IL TRATTAMENTO DEI DATI PERSONALI
e
LA GESTIONE DELLA LORO SICUREZZA

aggiornamento 06/06/2018

contenuto

Il presente manuale si compone delle seguenti parti:

Il Regolamento UE n.679/2016 (General Data Protection Regulation)

- sintesi
- definizioni
- informazione e accesso ai dati personali
- diritti dell'interessato
- consenso
- sanzioni

Modulistica

- informative sul trattamento dei dati personali
- espressione del consenso
- contratti di servizio e fornitura e loro integrazioni

Adempimenti e prescrizioni

- Analisi del rischio
- Sicurezza dei dati personali
- Violazioni dei dati personali
- La Data Protection Impact Analysis (DPIA)
- Il Registro dei trattamenti
- Il Responsabile per la Protezione Dati (RPD)
- Sistemi di controllo interno

Altre cautele

- utilizzo della posta elettronica e di trasmissioni telefax

Il **Regolamento UE n.679/2016** (**G**eneral **D**ata **P**rotection **R**egulation), in vigore dal **25/05/2018**, disciplina il trattamento dei dati personali, la loro sicurezza; inoltre stabilisce i diritti degli interessati e i doveri dei titolari del trattamento.

presupposti	la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale	
	▪ assicurare la libera circolazione dei dati personali tra Stati membri ▪ prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno	
finalita	protezione delle persone fisiche con riguardo al trattamento dei dati personali *(diritto alla protezione dei dati personali)*	
	libera circolazione dei dati personali nell'Unione *(che non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali)*	
ambito di applicazione materiale	**si applica**	al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi
	non si applica	ai trattamenti di dati personali: a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.
	non pregiudica	l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva
ambito di applicazione territoriale	**si applica**	al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un Titolare del trattamento o di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione
	si applica	al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un Titolare del trattamento o da un Responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: - l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure - il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione
	si applica	al trattamento dei dati personali effettuato da un Titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico

definizioni

dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («**interessato**»)	si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione	
limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro	
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	
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	

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	
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	
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	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
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	
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	
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	
dati biometrici	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	

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	
stabilimento principale	il luogo della sua amministrazione centrale nell'Unione *(per un Titolare del trattamento con stabilimenti in più di uno Stato membro)*	salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale
	il luogo in cui ha sede la sua amministrazione centrale nell'Unione *(per un Responsabile del trattamento con stabilimenti in più di uno Stato membro)*	o, se il Responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento
rappresentante	la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;	
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	
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	

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: 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 de ltrattamento 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	
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	

Informazione e accesso ai dati personali

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato	a) l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal Titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.	**In aggiunta** a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
	Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.	le prescrizioni precedenti **non si applicano** se e nella misura in cui l'interessato dispone già delle informazioni.

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato	a) l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) le categorie di dati personali in questione; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del Titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.	**In aggiunta** a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal Titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
	Il Titolare del trattamento fornisce le informazioni di cui sopra a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.	

	Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.	I paragrafi sopracitati **non si applicano** se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto

diritti dell'interessato

Diritto di accesso dell'interessato	**1.** L'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.	**2.** Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. **3.** Il Titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il Titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. **4.** Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.
Diritto di rettifica	L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.	

Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il Titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 **non si applicano** nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Diritto di limitazione di trattamento	**1**. L'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato. **2**. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.	**3**. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal Titolare del trattamento prima che detta limitazione sia revocata.
Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento	Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.	

Diritto alla portabilità dei dati	**1.** L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati. **2.** Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.	**3.** L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento 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. **4.** Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.
Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche	**1**. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. **2**. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. **3**. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.	**4**. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
	5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione	

con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:

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

3. Nei casi di cui al paragrafo 2, lettere a) e c), il Titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

consenso

condizioni	Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
	Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
	L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
	Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.
consenso dei minori in relazione ai servizi della società dell'informazione	il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
	Il Titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

sanzioni

l'articolo 83 del Regolamento stabilisce le sanzioni e le condizioni per la loro applicazione:

condizioni

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento … siano in ogni singolo caso effettive, proporzionate e dissuasive.

Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle seguenti misure correttive dell'Autorità di Controllo o in luogo delle stesse

a) rivolgere avvertimenti al Titolare del trattamento o al Responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
b) rivolgere ammonimenti al Titolare e del trattamento o al Responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
c) ingiungere al Titolare del trattamento o al Responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
i) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal Titolare del trattamento o dal Responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del Titolare del trattamento o del Responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

	e) eventuali precedenti violazioni pertinenti commesse dal Titolare del trattamento o dal Responsabile del trattamento; f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il Titolare del trattamento o il Responsabile del trattamento ha notificato la violazione; i) il rispetto da parte del Titolare del trattamento o del Responsabile del trattamento in questione di provvedimenti di cui all'articolo 58, paragrafo 2, che siano stati precedentemente disposti relativamente allo stesso oggetto; j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.
	Se, in relazione allo stesso trattamento o a trattamenti collegati, un Titolare del trattamento o un Responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.
sanzioni	La violazione degli obblighi del Titolare del trattamento e del Responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43 del Regolamento è soggetta a sanzioni amministrative pecuniarie **fino a 10 000 000 EUR**, o per le imprese, **fino al 2 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.
	la violazione delle disposizioni seguenti: a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione d) internazionale a norma degli articoli da 44 a 49; e) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; f) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1 è soggetta a sanzioni amministrative pecuniarie **fino a 20 000 000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore
	L'inosservanza di un ordine da parte dell'Autorità di Controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie **fino a 20 000 000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore.

modulistica

Una adeguata e corretta gestione dei dati personali delle persone fisiche, richiede che vengano rese agli interessati opportune informazioni in merito alla raccolta e al trattamento dei dati. Le informazioni sono normalmente rese per iscritto o rese reperibili in rete, con accesso libero.
A tal fine devono essere redatte, secondo necessità:

a. **Informativa** da rendere a Clienti, Fornitori e parti correlate
b. **Informativa** da rendere a Dipendenti e Collaboratori

Per raccogliere il consenso al trattamento dei dati personali, in forma scritta o mediante applicazioni elettroniche, devono essere predisposti, secondo necessità:

a. modulo per la raccolta del **consenso informato** di Clienti, Fornitori e parti correlate
b. modulo per la raccolta del **consenso informato** di Dipendenti e Collaboratori

L'acquisto di servizi e lavorazioni esterne implicanti la trasmissione di dati personali riferiti a persone fisiche, devono essere assoggettati ad apposita pattuizione che preveda per la controparte il rispetto e l'applicazione della normativa vigente in materia di privacy e protezione dei dati personali.
Pertanto, i contratti stipulati con i fornitori di servizi e lavorazioni andranno, se necessario, integrati con apposite **sideletters** per richiedere alla controparte il rispetto e l'applicazione della normativa vigente in materia di privacy e protezione dei dati personali e ottenerne esplicito impegno.
Ove non esistenti, sarà necessario stipulare con le controparti **contratti di servizio** e **fornitura** perlomeno normanti il rispetto della privacy e la protezione dei dati personali.

Tale modulistica, predisposta e personalizzata secondo le necessità aziendali, viene fornita in formato elettronico al committente, per gli utilizzi che questi ne deve fare.

