

# Manuale del Sistema di Gestione per la Protezione dei dati personali Agenzia delle entrate-Riscossione

<b>REDAZIONE</b>	UFFICIO PRIVACY E QUALITÀ	FABIO ESPOSITO
<b>VERIFICA</b>	RDP	FABIO ESPOSITO
<b>APPROVAZIONE</b>	PRESIDENTE DETERMINAZIONE N. 21 DEL 11/06/2018	ERNESTO MARIA RUFFINI
<b>VERSIONE</b>	v.1.0	
<b>VALIDITÀ</b>	DATA DI DECORRENZA DEL DOCUMENTO: 14/06/2018	

## Diffusione del documento

LISTA DI DIFFUSIONE
Tutto il Personale di Agenzia delle Entrate - Riscossione

DESTINATARI DELLA PROCEDURA
Tutto il Personale di Agenzia delle Entrate - Riscossione

## INDICE

<b>PREMESSA, DEFINIZIONI, RIFERIMENTI NORMATIVI .....</b>	<b>4</b>
Premessa .....	4
Regolamento Europeo 679/2016 (General Data Protection Regulation-GDPR) .....	5
Definizioni.....	8
Riferimenti normativi .....	12
<b>SEZIONE 1 – SISTEMA DI GESTIONE PER LA PROTEZIONE DATI PERSONALI .....</b>	<b>13</b>
1.1. Il sistema documentale del SGPD .....	15
<b>SEZIONE 2 – ACCOUNTABILITY (RESPONSABILIZZAZIONE) .....</b>	<b>17</b>
2.1 Figure di responsabilità in materia di protezione dati personali previste dal GDPR .....	17
2.1.1 Titolare del trattamento .....	18
2.1.2 Responsabile della Protezione dei dati (RPD) o Data Protection Officer (DPO) .....	18
2.1.3 Autorizzati al trattamento .....	20
2.1.4 Responsabili esterni del trattamento .....	21
2.2 Responsabilità attribuite all'interno del Sistema di Gestione per la Protezione dei dati .....	22
<b>SEZIONE 3 – MODELLO OPERATIVO .....</b>	<b>26</b>
3.1. Registro delle attività di trattamento .....	28
3.2. Informativa agli interessati .....	29
3.3. Diritti degli interessati .....	29
3.4. Violazione dei dati personali (data breach) .....	32
3.5. Privacy by design e privacy by default .....	33
3.5.1. Coinvolgimento del RPD e degli <i>stakeholders</i> .....	34
3.5.2. Descrizione delle caratteristiche del trattamento .....	35
3.5.3. Valutazione dei rischi e delle misure di sicurezza .....	36
3.5.4. Aggiornamento del Registro delle attività di trattamento .....	37
3.6. Data Protection Impact Assessment (DPIA) .....	37
3.7. Verifica e monitoraggio della compliance del Sistema .....	38
3.7.1. Sistemi di audit .....	39
3.7.2. Documenti di riesame .....	39
3.8. Relazione sullo stato di attuazione del sistema di protezione dei dati .....	40

## Indice delle sezioni del Manuale

Di seguito è riportato l'indice delle sezioni che compongono il Manuale del Sistema di Gestione per la protezione dei dati personali di Agenzia delle entrate – Riscossione con i relativi indici di revisione, la data di emissione e i riferimenti al Regolamento generale sulla protezione dei dati n. 679/2016 (cd. GDPR).

Manuale	Titolo	Rev	Data	GDPR
0	PREMESSA, DEFINIZIONI, RIFERIMENTI NORMATIVI	1	01/06/2018	--
1	IL SISTEMA DI GESTIONE PER LA PROTEZIONE DEI DATI PERSONALI	1	01/06/2018	--
2	ACCOUNTABILITY	1	01/06/2018	--
3	Modello operativo	1	01/06/2018	--

## Storia delle revisioni

Sez.	Rev.	Data	Parte revisionate

## PREMESSA, DEFINIZIONI, RIFERIMENTI NORMATIVI

### Premessa

Agenzia delle entrate - Riscossione, di seguito denominata "Agenzia" (o "Agente della riscossione" o "Ente"), è un Ente pubblico economico istituito ai sensi dell'articolo 1 del decreto-legge 22 ottobre 2016, n. 193, convertito con modificazioni, dalla legge 1° dicembre 2016, n. 225, e svolge le funzioni concernenti la riscossione nazionale e tutte le funzioni e i compiti ad essa attribuiti dalle previsioni normative vigenti.

L'Agenzia persegue l'obiettivo primario di favorire il regolare adempimento delle obbligazioni da parte dei contribuenti in modo da garantire, al contempo, l'esatta osservanza della legge, la massima efficienza della propria organizzazione e la corretta percezione della funzione delle entrate pubbliche come vantaggio esclusivo della collettività.

L'Agenzia opera con criteri di efficienza gestionale, economicità dell'attività ed efficacia dell'azione al fine di perseguire gli obiettivi prestabiliti (tra i quali quelli di cui all'atto aggiuntivo previsto all'articolo 1, comma 13, del decreto legge n. 193 del 2016) e garantendo, altresì, la trasparenza degli obiettivi stessi, dell'attività svolta e dei risultati conseguiti.

Come previsto nello Statuto, approvato con decreto del Presidente del Consiglio dei Ministri 5 giugno 2017, l'Agenzia ha autonomia organizzativa, patrimoniale, contabile e di gestione e adotta propri regolamenti di amministrazione e di contabilità.

