Attribuzione di funzioni e compiti a soggetti designati in qualità di

Dirigente

operanti sotto l'autorità del titolare del trattamento, art. 29 del Regolamento Europeo (UE) 2016/679.

L'Agenzia della Mobilità Piemontese,

nella persona del suo legale rappresentante pro-tempore

Ai sensi e per gli effetti del Regolamento (UE) 2016/679,

nella persona di: _____, ai sensi e per gli effetti dell'art. 29 del Regolamento (UE) 2016/679 ed in riferimento all'Art. 2 – quaterdecies D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018 (Attribuzione di funzioni e compiti a soggetti designati),

considerato che quest'ultimo può prevedere, sotto la propria responsabilità e nell'ambito dell'assetto organizzativo dell'Ente, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto l'autorità del titolare con il presente atto

INDIVIDUA

Il Sig./Sig.ra: (dirigente) _____

Area/Servizio: _____

Quale **REFERENTE** con attribuzione di specifici compiti e funzioni, ed alla delega dell'esercizio e svolgimento degli stessi

Nello svolgimento dei compiti assegnati dovrà quindi:

[X] attenersi ai principi applicabili al trattamento dei dati,

[X] individuare e designare il Responsabile della Protezione dei Dati (art. 37 Reg. UE 2017/679);

[X] individuare eventuali ruoli quali contitolari del trattamento, responsabili del trattamento, persone autorizzate al trattamento dei dati sotto l'autorità del titolare, e definirne i rapporti nonché gli opportuni accordi interni;

[X] redigere idonee informative rivolte a tutti i soggetti interessati del trattamento in capo al Settore specifico, sulla base dei modelli proposti;

[X] designare ed istruire mediante specifici compiti ed istruzioni i soggetti che effettuano trattamenti dati sotto l'autorità del titolare, nonché assicurarsi che abbiano sottoscritto accordi di riservatezza,

[x] adottare il piano di formazione e stabilire un programma temporale

[x] assicurarsi nell'individuazione dei responsabili esterni del trattamento (art. 28 Reg. UE 2017/679) l'adozione di idonee garanzie, specifiche istruzioni, accordi di riservatezza, e controlli successivi.

(Principi applicabili ai dati personali)

- I dati personali sono:

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

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

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

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

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

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

- Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74) - principio di accountability -

Inoltre:

(Compiti del titolare)

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo precedente includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

(Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78) – Privacy by design e privacy by default)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati;

il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

(Registro del trattamento art. 30 del Regolamento)

Effettuare la mappatura e censimento di tutti i trattamenti dati, eventualmente individuando ulteriori referenti per competenza, al fine della redazione del registro delle attività del trattamento; coinvolgere e collaborare con gli altri referenti al fine di completare le attività atte alla definizione del registro, nonché del suo aggiornamento e revisione.

Verificare eventuali trattamenti dati ove si possa configurare il ruolo dell'Ente quale Responsabile del trattamento dei dati, o contitolare del trattamento, e contribuire alla mappatura e censimento, nonché il loro aggiornamento e revisione.

(Sicurezza del trattamento)

mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

(Violazione di dati personali)

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo

(Valutazione d'impatto)

quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in

assenza di misure adottate dal titolare del trattamento per attenuare il rischio si assicura che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica si assicura che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti;

documenta, per iscritto ed è in grado di provare, in caso di richiesta dell'autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;

In generale il dirigente designato dovrà:

- collaborare con gli altri referenti designati e delegati, per l'elaborazione degli obiettivi strategici e operativi del sistema di sicurezza e di protezione dei dati personali, particolari e relativi a condanne,
- collaborare e coinvolgere il RPD nelle sue attività proprie rispetto agli art. 37, 38, 39 del Regolamento;
- effettuare la ricognizione integrale di tutti i trattamenti di dati personali, particolari e giudiziari svolti nella struttura organizzativa / ufficio / area di competenza, in correlazione con i processi / procedimenti svolti;
- effettuare l'aggiornamento periodico, almeno annuale e, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa, con obbligo di sottoporre l'aggiornamento all'approvazione del titolare;
- effettuare la valutazione del rischio e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati,
- assicurare la formazione del personale mediante una appropriata procedura,
- tutto quanto rientra nei compiti delegati dal titolare del trattamento per il settore di competenza