ATTENZIONE

I modelli e I formulari che saranno forniti sono specifici per l'Azienda che li ha commissionati, perchè elaborati tenendo conto delle sue specificità, così come sono state dalla stessa dichiarate in sede di predisposizione di questa applicazione. Pertanto essi

NON SONO UTILIZZABILI

da altre Aziende o Entità, anche se consociate o controllate dalla Committente, o comunque collegate ad essa. L'estensore declina ogni responsabilità in tal senso.

adempimenti e prescrizioni

Di seguito vengono fornite le necessarie indicazioni per svolgere gli **adempimenti** del Regolamento e affrontare le situazioni che si venissero a creare:

Analisi del rischio
Sicurezza dei dati personali
Violazioni dei dati personali
La Data Protection Impact Analysis (DPIA)
Il Registro dei trattamenti
Il Responsabile per la Protezione Dati (RPD)
Sistemi di controllo interno

Le indicazioni di cui sopra costituiscono una traccia operativa anche per la realizzazione da parte del Committente delle **prescrizioni** che gli saranno impartite.

analisi del rischio

A cura del Responsabile del Trattamento, deve essere periodicamente condotta una **attenta e approfondita analisi** in grado di valutare, nei termini e per gli effetti della normative vigente, tutto quanto concerne la raccolta e il trattamento dei dati personali in azienda.
Tale documentazione costituirà la prova dell'applicazione e del rispetto della normativa e darà evidenza del grado di *compliance* raggiunto.

Si inizierà col descrivere la **SITUAZIONE DI FATTO** in cui si trova l'Azienda, relativamente alla raccolta e alla gestione dei dati.
Poi si descriverà la **STRUTTURA** mediante la quale l'Azienda può venire in possesso di dati personali e effettuarne, completamente o parzialmente, il trattamento.
Si indicheranno gli eventuali **SERVIZI**, erogati e/o acquisiti, che possono comportare la raccolta o la trasmissione di dati personali.
Procedendo, si descriveranno chi sono gli **INTERESSATI** fornendo per ciascuna tipologia le informazioni ritenute significative circa l'attività di raccolta, la tipologia dei dati, il loro utilizzo e trattamento.
Si indichi poi chi ha **ACCESSO** ai dati personali e ne effettua il trattamento.
Quindi verranno elencati i principi in base ai quali l'Azienda effettua il **TRATTAMENTO** dei dati personali.
Successivamente si descriverà il **CONTESTO** entro il quale avviene il trattamento.
Dopo di che si esaminerà il **DATABASE** aziendale dei dati personali: quali dati ospita, per ciascuna delle categorie di interessati, da quale fonte o processo vengono tratti.
Quindi si procederà alla **CLASSIFICAZIONE** dei dati con riferimento alla *privacy* e verranno individuate le possibili **MINACCE** cui sono assoggettati.
Seguirà la valutazione del **RISCHIO** servendosi delle tabelle che seguono

matrice di valutazione del rischio

PROBABILITA	4	**4**	**8**	**12**	**16**
	3	**3**	**6**	**9**	**12**
	2	**2**	**4**	**6**	**8**
	1	**1**	**2**	**3**	**4**
		1	2	3	4
		DANNO			

attribuzione del livello o indice di rischio

Indice di Rischio	Rischio
IR = 1	**molto basso**
2 <= IR <= 3	**basso**
4 <= IR <= 8	**medio**
IR > 8	**alto**

determinando così, per ciascun dato e per ciascuna fonte, gli **indici di rischio.**

Si analizzerà poi l'**ACCETTABILITA** dei rischi individuati, secondo lo schema

matrice di accettabilità del rischio

4 Tollerabile	8 Significativo	12 Inaccettabile	16 Inaccettabile
3 Insignificante	6 Tollerabile	9 Significativo	12 Inaccettabile
2 Insignificante	4 Tollerabile	6 Tollerabile	8 Significativo
1 Insignificante	2 Insignificante	3 Insignificante	4 Tollerabile

in ragione del quale si esprimono le valutazioni e si prefigurano, di conseguenza, le azioni correttive eventualmente da adottarsi, utilizzando la seguente tabella