Sono organi dell'Agenzia il Presidente, il Comitato di gestione e il Collegio dei revisori dei conti che esercitano le attribuzioni loro demandate dall'articolo 1 del decreto-legge 22 ottobre 2016, n. 193, convertito, con modificazioni, della legge 1 dicembre 2016, n. 225 e meglio esplicitate nello Statuto.

Il Comitato di gestione è composto da un Presidente identificato nel Direttore dell'Agenzia delle entrate (che assume anche il ruolo di Presidente di Agenzia delle entrate-Riscossione) e da due componenti nominati dall'Agenzia medesima tra i propri dirigenti. Il Presidente del Collegio dei revisori dei conti è scelto tra i magistrati della Corte dei conti.

Dal punto di vista della macrostruttura organizzativa, l'Agenzia si articola in:

- strutture centrali, con funzioni prevalenti di programmazione, indirizzo, coordinamento e controllo, nonché di erogazione di servizi gestionali-operativi accentrati;

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

- strutture regionali, organizzate con logica di presidio territoriale-geografico e con funzioni di gestione e coordinamento delle relative attività operative correlate alla riscossione.

La documentazione organizzativa dell'Agenzia è disponibile, con i relativi aggiornamenti, all'interno della [intranet aziendale](#).

### **Regolamento Europeo 679/2016 (General Data Protection Regulation-GDPR)**

Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento UE 2016/679 (di seguito anche "Regolamento" o "GDPR"), relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Al seguente link è possibile scaricare il testo completo del [Regolamento \(UE\) 2016/679](#).

Il Regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri della UE e trova applicazione a far data dal **25 maggio 2018** (cfr. art. 99 del Regolamento). La disciplina trova applicazione in riferimento al trattamento dei dati personali relativi alle persone fisiche.

I principi e le norme a tutela delle persone fisiche espresse all'interno del Regolamento, sono definite al fine di rispettarne i diritti e le libertà fondamentali con particolare riferimento al diritto alla protezione dei dati personali (Considerando 2). La prosecuzione dei processi di integrazione economica e sociale tra i Paesi dell'Unione, nonché la rapidità dell'evoluzione tecnologica, che hanno condotto ad un significativo aumento della condivisione e raccolta di dati personali (Considerando 5 e Considerando 6), hanno richiesto la definizione di un quadro normativo più solido e coerente in materia (Considerando 7).

Considerando l'opportunità che le persone fisiche abbiano il controllo dei dati personali che le riguardano (Considerando 7), un'efficace protezione degli stessi dati in tutta l'Unione Europea, presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali (Titolari e Responsabili del trattamento cfr. infra definizioni), nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri (Considerando 11).

L'art. 5 del Regolamento sancisce i principi applicabili al trattamento dei dati personali; in particolare i dati personali devono essere:

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

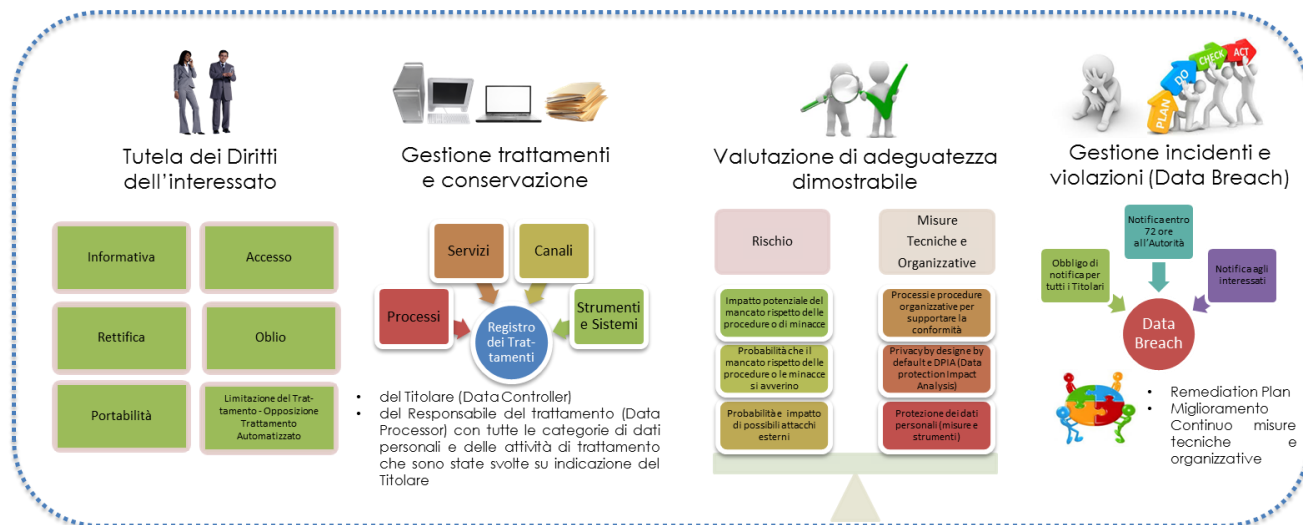
<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («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 («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Con riferimento agli obblighi di coloro che effettuano e determinano il trattamento di dati personali, l'art. 24 del Regolamento introduce il principio centrale di "accountability" (Responsabilizzazione) che, al comma 1, prevede: *"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"*.