Ruolo del referente in qualità di persona autorizzata sotto l'autorità del titolare al trattamento dei dati – art. 29 Reg.UE 2016/679

L'ambito di applicazione della presente nomina fa riferimento ai tipi di dati ed alle mansioni sotto elencate:

Descrizione del/i trattamenti dati e finalità, in riferimento alla sua mansione, settore di competenza ed ufficio; ad integrazione di quanto indicati nel Registro del trattamento	**Trattamenti effettuati dalle strutture organizzative dell'Agenzia.**
Tipo di dati	**Dati di tipo:** **☒Comuni (Nome, cognome, indirizzo, etc.)** **☒Particolare (Origini razziali o etniche, opinioni politiche, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale, etc.)** **☒Relativi a condanne penali e reati**
Soggetti interessati al trattamento	**☒Utenti ☒Fornitori ☒Dipendenti ☐Altro (indicare):** **_____**

Particolare importanza rivestirà l'attenzione che verrà dedicata alle procedure indicate nelle istruzioni per l'Addetto (Allegato 1) alle quali vi è l'obbligo di attenersi scrupolosamente. Nello svolgimento della propria mansione, l'Addetto viene reso edotto che dovrà prendere visione dei nominativi di eventuali/ulteriori Addetti che sono stati autorizzati a trattare i dati da parte del Titolare o degli altri *Referenti del titolare* (Registro del trattamento). L'Addetto è tenuto a prenderne visione ed a comunicare al Titolare o agli altri *Referenti del titolare* eventuali inesattezze. Se gli strumenti elettronici di lavoro consentissero la connessione con altre banche dati, la sua nomina come addetto al trattamento comprenderà l'incarico di trattare anche i dati delle banche dati connesse, nei limiti in cui ciò sarà necessario all'efficiente e corretto svolgimento delle Sue mansioni e sempre in conformità al profilo di autorizzazione e alle procedure indicate nelle istruzioni per l'Addetto (Allegato 1).

Il presente incarico è strettamente collegato e funzionale alle mansioni svolte da ciascun addetto e necessario per lo svolgimento delle stesse e che, pertanto, non costituisce conferimento di nuova mansione o ruolo. L'Addetto dichiara di aver ricevuto, in Allegato 1, le istruzioni e si impegna, dopo averne presa visione, ad adottare tutte le misure necessarie alla loro attuazione. Dichiara, inoltre, di aver preso visione del registro del trattamento, o di averne iniziata la redazione. L'addetto dovrà osservare scrupolosamente tutte le istruzioni ricevute e le misure di sicurezza già in atto, sia per effetto del Regolamento UE 2016/679, o che verranno comunicate in seguito dal titolare o condivise ed individuate dagli altri *Referenti del titolare*. Il presente incarico costituisce consapevole accettazione degli obblighi assunti.

Dichiarazione di ricevimento dell'atto di designazione, istruzioni di cui all'allegato 1, autorizzazione e delega e di impegno all'assunzione ed all'esercizio dei compiti e delle funzioni e delle responsabilità attribuite e delegate

Il/La sottoscritto/a: _____

Dichiara

di aver ricevuto il sovrascritto atto di designazione, attribuzione e delega di funzioni e responsabilità per il trattamento dei dati personali, particolari, relativi a condanne (giudiziari), nell'ambito della struttura organizzativa al quale preposto;

di aver attentamente letto e compreso il contenuto di detto atto, e di impegnarsi a attuare la delega;

di dare atto che l'obbligo di riservatezza correlato al ruolo assunto va osservato anche per il tempo successivo alla sua cessazione dell'incarico medesimo.