ponderazione del rischio

Indice di rischio	*rischio*	*valutazione*	***Azioni richieste***	*note*
IR = 1	INSIGNIFICANTE	Evento altamente improbabile perché l'accadimento considerato non ha alcuna attinenza con l'attività di business.	Non sono necessarie azioni di trattamento	
1 <= IR <=3	ACCETTABILE	Evento poco probabile e/o conseguenze del verificarsi dell'evento ritenute accettabili.	Non sono richiesti trattamenti addizionali rispetto a quelli già in essere.	Si possono implementare soluzioni migliorative che non richiedano costi aggiuntivi. E' necessario un monitoraggio per assicurare che i controlli ed i presidi in essere siano mantenuti.
4 <= IR <=8	MODERATO	Evento probabile e/o conseguenze del verificarsi dell'evento gravi.	Sono necessarie azioni di trattamento per ridurre il rischio	I trattamenti per la riduzione del rischio dovranno essere attuati con stanziamento di risorse economiche ed entro un breve periodo di tempo.
9 <= IR <=16	**NON ACCETTABILE**	Evento molto probabile e/o conseguenze del verificarsi dell'evento molto gravi o irreparabili.	Sono necessarie azioni di trattamento **immediate con stanziamento di tutte le risorse economiche disponibili.**	

Si procederà infine a valutare l'**operatività aziendale** in riferimento alla gestione delle informazioni.
Esaminando l'analisi condotta, scaturirà l'eventuale **Piano degli interventi** da adottarsi per la riduzione di rischi, avendo bene a mente che le azioni di correzione che possono essere prese in considerazione per la riduzione del rischio sono essenzialmente:

1. Formazione al personale
2. Modifica o creazione di una procedura operativa o di controllo
3. Progetto di miglioramento e/o piano di investimento

Per lo svolgimento e la stesura dell'analisi sono disponibili per il Committente files contenenti le tracce delle operazioni da svolgere.

sicurezza dei dati personali

Il Titolare del trattamento e il Responsabile del trattamento, quando nominato, deve mettere in atto misure tecniche e organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

codice di condotta da adottare

Il Titolare del trattamento e il Responsabile del trattamento si impegnano a

a) effettuare un trattamento corretto e trasparente dei dati personali
b) fornire adeguata informazione agli interessati
c) raccogliere il consenso degli interessati
d) consentire agli interessati l'esercizio dei propri diritti
e) istruire adeguatamente tutti i collaboratori che partecipano alla raccolta e al trattamento dei dati personali
f) mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento vigente
g) riesaminare periodicamente e aggiornare quando necessario le misure di cui al punto precedente
h) mettere 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; ciò in ordine alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità
i) garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche
j) attuare politiche adeguate in materia di protezione dei dati
k) notificare eventuali violazioni dei dati personali alle autorità di controllo e a comunicare tali violazioni dei dati personali all'interessato, nei tempi e nei modi previsti dalla legge
l) aderire ai codici di condotta promulgati o raccomandati dalle associazioni e dagli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento

Nello specifico, il Titolare del trattamento e il Responsabile del trattamento garantiscono quanto segue, adottando le opportune misure:

pseudonimizzazione e cifratura dei dati personali

I dati personali sono archiviati in modo destrutturato, ossia scomponendo la totalità dei dati riferiti a ciascun interessato in archivi diversi e distinti, lasciando al sistema informatico il compito di ricomporre la coerenza dei dati di ciascun interessato utilizzando opportuni codici o pseudonimi; in tal modo, se non si possiedono tutte le parti che compongono l'archivio, viene impedita la riconducibilità all'interessato dei dati che per qualsiasi motivo e in qualsiasi modo venissero sottratti o dispersi.