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

## RESPONSABILIZZAZIONE DEL TITOLARE DEL TRATTAMENTO



**Fig.1. I principali elementi a supporto del principio di "Accountability"**

Nel quadro delle previsioni in materia di "accountability", il Regolamento richiede al Titolare del trattamento:

- **Trasparenza:** si richiede di fornire all'interessato tutte le informazioni (artt. 13-14) e le comunicazioni (artt. da 15 a 22 e 34) richieste dal Regolamento. Le richieste dell'interessato sono gestite al più tardi nel termine di 30 gg, secondo le specificazioni di cui all'art. 12 del Regolamento.
- **Gestione sistematica delle attività di trattamento:** oltre ad accertarsi che i dati personali raccolti siano utilizzati esclusivamente per finalità determinate, esplicite e legittime, il Titolare, che gestisce le attività di trattamento attraverso specifici registri (art. 30), può ricorrere unicamente a Responsabili esterni che presentino garanzie sufficienti per mettere in atto misure (tecniche e organizzative) per soddisfare i requisiti del regolamento e garantire la tutela dei diritti dell'interessato.
- **Bilanciamento:** si richiede la capacità di effettuare, in riferimento alle attività di trattamento, un'adeguata valutazione del rapporto tra rischi individuati (gestione basata sul rischio) e misure tecniche e organizzative adottate e di essere in grado di dimostrarlo.
- **Tempestività nella gestione delle notifiche delle violazioni:** si richiede che, in caso di violazione dei dati personali, il Titolare del trattamento notifichi la violazione all'autorità di controllo e, nei casi previsti, agli interessati senza ingiustificato ritardo (artt. 33 -34).

Il Regolamento rafforza in maniera significativa l'ammontare delle sanzioni in caso di violazione delle disposizioni ivi contenute, fissandone all'art.83, comma 5 il limite massimo a 20 milioni di euro.

## Definizioni

Ai fini del presente manuale si intende:

**Codice privacy:** il Decreto legislativo 30 giugno 2003, n. 196 recante il "*Codice in materia di protezione dei dati personali*".

**Dato personale:** qualsiasi informazione riguardante 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 e geografico.

**Archivio logico:** è una rappresentazione strutturata dell'informazione degli oggetti della realtà all'interno del sistema informatico; la sua realizzazione consiste nella traduzione dei dati di business, integrati dai vincoli tecnologici e dal modello logico prescelto, in oggetti logici all'interno del sistema informatico; gli oggetti sono idonei alla distinzione, dal punto di vista del business, delle diverse categorie di banche dati, coerenti con gli indirizzi strategici di circolarità dell'informazione e della cooperazione di servizi.

**Interessato:** la persona fisica a cui si riferiscono i dati personali.

**Trattamento:** qualsiasi operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insieme di dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione, o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

**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.

**WP29 (Working Party art.29):** Gruppo istituito dall'art. 29 della direttiva 95/46/CE. È un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione

dei dati), nonché da un rappresentante della Commissione. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al Comitato europeo per la protezione dei dati istituito dal Regolamento con l'art. 68 (cfr. art. 94 par. 2 del Regolamento).

**Autorità di controllo:** l'autorità pubblica indipendente prevista dall'art. 51 del Regolamento; l'Autorità pubblica di controllo italiana è il Garante per la protezione dei dati personali.

**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 un altro organismo che tratta dati personali per conto del Titolare del trattamento.

**Responsabile della protezione dei dati (RPD): o Data Protection Officer (DPO).** È il soggetto che deve essere obbligatoriamente nominato dal Titolare e dal Responsabile del trattamento quando ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali) oppure quando l'attività principale del Titolare o del Responsabile consista in trattamenti che per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

**Violazione di 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.

**Sistema di gestione (*management system*):** Insieme di elementi interrelati e interagenti di un'organizzazione per stabilire politiche e obiettivi e [insieme di] processi [interrelati e interagenti] per raggiungere tali obiettivi.

**Rischio:** scenario che descrive un evento e le sue conseguenze stimato in termini di gravità e probabilità.

**Gestione dei Rischi:** insieme delle attività coordinate volte ad indirizzare e controllare un'organizzazione in relazione ai rischi.

**Rischio residuo:** Il rischio residuo è il livello di rischio che permane dopo aver attuato interventi per ridurlo.

**Rischio inerente:** rischio massimo teorico, intrinseco al trattamento, nel caso in cui l'organizzazione non metta in atto specifiche attività o strategie di controllo/mitigazione.

**Analisi del rischio:** il processo di identificazione, di analisi in senso stretto e di risposta al rischio attraverso misure tecniche ed organizzative 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.

**Probabilità:** indica la possibilità che si verifichi un evento dannoso.

**Gravità:** conseguenza derivante dal concretizzarsi di un evento dannoso.

**Misure tecniche:** sono espressamente citate, insieme alle misure organizzative, dagli artt. 22 e 32 del Regolamento; per misure tecniche si intendono gli strumenti tecnici e tecnologici offerti dallo stato dell'arte della tecnologia disponibile (in particolare quella dei sistemi informatici) idonei a garantire un livello di sicurezza adeguato al rischio.