Luogo, data, firma

_____

Allegato 1

ISTRUZIONI PER IL REFERENTE

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 all'ambito di competenza a Lei assegnato nella Nomina dal Titolare o dal Responsabile, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti in materia di trattamento dei dati personali ed in particolare al GDPR.
L'incaricato deve essere sempre in grado di comprendere il 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 6 del GDPR.
Qualora avesse necessità di chiarimenti, deve fare riferimento al Responsabile o al Titolare del Trattamento.

Contesto normativo di riferimento:

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

Vengono riportate di seguito le definizioni, i riferimenti normativi ed i relativi considerando per una più chiara lettura e comprensione del GDPR.

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);
- «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;
- «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.

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

1. I dati personali sono (C39):
   - Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
   - 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»);
   - Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
   - 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»);
   - 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»);
   - 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);

Liceità del trattamento (Articolo 6):

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.

2. 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):

- dal diritto dell'Unione; o

- 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)

- di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
- 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;
- 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 porta la definizione sotto riportata:

Trattamento di categorie particolari di dati personali (Articolo 9):

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)

Trattamento dei dati personali relativi a condanne penali e reati (Articolo 10)

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.

Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (Art. 2-ter)

1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento e' costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e' ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e puo' essere iniziata se e' decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalita' sono ammesse unicamente se previste ai sensi del comma 1.

4. Si intende per:

- "comunicazione", il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante (Art. 2-sexies)

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

- accesso a documenti amministrativi e accesso civico;
- tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonche' rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalita';
- tenuta di registri pubblici relativi a beni immobili o mobili;
- tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
- cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonche' documentazione delle attivita' istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attivita' di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
- esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonche' l'accertamento delle cause di ineleggibilita', incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
- svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
- attivita' dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
- attivita' di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- conferimento di onorificenze e ricompense, riconoscimento della personalita' giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilita' e di professionalita' per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonche' rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- obiezione di coscienza;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
- attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
- attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonchè alle trasfusioni di sangue umano;
- compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonche' compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
- vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
- tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
- istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
- trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonche' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva.

3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies.

Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute (Art. 2-septies)

1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformita' alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.

2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 e' adottato con cadenza almeno biennale e tenendo conto:

- delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;
- dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;
- dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

3. Lo schema di provvedimento e' sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni.

4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a:

- contrassegni sui veicoli e accessi a zone a traffico limitato;
- profili organizzativi e gestionali in ambito sanitario;
- modalita' per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute;
- prescrizioni di medicinali.

5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalita' del trattamento e possono individuare, in conformita' a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati e' consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalita' per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonche' le eventuali altre misure necessarie a garantire i diritti degli interessati.

6. Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalita' di prevenzione, diagnosi e cura nonche' quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanita'. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del regolamento, o altre cautele specifiche.

7. Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo.

8. I dati personali di cui al comma 1 non possono essere diffusi.

Principi relativi al trattamento di dati relativi a condanne penali e reati (Art. 2-octies)

1. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorita' pubblica, e' consentito, ai sensi dell'articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonche' le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.

3. Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza e' consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

- l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;
- l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
- la verifica o l'accertamento dei requisiti di onorabilita', requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
- l'accertamento di responsabilita' in relazione a sinistri o eventi attinenti alla vita umana, nonchè la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attivita' assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
- l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
- l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza;
- l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosita' sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
- l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
- l) l'attuazione della disciplina in materia di attribuzione del rating di legalita' delle imprese ai sensi dell'articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27;
- m) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo.

4. Nei casi in cui le disposizioni di cui al comma 3 non individuano le garanzie appropriate per i diritti e le liberta' degli interessati, tali garanzie sono previste con il decreto di cui al comma 2.

5. Quando il trattamento dei dati di cui al presente articolo avviene sotto il controllo dell'autorita' pubblica si applicano le disposizioni previste dall'articolo 2-sexies.