Ove sia necessario ricorrere all'uso di copie del database al fine di testare applicazioni, soluzioni informatiche e procedure operative, i dati personali saranno opportunamente mascherati e resi irriconoscibili (data masking).
I dati personali sono cifrati o crittografati con opportuno algoritmo in modo da impederne il riconoscimento qualora essi vengano illecitamente sottratti o intercettati da terzi soggetti.
Particolare attenzione deve essere posta alla sicurezza dei dati ospitati, anche temporaneamente, su dispositivi mobili quali:

- tablet, notebook e computer portatili
- chiavette USB, HD, SSD e altri dispositive di archiviazione di massa esterni
- contenitori remoti (in cloud) di dati
- tabulati destinati alla frequente consultazione locale (devono essere distrutti e vietati)

La cifratura dei dati e delle loro transazioni avverrà mediante:

- ❖ funzioni hash
- ❖ algoritmi a chiave simmetrica (AES)
- ❖ algoritmi a chiave asimmetrica

Ogniqualvolta saranno progettate nuove applicazioni o funzionalità del sistema, esse saranno progettate per la massima sicurezza dei dati, che sarà garantita per impostazione predefinita (default).

capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

Ogniqualvolta sia necessario avvalersi di terzi soggetti per il trattamento dei dati personali, il Titolare del trattamento ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento vigente e garantisca la tutela dei diritti dell'interessato.
Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il Responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.
I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che

a) vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
b) vincoli il Responsabile del trattamento a trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
c) garantisca, da parte del Responsabile incaricato, che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

d) prescriva che il Responsabile incaricato adotti tutte le misure richieste dalle leggi vigenti in materia di sicurezza dei dati personali;
e) prescriva che il Responsabile incaricato rispetti analoghe condizioni per ricorrere a un altro Responsabile del trattamento;
f) prescriva che il Responsabile incaricato utilizzi misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
g) prescriva che il Responsabile incaricato assista il Titolare del trattamento nel garantire il rispetto degli obblighi in ordine alla sicurezza dei dati, alla notifica delle violazioni e alla valutazione d'impatto, compresa la consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento;
h) imponga che il Responsabile incaricato, su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
i) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge; consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

Il Titolare del trattamento e i Responsabili del trattamento devono adottare tutte le misure necessarie affichè in caso di incidente fisico o tecnico la disponibilità e l'accesso dei dati personali siano ripristinati tempestivamente.

procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Il Titolare del trattamento e i Responsabili del trattamento devono adottare tutte le misure tecniche e organizzative necessarie per garantire la sicurezza del trattamento.
In particolare dovranno essere redatte e deliberate procedure che prevedano il test la verifica e l'efficacia delle misure tecniche adottate.

violazioni dei dati personali

notifica di una violazione dei dati personali all'autorità di controllo

In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Comunicazione di una violazione dei dati personali all'interessato

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.

La comunicazione, con un linguaggio semplice e chiaro:

a) descrive la natura della violazione dei dati personali;
b) comunica il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrive le probabili conseguenze della violazione dei dati personali;
d) descrive le misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negative

La comunicazione all'interessato non è richiesta qualora sia soddisfatta almeno una delle seguenti condizioni

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia

La Data Protection Impact Analysis (DPIA)

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.
Per tale valutazione il Titolare del trattamento si consulta con il Responsabile del trattamento, o con i diversi Responsabili se individuati.
La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata
b) su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
c) il trattamento, su larga scala, di categorie particolari di dati personali quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o di dati relativi a condanne penali e a reati o a connesse misure di sicurezza;
d) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
e) altre tipologie di trattamento soggette al requisito di una valutazione d'impatto sulla protezione dei dati come stabilito dall'Autorità di controllo.

La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento per la protezione dei dati personali, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare del trattamento procede, se necessario, a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati.

Consultazione dell'Autorità di controllo

Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta un elevato rischio residuale, il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di controllo, comunicando:

a) ove applicabile, le rispettive responsabilità del Titolare del trattamento, dei contitolari del trattamento e dei Responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del Regolamento;
d) ove applicabile, i dati di contatto del Titolare della protezione dei dati;
e) la valutazione d'impatto sulla protezione dei dati eseguita;
f) ogni altra informazione richiesta dall'Autorità di controllo.