**Misure organizzative:** si intendono quelle che intervengono, in maniera più o meno formalizzata, sull'organizzazione degli strumenti di lavoro e del personale al fine di garantire in maniera permanente la protezione da un rischio. Le misure organizzative possono essere adottate anche ad integrazione o temporanea sostituzione (c.d. controlli compensativi) delle misure tecniche (vedasi voce dedicata). Le misure organizzative, insieme a quelle tecniche, devono essere adeguatamente documentate dal Titolare e/o dal Responsabile del Trattamento per poterne dimostrare la conformità al Regolamento. Più nello specifico, alcune delle misure tecniche e organizzative che il Titolare e il Responsabile del trattamento dei dati possono concretamente adottare sono elencate a titolo esemplificativo dal predetto art. 32.

**Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardante 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.

**Larga scala:** il trattamento effettuato su un elevato numero di soggetti e/o su un numero elevato di dati; l'eccessiva durata del trattamento ovvero la persistenza del trattamento; l'estensione geografica dell'attività di trattamento.

**Monitoraggio regolare:** il trattamento utilizzato per osservare, monitorare o controllare gli interessati che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo

definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici.

**Monitoraggio sistematico:** trattamento utilizzato per osservare, monitorare o controllare gli interessati il trattamento che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia.

**Privacy by default:** misure tecniche e organizzative adeguate, messe in atto dal Titolare, per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

**Privacy by design:** misure tecniche e organizzative adeguate, quali la pseudonimizzazione, messe in atto dal Titolare, volte ad attuare in modo efficace i principi di protezione dei dati quali la minimizzazione, sin dalla fase della progettazione, di un qualsiasi trattamento di dati.

**DPIA (Data Protection Impact Assessment) o valutazione d'impatto sulla protezione dei dati:** procedura che mira a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità ed a gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

**Minaccia:** una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale e corrisponde a scenari generali e specifici di rischio.

**Gap Analysis:** attività di analisi dell'attuale profilo di rischio rispetto a quello desiderato al fine di individuarne i punti di distanza (gap). Successivamente si stabilisce un *action plan* prioritizzato per indirizzare i gap individuati che attinge dagli obiettivi strategici, da un'analisi costi benefici e dall'analisi dei rischi con l'obiettivo di raggiungere il livello di rischio desiderato. L'organizzazione deve determinare le risorse necessarie per indirizzare i gap.

**Action Plan:** Piano che identifica le azioni da intraprendere per sanare uno o più gap. Un *action plan* dovrebbe indicare almeno: un Responsabile della sua realizzazione; una pianificazione degli interventi; le risorse necessarie alla realizzazione degli interventi; un processo per il monitoraggio dell'implementazione; un processo per il monitoraggio dell'efficacia.

**Particolari categorie di dati (dati sensibili e ipersensibili):** Dati personali idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza

sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute fisica o mentale (compresa la prestazione di servizi di assistenza sanitaria idonei a rilevare informazioni relativi allo stato di salute) o alla vita sessuale o all'orientamento sessuale della persona.

**Dati relativi a condanne penali e reati giudiziari:** Dati personali idonei a rivelare l'esistenza di condanne penali e reati o connesse misure di sicurezza.

**Dati genetici:** Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite dell'interessato di una persona fisica idonei a fornire informazioni univoche sulla fisiologia o sulla salute, 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, ad esempio, l'immagine facciale o i dati dattiloscopici.

**Dati finanziari:** dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.).

**Responsabili apicali delle strutture centrali/regionali:** sono per le strutture centrali - i Direttori Centrali e di Area; Direttori a Riporto dei Direttori di Area; i Responsabili delle Reti Territoriali; per le strutture regionali i Direttori Regionali.

## Riferimenti normativi

Nella redazione del presente Manuale di Gestione si è tenuto conto, in particolare, di quanto previsto dalle seguenti norme in materia di gestione dei documenti amministrativi e dei flussi documentali:

- legge 7 agosto 1990 n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- decreto legislativo 7 marzo 2005, n. 82 e s.m.i. - Codice dell'amministrazione digitale;
- decreto del Presidente Del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis), 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale;

- decreto del Presidente Del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis), 23 - ter), comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale.

## SEZIONE 1 – SISTEMA DI GESTIONE PER LA PROTEZIONE DATI PERSONALI

Revisioni	Data Modifica	Descrizione delle modifiche	Natura delle modifiche
1.0	__/__/2018		

Attraverso il principio di responsabilizzazione (*accountability*), il Regolamento introduce un **"approccio orientato al risultato"** in materia di protezione dei dati personali che si focalizza sul raggiungimento di obiettivi concreti di tutela dei diritti e delle libertà degli interessati.

Viene affidato al titolare il compito di decidere autonomamente **le modalità, le garanzie e i limiti del trattamento dei dati personali** – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento. Tale approccio, che costituisce un radicale cambiamento di prospettiva per le Organizzazioni, impone tuttavia specifici obblighi nel dimostrare in maniera costante l'adeguatezza delle scelte assunte.

Lo stesso Regolamento, inoltre, richiede che tali decisioni derivino da un'attenta e sistematica **gestione dei rischi** relativi tanto alla sicurezza dei dati personali gestiti dal titolare e dai responsabili, quanto alla tutela dei diritti e delle libertà delle persone fisiche interessate.