6. Con il decreto di cui al comma 2 e' autorizzato il trattamento dei dati di cui all'articolo 10 del Regolamento, effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalita' organizzata, stipulati con il Ministero dell'interno o con le prefetture-UTG. In relazione a tali protocolli, il decreto di cui al comma 2 individua, le tipologie dei dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione e prevede le garanzie appropriate per i diritti e le liberta' degli interessati. Il decreto e' adottato, limitatamente agli ambiti di cui al presente comma, di concerto con il Ministro dell'interno.

Limitazioni ai diritti dell'interessato (Art. 2-undecies)

1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

- agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
- agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive; c) all'attivita' di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
- alle attivita' svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalita' inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonche' alla tutela della loro stabilita';
- allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

- alla riservatezza dell'identita' del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta.

3. Nei casi di cui al comma 1, lettere a), b), d), e) ed f) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti puo', in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalita' della limitazione, per il tempo e nei limiti in cui cio' costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e) ed f). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalita' di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonche' del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facolta' di cui al presente comma.

Limitazioni per ragioni di giustizia (Art. 2-duodecies)

1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonche' dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalita' previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento.

2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalita' della limitazione, nella misura e per il tempo in cui cio' costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.

3. Si applica l'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.

4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonche' i trattamenti svolti nell'ambito delle attivita' ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attivita' amministrativo-gestionale di personale, mezzi o strutture, quando non e' pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.

Diritti riguardanti le persone decedute (Art. 2-terdecies)

1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione.

2. L'esercizio dei diritti di cui al comma 1 non e' ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della societa' dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.

3. La volonta' dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto puo' riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.

5. In ogni caso, il divieto non puo' produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonche' del diritto di difendere in giudizio i propri interessi.

Attribuzione di funzioni e compiti a soggetti designati (Art. 2-quaterdecies)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilita' e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2. Il titolare o il responsabile del trattamento individuano le modalita' piu' opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorita' diretta.

Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico (Art. 2-quinquiesdecies)

1. Con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'articolo 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

Art. 59. Accesso a documenti amministrativi e accesso civico

1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. 1-bis. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.

Art. 60 (Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)

1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Istruzioni operative per il corretto trattamento dei dati

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.

AFFIDAMENTO AGLI INCARICATI DI DOCUMENTI, CONTENENTI DATI PERSONALI, E MODALITÀ DA OSSERVARE PER LA CUSTODIA DEGLI STESSI.

Trattamento Senza L'ausilio Di Strumenti Elettronici

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del Responsabile 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 Titolare e il Responsabile 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.
Nello svolgimento della propria mansione, ogni dipendente/collaboratore che trattata dati personali, siano essi identificativi o sensibili, con strumenti elettronici e non, deve adottare le precauzioni sotto riportate.

I SISTEMI INFORMATICI DELL'ENTE

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 e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'Ente il furto, danneggiamento o smarrimento di tali strumenti.
Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni disciplinari, la Pubblica Amministrazione 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 comunali.
In questo contesto la Pubblica Amministrazione potrà per necessità di sicurezza 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.

È consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete; compatibilmente con le esigenze dell'Agenzia in ordine alle prestazioni richieste tale possibilità è ammessa anche durante l'orario di lavoro.

All'utente non è consentito usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

Utilizzo del personal computer

- È consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal Responsabile; 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; è consentita l'installazione sul proprio PC di mezzi di comunicazione propri solo se espressamente autorizzati dal Titolare o dal Responsabile.
- 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'Ente 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.

Utilizzo di internet – regole generali

- Non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge.
- 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 del trattamento.
- Lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) può essere effettuato nel rispetto di dette normative.
- È 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.

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 dell'ente 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 dell'ente per la partecipazione a dibattiti, Forum o mail-list. Tale partecipazione può avvenire solo previa autorizzazione da parte del Titolare o del Responsabile del trattamento;
- Non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini dell'ente salvo diversa ed esplicita autorizzazione.

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 Responsabile per i dettagli operativi della procedura. Elaborare le password seguendo le istruzioni sotto riportate.

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.

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.

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.

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.

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. È 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.

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.

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)

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:

1. 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.

2. 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).

3. 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.

4. 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).

5. 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.

