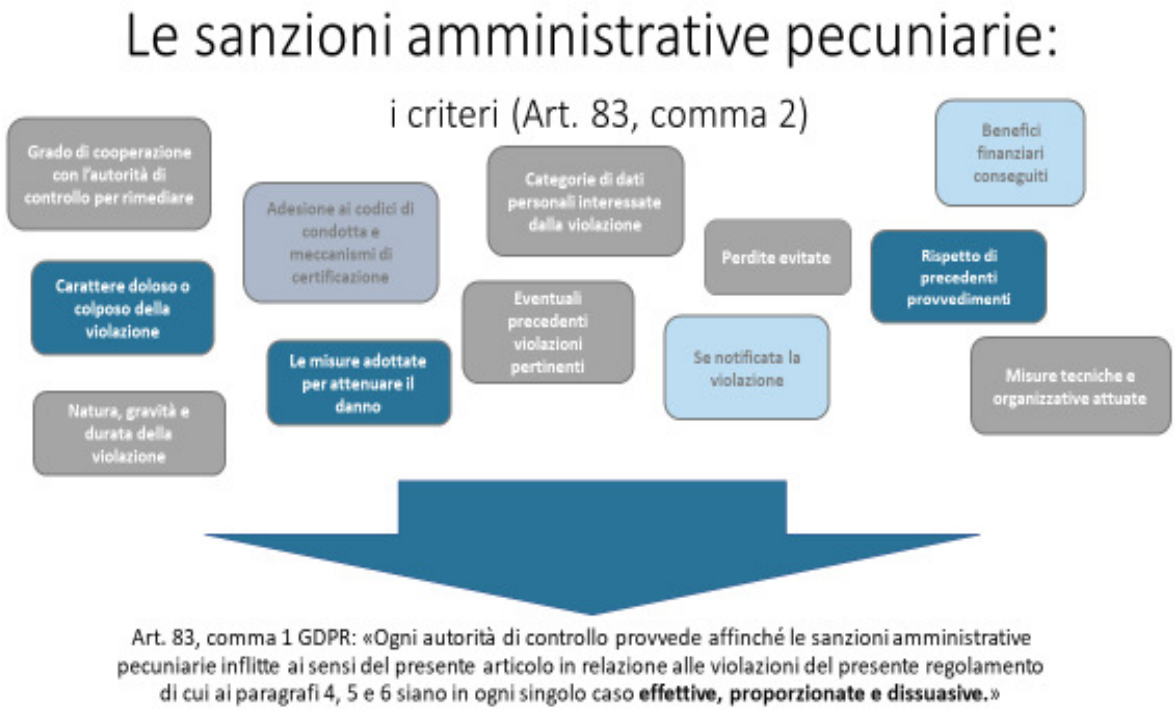
SANZIONI NELLE SEGUENTI MATERIE

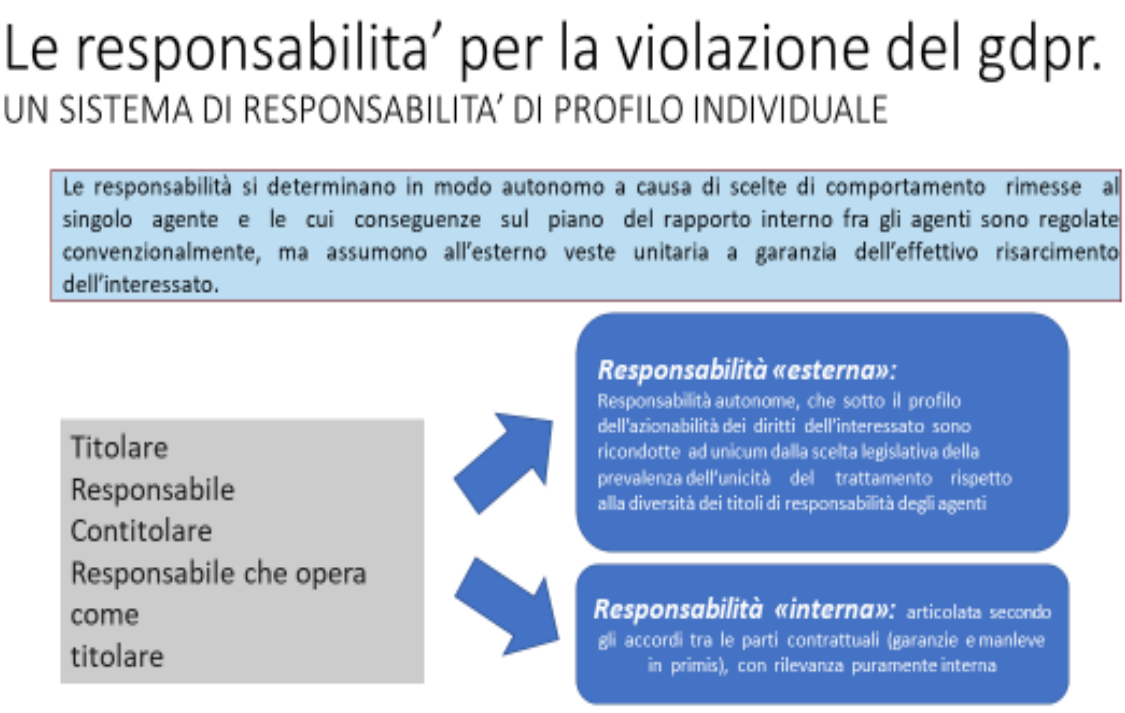
Consenso minori;
Trattamento che non richiede identificazione;
Protezione dei dati by design e by default;
Obblighi dei contitolari;
Stabilimento in ambito UE;
Doveri del Responsabile del trattamento;
Trattamenti consentiti;
La registrazione dei trattamenti;
La cooperazione con le autorità di supervisione;
Sicurezza del trattamento;
Notificazione del Data breach e sua comunicazione all'interessato;
Data Protection Impact Assessment;
Prior Consultation;
Designazione, Posizione, Attribuzioni del DPO;
Certificazioni e organismi di certificazione;
Monitoraggio dei codici di condotta;
Consenso dei bambini nella società dell'informazione

4% del fatturato
(od € 20.000.000,00)

SANZIONI NELLE SEGUENTI MATERIE

Principi sul trattamento dei dati;
Legalità del trattamento;
Consenso;
Trattamento di speciali categorie di dati;
Diritti dell'interessato;
Trasferimento dei dati in ambito extra UE;
Trattamento in ambito giornalistico e del diritto di espressione;
Rispetto delle disposizioni delle autorità;
Accesso ai dati da fonti pubbliche;
Trattamento dei numeri identificativi;
Trattamento dei dati del personale;
Trattamenti archivistici di interesse pubblico riguardo dati scientifici, storici, di ricerca, o statistici;
Obbligo di segretezza;
Opinioni religiose.


Le sanzioni amministrative pecuniarie:
i criteri (Art. 83, comma 2)