Ciò si sostanzia nella definizione di un modello di gestione della protezione dei dati personali basata, oltre che sulla puntuale applicazione di prescrizioni codificate, sulla **generale capacità da parte di ciascuna componente dell'Organizzazione, di assumere, quando necessario, le decisioni di competenza e intraprendere le azioni conseguenti come risultato di una corretta valutazione dei possibili effetti, positivi o negativi, degli eventi considerati.**

In definitiva la gestione del rischio per la protezione dei dati personali, si esprime a tutti i livelli della struttura organizzativa e del processo decisionale a:

- livello strategico: attraverso la considerazione dell'ambiente di contesto e delle sue sollecitazioni, attuali e potenziali, sul complessivo funzionamento organizzativo e sulla sostenibilità del modello applicativo proposto;
- livello tattico: attraverso una adeguata determinazione di processi organizzativi, di sistemi operativi e strumenti specifici che supportano la protezione dei dati personali;
- livello operativo: attraverso l'identificazione di punti o aree critiche nei processi organizzativi di funzionamento, nelle funzioni e nelle attività al fine del loro controllo.

**L'Agenzia delle Entrate Riscossione, in qualità di Titolare del trattamento dei dati, pianifica (Plan), realizza (Do), monitora (Check) e migliora (Act) - secondo il cd. Ciclo di Deming o PDCA - le modalità, le garanzie ed i limiti ai trattamenti dei dati personali che effettua per il conseguimento delle finalità istituzionali della riscossione nazionale dei tributi che le sono affidate dalla normativa di settore, attraverso l'adozione del proprio Sistema di Gestione per la Protezione dei Dati Personali (SGDP).**

In particolare, l'Ente cura la protezione dei dati personali anche considerando:

- la natura, l'organizzazione e il funzionamento del settore in cui opera;
- le variazioni del contesto, della normativa cogente e dei requisiti delle parti interessate (portatori d'interesse o *stakeholders*).

Tali elementi consentono all'Agenzia delle entrate-Riscossione di definire un profilo caratteristico di funzionamento per il proprio SGPD, che esprime requisiti specifici per:

- a) identificare e applicare correttamente le previsioni del Regolamento e della normativa vigente in materia di protezione dei dati personali;
- b) progettare la protezione dei dati (cd. *privacy by design*) e adeguare (cd. *privacy by default*) i processi organizzativi che trattano dati personali e i sistemi e gli strumenti a loro supporto, considerando i rischi per la sicurezza e per i diritti e le libertà degli interessati.

L'applicazione di tale requisito del Sistema consente:

- l'individuazione dei processi/attività critici per la protezione dei dati e una loro conseguente gestione secondo priorità;
- la determinazione dei passaggi da sottoporre a controllo (input, vincoli, risorse e strumenti a disposizione, output) nelle attività di trattamento;
- il controllo dell'assunzione di responsabilità nelle decisioni di trattamento;
- la migliore gestione delle informazioni, incluse quelle necessarie a documentare il rispetto dei criteri richiesti per il trattamento dei dati.

- c) la selezione e conduzione delle attività di audit (tali aree di attenzione variano in funzione dei mutamenti del contesto in cui l'Ente opera);
- d) la ponderazione, in riferimento ai rischi specifici presenti in AdeR, delle situazioni di non conformità rispetto a quanto pianificato e la conseguente attivazione delle iniziative di miglioramento.

L'Ente ritiene che la **partecipazione attiva e responsabile** dell'intera Organizzazione al miglioramento continuo della protezione dei dati personali degli interessati, sia un fattore strategico correlato alla funzione istituzionale svolta e che questo costituisca un importante obiettivo di Agenzia delle entrate – Riscossione.

Ciò anche al fine di favorire la diffusione di un clima di fiducia da parte dei cittadini nella corretta e trasparente gestione dei dati personali da parte di Agenzia delle entrate-Riscossione per lo svolgimento delle attività istituzionali di riscossione.

### 1.1. Il sistema documentale del SGPD

Il presente Manuale è parte integrante della documentazione di sistema (cd sistema documentale del SGPD) e ha lo scopo di individuare, in coerenza con il Modello organizzativo ed il funzionigramma di Agenzia delle entrate-Riscossione, i ruoli e le responsabilità dei diversi attori coinvolti, specificando le principali modalità di coordinamento tra le strutture per presidiare gli obblighi e realizzare gli obiettivi dell'Agenzia in materia di protezione dei dati personali trattati.

Il Manuale, inoltre, descrive le politiche, il funzionamento del sistema stesso, comprese le modalità di monitoraggio, verifica e riesame realizzate e sottoposte all'Alta Direzione.

Altre componenti del Sistema sono le seguenti:

- **modello organizzativo dell'Agenzia** con la necessaria integrazione dei compiti richiesti in materia di protezione dei dati personali (descritti nel presente Manuale);
- le **Misure Tecniche e Organizzative** predisposte per assicurare l'adeguatezza del trattamento dei dati ai principi del Regolamento, ivi incluse le regole di "disciplina dell'utilizzo degli strumenti elettronici, degli accessi alle risorse e ai dati di Agenzia delle entrate-Riscossione";
- le **procedure gestionali** dell'SGPD che, tra l'altro, descrivono le modalità con le quali l'Ente integra i principi della privacy by design, effettua la valutazione dei rischi

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

(comprese le modalità con le quali si attua la *Data Protection Impact Assessment*) e gestisce gli episodi di violazione dei dati personali (*data breach*);

- la **modulistica** e le **registrazioni** del Sistema di gestione.

I documenti del SGPD sono predisposti e aggiornati dall'Ufficio Privacy e Qualità, verificati dal Responsabile della Protezione Dati ed approvati dal Presidente. La distribuzione di detta documentazione in versione aggiornata è a cura dell'Ufficio Privacy e Qualità, avviene attraverso la pubblicazione sulla rete Intranet dell'Agenzia.