6. Eviti la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;

7. Non utilizzi i server di rete come stazioni di lavoro;

8. 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;

9. 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.

OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità lavorative 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 dell’ente, 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.

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'Ente 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.

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

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 dell'ente, 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 Responsabile o il Titolare.

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.

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:

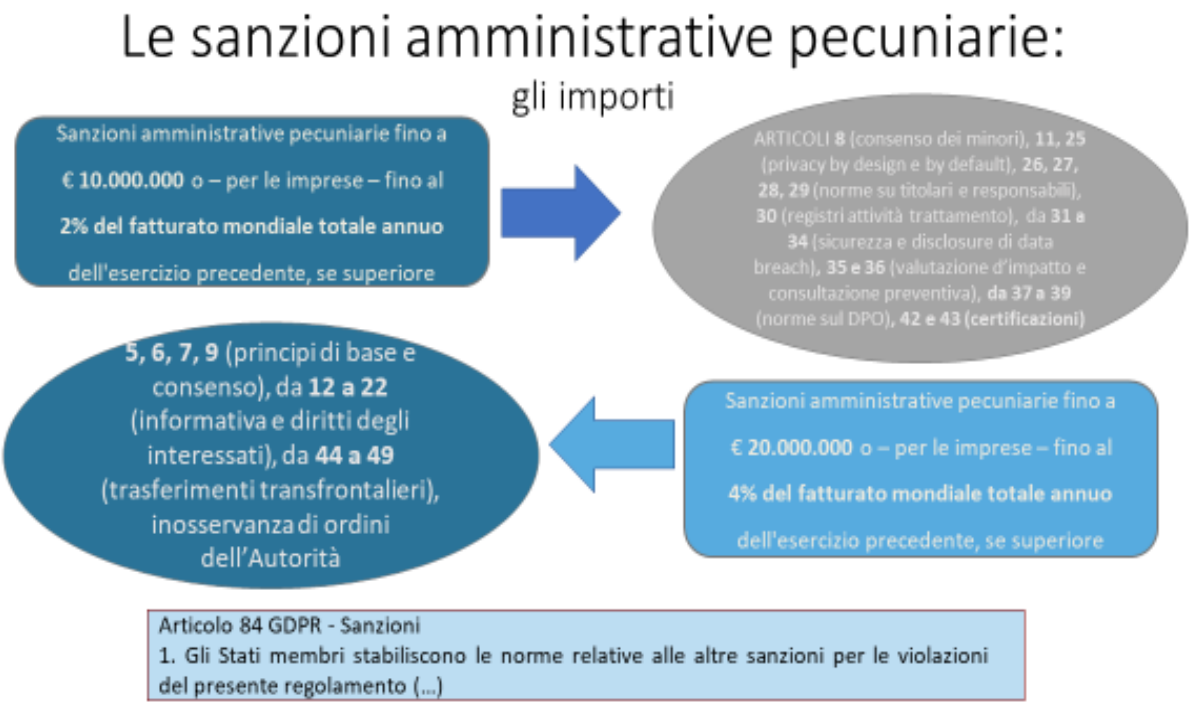
- I supporti rimovibili contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro 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.