i Registri dei trattamenti

Se il trattamento che viene effettuato

- può presentare un rischio per i diritti e le libertà dell'interessato
- non è occasionale,
  oppure
- include il trattamento di categorie particolari di dati quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o di dati relativi a condanne penali e a reati o a connesse misure di sicurezza

e, *tassativamente*,

- se l'impresa o l'organizzazione ha oltre 250 dipendenti,

il Titolare del trattamento e il Responsabile del trattamento tengono ciascuno un **registro delle attività di trattamento svolte** sotto la propria responsabilità.

il registro del Titolare del trattamento

il Titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro che contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del Responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti in mancanza di decisione di adeguatezza, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative relative a:
   1. la pseudonimizzazione e la cifratura dei dati personali;
   2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   4. procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

il registro del Responsabile del trattamento

Il Responsabile del trattamento e, ove applicabile, il suo rappresentante tengono **un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare** del trattamento, contenente:

a) il nome e i dati di contatto del Responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti in mancanza di decisione di adeguatezza, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative relative a:
    1. la pseudonimizzazione e la cifratura dei dati personali;
    2. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    3. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    4. procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Ogni registro è tenuto in forma scritta, anche in formato elettronico e, se richiesto, viene messo a disposizione dell'Autorità di controllo.
Ogni registro

- deve tenere traccia in modo adeguato di tutte le operazioni di trattamento effettuate all'interno della singola organizzazione;
- deve costituire uno strumento operativo di lavoro, per censire le raccolte di dati esistenti in azienda e che deve tenersi sincronizzato con la evoluzione di queste;
- rappresenta anche un documento probatorio con il quale il titolare dei dati può dimostrare, ad esempio, in caso di ispezione, di avere adempiuto alle prescrizioni del GDPR;
- può contenere informazioni ulteriori rispetto a quelle obbligatorie sulla base del GDPR e può essere costituito da più moduli, per poter individuare i trattamenti, gli addetti e gli applicativi/servizi di riferimento;
- deve essere inserito in un processo di gestione per poter essere adeguato ed allo stesso tempo utile.

La costruzione di un registro è operazione complessa che pertanto va affrontata con una trattazione specifica, nel caso in cui si sia ravvisato l'obbligo o l'opportunità della sua tenuta.

L'obbligatorietà o meno dei registri del trattamento, cosi come la loro spontanea adozione, devono essere menzionate al termine della analisi del rischio.

il Responsabile per la protezione dei dati (RPD)

Il Titolare del trattamento e il Responsabile del trattamento, se nominato, devono designare un **Responsabile per la protezione dei dati** (**RPD**) se:

a) vengono effettuati trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
b) viene effettuato il trattamento, su larga scala, di categorie particolari di dati personali quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o di dati relativi a condanne penali e a reati o a connesse misure di sicurezza;

Il Responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i seguenti compiti

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'Autorità di controllo;
e) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva in sede di valutazione d'impatto sulla protezione dei dati, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il Responsabile della protezione dei dati può essere un dipendente del Titolare del trattamento o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. I suoi dati di contatto devono essere pubblici e comunicati all'Autorità di controllo.

Il Responsabile della protezione dei dati è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, dispone delle risorse necessarie per assolvere ai suoi compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. Il Responsabile della protezione dei dati non è rimosso o penalizzato dal Titolare del trattamento o dal Responsabile del trattamento per

l'adempimento dei propri compiti, e riferisce direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento.
Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.
Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
Il Responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il Titolare del trattamento o il Responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.
Il Responsabile della protezione dei dati è l'autorità di controllo interna e pertanto deve operare in modo indipendente.

L'obbligatorietà o meno del Responsabile per la protezione dei dati (RPD), cosi come la sua spontanea nomina, devono essere menzionate al termine della analisi del rischio.