La documentazione a supporto dell'operatività dei processi è invece gestita attraverso il Sistema Normativo dell'Agenzia (SNA); i documenti del SNA che supportano l'attuazione dei processi sono contenute nell'apposita sezione intranet "Normativa/Sistema Normativo Agenzia" dove è possibile consultare la documentazione anche attraverso appositi filtri rispetto alla tipologia (circolare/direttive, Note informative, etc.) o al tipo di processo (governo, supporto, operativo). La manutenzione del Sistema Normativo dell'Agenzia è gestita dalla Direzione Organizzazione e Processi.

Titolare, attraverso il suo Presidente e con il supporto del Responsabile della Protezione dati, riesamina con frequenza almeno annuale, anche nel corso di riunioni di Direzione con i responsabili dei processi dell'Agenzia (cd *Process Owner*), il Sistema di Gestione per Protezione dei dati personali per valutarne l'idoneità, l'efficacia e l'efficienza nel tempo, oltre che la sua capacità di raggiungere, in coerenza con le politiche assunte, gli obiettivi in materia.

Per ogni eventuale esigenza di supporto o per la segnalazione di criticità nella gestione delle attività di trattamento è possibile scrivere al seguente indirizzo di posta elettronica: [protezione.dati@agenziaiscossione.gov.it](mailto:protezione.dati@agenziaiscossione.gov.it)

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

## SEZIONE 2 – ACCOUNTABILITY (RESPONSABILIZZAZIONE)

Revisioni	Data Modifica	Descrizione delle modifiche	Natura delle modifiche
1.0	__/__/2018		

Nell'ottica di assicurare un modello di gestione attivo, diffuso e responsabile dell'intera Organizzazione alla protezione dei dati personali, **ciascun dipendente**, a prescindere dal ruolo ricoperto, è tenuto a:

- rispettare i principi generali e le prescrizioni della normativa in materia di protezione dei dati personali e ad adeguare i propri comportamenti a quanto previsto dalle policy definite dall'Ente, dalle norme comportamentali e dalle procedure tecnico-organizzative;
- accedere esclusivamente ai dati necessari all'esercizio delle proprie funzioni e compiti;
- trattare i dati personali relativamente all'ambito di operatività assegnato, nei limiti della pertinenza, completezza e non eccedenza rispetto alle finalità per cui sono raccolti e trattati;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso delle attività svolte;
- utilizzare i dati ai quali ha accesso e per i quali è autorizzato al trattamento solamente per finalità compatibili all'esecuzione dei compiti affidati;
- rispettare le misure di sicurezza, atte a salvaguardare la protezione, riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, violazioni o perdite di dati;
- proporre miglioramenti al sistema.

### 2.1 Figure di responsabilità in materia di protezione dati personali previste dal GDPR

Il Regolamento europeo identifica le seguenti figure di responsabilità coinvolte nella Protezione dei dati personali in Agenzia delle entrate – Riscossione.

### 2.1.1 Titolare del trattamento

L'Agenzia delle entrate Riscossione assume la qualità di Titolare dei trattamenti dei dati personali. La realizzazione degli obblighi per l'adeguamento alle previsioni del Regolamento viene effettuata, per competenza rispetto ai processi organizzativi presidiati, dai Responsabili delle strutture.

Sono contitolari del trattamento ai sensi dell'art.26 del Regolamento due o più soggetti che determinano congiuntamente le finalità ed i mezzi del trattamento.

### 2.1.2 Responsabile della Protezione dei dati (RPD) o *Data Protection Officer (DPO)*

I compiti attribuiti al RPD, in coerenza con quanto previsto dall'art. 39 del Regolamento, sono:

- informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché dalle altre normative, anche europee, in materia di protezione dei dati, comprese le procedure operative definite dall'Ente;
- sorvegliare l'osservanza del Regolamento e di tutta la della normativa, nonché delle politiche dell'Agenzia in merito al trattamento dei dati 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;
- cooperare con il Garante per la Protezione dei Dati Personali (di seguito anche "Garante" o "Autorità di controllo") e fungere da punto contatto con lo stesso per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- fornire, se richiesto, un parere circa la valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento.

Il RPD svolge i compiti assegnati considerando debitamente i rischi inerenti al trattamento (tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo), in autonomia e indipendenza, riferendo direttamente al Titolare del trattamento, osservando gli obblighi di segretezza e riservatezza in merito all'adempimento dei propri compiti.

Il RPD, inoltre, presidia il Sistema di Gestione per la protezione dei dati descritto nel presente Manuale e, in questo ambito:

- cura l'aggiornamento della documentazione del Sistema composta dal presente Manuale e dalle procedure operative previste dal Sistema;
- supporta le strutture, fornendo consulenza, nella definizione delle modalità di trattamento dei dati personali nella realizzazione dei processi/servizi (*privacy by design*), sia in fase di prima progettazione che di aggiornamento;
- fornisce consulenza nella gestione delle violazioni dei dati personali (*data breach*);
- fornisce consulenza nella risposta alle istanze presentate dagli interessati, comprese quelle finalizzate all'esercizio dei diritti previsti dagli artt. 13-22 del Regolamento.

I dati di contatto del RPD sono pubblicati sul sito istituzionale dell'Agenzia e comunicati al Garante per la Protezione dei Dati Personali (art. 37, paragrafo 7, del Regolamento).