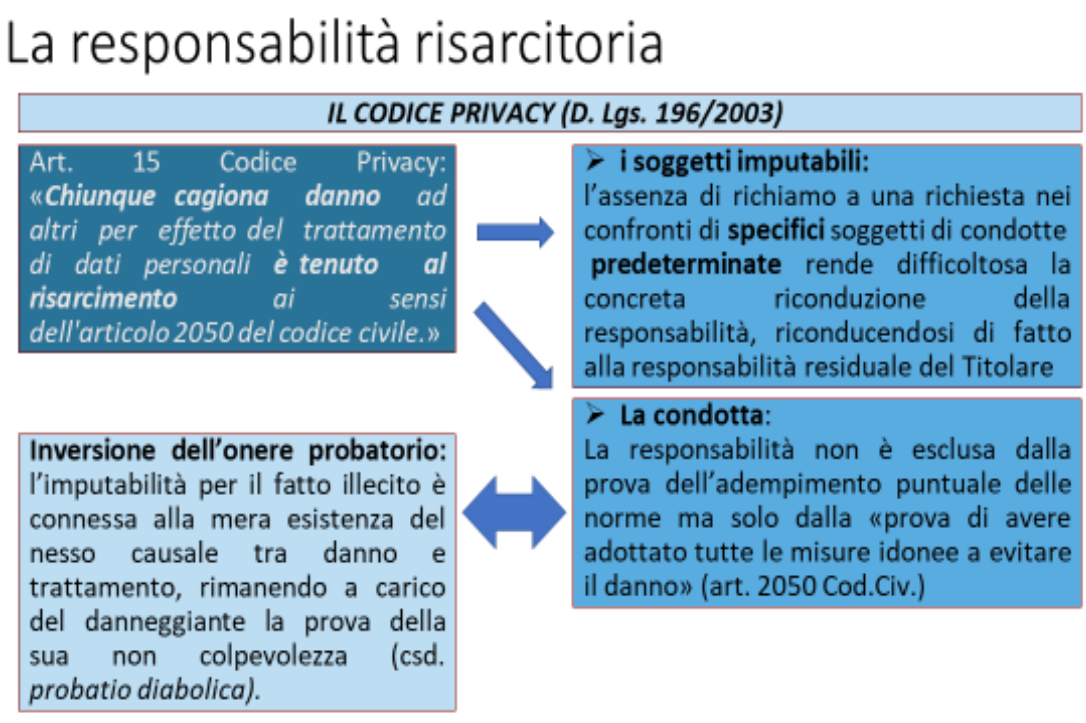
DOVERE DI AGGIORNARSI, UTILIZZANDO IL MATERIALE E GLI STRUMENTI FORNITI DALL'ORGANIZZAZIONE, ATTINENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

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 dal titolare.

Di seguito alcune slide sulle sanzioni del GDPR e sulla responsabilità





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

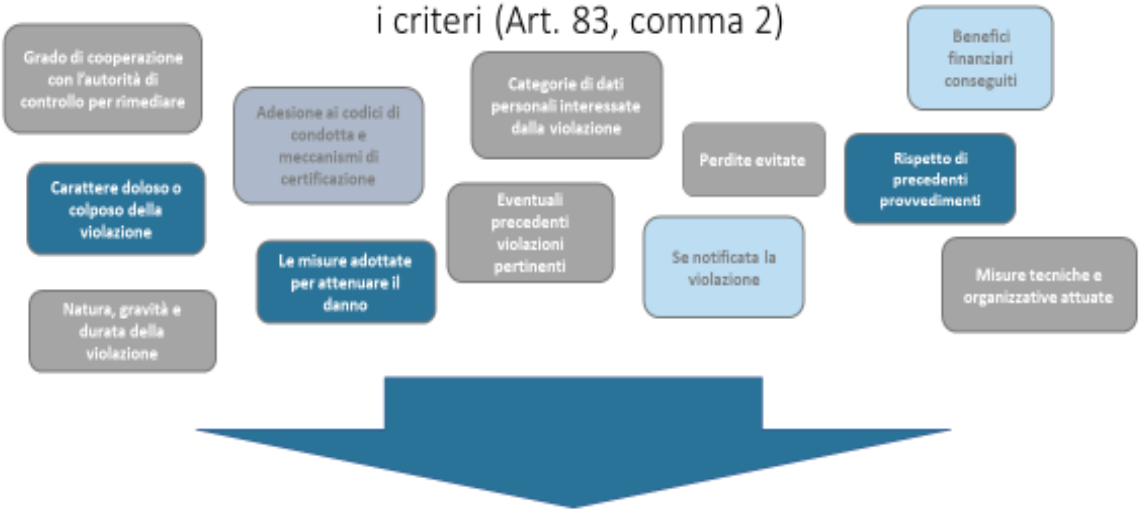
4% del fatturato
(od € 20.000.000,00)

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)



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