Grado di cooperazione con l'autorità di controllo per rimediare
Adesione ai codici di condotta e meccanismi di certificazione
Categorie di dati personali interessate dalla violazione
Benefici finanziari conseguiti
Carattere doloso o colposo della violazione
Perdite evitate
Rispetto di precedenti provvedimenti
Eventuali precedenti violazioni pertinenti
Le misure adottate per attenuare il danno
Se notificata la violazione
Misure tecniche e organizzative attuate
Natura, gravità e durata della violazione
Art. 83, comma 1 GDPR: «Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.»


Le responsabilita' per la violazione del gdpr.
UN SISTEMA DI RESPONSABILITA' DI PROFILO INDIVIDUALE
Le responsabilità si determinano in modo autonomo a causa di scelte di comportamento rimesse al singolo agente e le cui conseguenze sul piano del rapporto interno fra gli agenti sono regolate convenzionalmente, ma assumono all'esterno veste unitaria a garanzia dell'effettivo risarcimento dell'interessato.
Titolare
Responsabile
Contitolare
Responsabile che opera come titolare
Responsabilità «esterna»:
Responsabilità autonome, che sotto il profilo dell'azionabilità dei diritti dell'interessato sono ricondotte ad unicum dalla scelta legislativa della prevalenza dell'unicità del trattamento rispetto alla diversità dei titoli di responsabilità degli agenti
Responsabilità «interna»: articolata secondo gli accordi tra le parti contrattuali (garanzie e manleve in primis), con rilevanza puramente interna