Sistemi di controllo interno

E' possible adottare sistemi di controllo interno al fine di migliorare e governare la compliance al Regolamento.
In base al fine desiderato i sistemi di controllo interno sono implementati e condotti mediante:

Deleghe	*per circoscrivere e definire le responsabilità in ordine agli adempimenti prescritti dal GDPR ed altre disposizioni*
Procedure	*per definire processi e regole da seguire per garantire il rispetto dal GDPR ed altre disposizioni*
Internal audit	*per valutare l'esistenza, l'adeguatezza e l'effettiva applicazione di un sistema di controllo interno per la protezione dei dati personali*
Disciplinare	*per sanzionare il mancato rispetto delle prescrizioni del GDPR ed altre disposizioni e procedure aziendali*

L'adozione di questi sistemi, salvo situazioni di stringente necessità, è lasciata alla volontà del Titolare del trattamento e la loro eventuale definizione ed implementazione è demandata ad uno specifico intervento.
L'adozione di questi sistemi deve essere menzionata nell'analisi del rischio.

altre cautele

Di seguito vengono fornite alcune indicazioni di cautela e responsabilizzazione ai sensi del Regolamento da utilizzarsi nelle attività quotidiane che seguono:

utilizzo della posta elettronica e di trasmissioni telefax

Le indicazioni di cui sopra costituiscono una traccia operativa per la realizzazione da parte del Committente di *best practices* che dovrebbero essere diligentemente osservate, indipendentemente e a prescindere dalle prescrizioni che impartite.

utilizzo della posta elettronica e di trasmissioni telefax

Il quotidiano utilizzo della posta elettronica e di trasmissioni telefax, per la natura stessa dei mezzi utilizzati, espone i mittenti a diversi rischi, tra i quali la violazione dei dati personali, e alle conseguenze derivanti.
Ricordando che il Regolamento in oggetto si fonda sulla responsabilizzazione ed inoltre prescrive precisi adempimenti in caso di violazione dei dati personali, è necessario non solo prestare la massima attenzione all'invio dei messaggi, verificare i destinatari e l'esattezza dei loro indirizzi e numeri telefonici, da digitarsi e comporsi senza errori, ma anche aggiungere in calce dei messaggi stessi un *disclaimer* in accordo con le prescrizioni del presente regolamento.
Il testo da utilizzarsi per i messaggi di posta elettronica, può essere il seguente

> Questa e-mail e tutti i file trasmessi con essa sono confidenziali e possono contenere informazioni privilegiate o riservate. Essa è destinata esclusivamente alla persona o all'entità a cui è indirizzata. Qualsiasi distribuzione, utilizzo o copia di questa e-mail o delle informazioni in essa contenute da parte di un destinatario diverso è severamente vietata e potrebbe essere illegale.
> Chiunque ricevesse questa comunicazione per errore o, non autorizzato, ne venisse in possesso è pregato di **informare tempestivamente il mittente** ed eliminare immediatamente il materiale da qualsiasi computer o archivio.
> Dei contenuti della presente comunicazione è responsabile il mittente sopra indicato; ciononostante, tenuto conto del mezzo utilizzato, egli non si assume alcuna responsabilità in ordine alla segretezza e riservatezza delle informazioni contenute nella presente comunicazione, così come per ogni e qualsiasi danno o perdita derivanti dal suo ricevimento o utilizzo. Il mittente declina ogni responsabilità per le modifiche apportate a questo messaggio o alle informazioni in esso contenute dopo la sua spedizione.

Esso contiene anche generici richiami a responsabilità civili e penali, ma si consiglia vivamente di consultare anche il proprio legale nel caso in cui i dati e le informazioni che abitualmente vengono trasmessi possano produrre, in caso di trasmissione errata, serie conseguenze legali e ingenti danni.

Il testo è facilmente adattabile alle comunicazioni a mezzo telefax, e per una sua migliore comprensione può essere tradotto anche nella lingua degli abituali destinatari ovvero in una lingua universalmente utilizzata quale, ad esempio, l'inglese.

Qualora si ricevesse un avviso o una notizia di errato recapito del messaggio, il presente Regolamento impone che **vengano messe in atto le misure** previste in caso di **violazioni dei dati personali** come esposto nella omonima sezione di questo manuale.