Il RPD produce, con cadenza almeno annuale, una relazione sullo stato di attuazione del sistema di protezione dei dati (cfr. *infra*), sulla base anche delle rendicontazioni e delle segnalazioni delle strutture organizzative dell'Agenzia.

L'RPD, avvalendosi del supporto dell'Ufficio Privacy e Qualità, che:

- coordina il ciclo di lavorazione delle segnalazioni di possibile violazione dei dati personali (*data breach*) attivando, di volta in volta, se necessario, le strutture competenti in base ai processi nel cui ambito si è prodotta la violazione (cfr. procedura SGPD Violazione dati personali);
- mantiene aggiornato il Registro delle Violazioni;
- effettua le relative notifiche al Garante delle violazioni dei dati personali previste dal GDPR;
- conduce gli audit previsti dal Piano di audit definito dal RPD;
- coordina le attività finalizzate a garantire l'esercizio dei diritti degli interessati previsti dal Regolamento curando, in particolare, il trattamento delle istanze e delle richieste di accesso ai dati dei trattamenti;
- rappresenta il punto di contatto del Titolare per le istanze e le richieste degli interessati;
- cura l'aggiornamento del Registro delle attività di Trattamento sulla base delle segnalazioni e delle proposte provenienti dalle strutture competenti;

### 2.1.3 Autorizzati al trattamento

Il Regolamento prevede che il trattamento di dati personali possa essere effettuato da parte di "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile" (articolo 4, paragrafo 1, n.10 del Regolamento).

Nell'ambito del SGDP di Agenzia delle entrate-Riscossione ciascun dipendente dell'Agenzia, nonché ciascun distaccato presso la stessa, è autorizzato al trattamento dei dati secondo quanto previsto nel "Registro delle attività di trattamento", e con riguardo ai dati contenuti nelle banche dati elettroniche e negli archivi cartacei dell'Agenzia connessi alle funzioni e attività svolte all'interno della struttura organizzativa di assegnazione.

Dunque, in relazione alle mansioni ricoperte, ciascun dipendente è autorizzato ad effettuare in modo lecito, corretto e diligente le attività di trattamento dei dati personali strettamente connesse ai processi che ricadono nelle competenze della struttura di assegnazione, per un periodo di tempo non superiore a quello necessario in riferimento alle finalità del trattamento stesso.

Una specifica autorizzazione è invece necessaria nei casi in cui un dipendente sia chiamato ad eseguire un trattamento di dati personali riferito a processi che esulano dalle competenze della struttura nel quale è assegnato (ad esempio, nel caso di partecipazione ad un gruppo di lavoro con competenze trasversali ecc.). L'autorizzazione formale dovrà essere attribuita secondo modalità documentabili e dovrà individuare puntualmente l'ambito del trattamento consentito.

Il personale autorizzato è tenuto, in particolare, a effettuare il trattamento dei dati nel rispetto delle istruzioni contenute nell'Allegato **"Disciplinare per l'utilizzo degli strumenti elettronici, per gli accessi alle risorse e ai dati di ADER"**, nonché della normativa vigente ed in conformità ad ogni altra disposizione di legge e/o regolamento in materia ed alle apposite note, direttive, prescrizioni e/o istruzioni già impartite o che verranno rese dal Titolare per la struttura organizzativa dell'Agenzia alla quale il personale è assegnato.

Potranno essere disposte verifiche periodiche sull'osservanza delle disposizioni cui ciascuno è obbligato ad attenersi. Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione per competenza dovranno essere scrupolosamente osservati anche in seguito all'eventuale cessazione dell'incarico.

I Responsabili di ciascuna struttura organizzativa, nell'ambito del coordinamento delle attività di competenza, monitorano le attività di trattamento di dati personali effettuate dalla struttura,

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

verificando il rispetto dei principi previsti dal Regolamento, del Sistema di Gestione per la Protezione dati e di quanto indicato nel "Registro delle attività di Trattamento".

### 2.1.4 Responsabili esterni del trattamento

Il Responsabile esterno del trattamento è *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento"*.

Il Titolare può pertanto ricorrere a **Responsabili esterni del trattamento**, ai sensi dell'art. 28 del Regolamento, per l'effettuazione di trattamenti per suo conto che presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I trattamenti effettuati da parte di un Responsabile esterno del trattamento devono essere disciplinati da un contratto o da altro atto giuridico che vincoli il Responsabile esterno del trattamento ad attenersi alle indicazioni del Titolare del trattamento anche in merito alla relativa durata, natura e finalità, tipo di dati personali trattati e categorie di interessati, obblighi e diritti del Titolare del trattamento. Tale contratto (o altro atto giuridico) viene conservato unitamente al contratto/convenzione di affidamento dei servizi alla controparte.

L'identificazione dei Responsabili per il trattamento di dati in occasione della stipula di contratti e convenzioni, viene registrata in uno specifico elenco tenuto aggiornato e reso disponibile all'Ufficio Privacy e qualità per il costante aggiornamento del registro delle attività di trattamento.

L'art. 28 del Regolamento disciplina i contenuti del citato contratto o altro atto giuridico e prevede che il Responsabile esterno del trattamento non possa ricorrere a un altro responsabile (sub-responsabile) senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

## 2.2 Responsabilità attribuite all'interno del Sistema di Gestione per la Protezione dei dati

L'Agenzia delle entrate-Riscossione attribuisce a ciascun Responsabile di struttura organizzativa compiti e funzioni inerenti al funzionamento del Sistema di Gestione per la protezione dei dati personali.

Tali Responsabili **sono sempre tenuti a:**

- diffondere i principi del GDPR, delle altre normative e delle procedure organizzative definite dall'Agenzia delle entrate Riscossione in materia di protezione dei dati personali;
- impartire istruzioni al personale dipendente per il trattamento dei dati personali nelle attività afferenti ai processi di competenza;
- vigilare sul rispetto dei principi stabiliti dalle norme in materia di protezione dei dati;
- vigilare sul rispetto delle misure tecniche e organizzative definite in materia di protezione dei dati.

Inoltre, al fine di garantire nel continuo l'efficacia e il corretto funzionamento del SGDP, nonché la dimostrabilità dell'adequatezza delle misure tecniche e organizzative predisposte per la sicurezza dei dati personali e per la tutela della libertà e dei diritti degli interessati, Il Sistema di Gestione attribuisce ruoli (**responsabilità specifiche all'interno del SGDP**) ai Responsabili in virtù della loro collocazione organizzativa.

Tali figure sono identificate a:

- **livello centrale:**
  - nei Direttori Centrali e di Area;
  - nei Direttori a riporto dei Direttori di Area;
  - nei Responsabili delle Reti Territoriali;
- **livello Regionale**
  - nei Direttori Regionali.

Ciascuno di tali attori, per quanto di competenza rispetto ai processi organizzativi e di protezione dati (svolti in coerenza con le responsabilità attribuite dal funzionigramma dell'Agenzia) e alle attività di trattamento realizzate, presidia - all'interno del Sistema di Gestione adottato dall'Ente - **le funzioni d'indirizzo, coordinamento e controllo interno per le strutture gestite.**

Tali funzioni implicano la responsabilità di:

- adottare e verificare periodicamente le misure di sicurezza (tecniche e organizzative) generali definite in materia di protezione dei dati e implementare, laddove consentito, eventuali misure organizzative particolari, ulteriori rispetto a quelle generali;
- applicare costantemente i principi previsti per il corretto funzionamento dell'architettura della protezione dei dati (*privacy by default*), attivando e coinvolgendo, sin dalle fasi di elaborazione di nuove esigenze di trattamento dati e/o di progettazione di nuovi servizi e/o strumenti, gli attori della "*privacy by design*" e in particolare il RPD;
- assicurare, in riferimento ai processi di competenza e alle attività di trattamento presidiate, la gestione dei rischi per la sicurezza dei dati personali e per la tutela dei diritti e delle libertà degli interessati, attivando, nel rispetto dell'art.35 del Regolamento secondo la metodologia adottata dall'Ente, la *Data Protection Impact assessment* (DPIA). La gestione del rischio viene realizzata anche sulla scorta di quanto al riguardo proposto dai Responsabili delle strutture di diretto coordinamento gerarchico;
- verificare periodicamente la corretta implementazione delle modalità di trattamento dei dati in coerenza con quanto definito all'interno del Registro delle attività di Trattamento, e dal complessivo SGPD, adoperando controlli e fornendo evidenza anche attraverso la documentazione al riguardo prevista (*schede rilevazione evidenze, check list* etc);
- coinvolgere tempestivamente il RPD in occasione dell'attivazione e/o rinnovo di contratti e convenzioni che prevedono il trattamento di dati personali di persone fisiche, rendendo preventivamente disponibili le informazioni relative alle misure tecniche e organizzative di sicurezza previste;
- segnalare, immediatamente e senza indugio, gli incidenti di sicurezza con possibili violazioni di dati personali all'Ufficio Privacy e Qualità e all'RPD alla casella email [protezione.dati@agenziariscossione.gov.it](mailto:protezione.dati@agenziariscossione.gov.it) e all'Ufficio SGSI Governance, secondo le modalità previste dalla procedura Gestione della violazione dei dati. Al riguardo i Responsabili effettuano le valutazioni preliminari e individuano iniziali misure di contenimento della violazione relative alla segnalazione proposta in coordinamento con l'Ufficio Privacy e Qualità;
- fornire al RPD le informazioni previste e il supporto richiesto per lo svolgimento dei compiti allo stesso assegnati. Ciò con particolare riguardo agli elementi e alle attività previste per la valutazione delle segnalazioni di violazione dei dati e per l'assolvimento delle altre attività al riguardo definite nella procedura Gestione della violazione dei dati;

- proporre al RPD, anche per conto delle strutture gerarchicamente dipendenti, integrazioni e/o aggiornamenti del Registro delle attività di Trattamento per i processi di competenza, così come descritto al paragrafo "Registri delle attività di trattamento";
- promuovere iniziative formative e di sensibilizzazione e segnalare, su indicazione dei Responsabili delle strutture gerarchicamente dipendenti, i fabbisogni formativi in materia di protezione dei dati;
- rendicontare in merito allo stato di attuazione del Sistema di Gestione per la protezione dei dati personali per gli ambiti di competenza e adottare le raccomandazioni, le azioni correttive e gli *action plan* previsti per la soluzione di non conformità rilevate.

In coerenza con le responsabilità specifiche attribuite dal SGDP, i Responsabili di Settore e di Ufficio delle strutture centrali, i Responsabili di Settore e di Ufficio delle strutture regionali e i Responsabili di Area Territoriale, di Ufficio di Area Territoriale e di Sportello, **danno seguito agli indirizzi ricevuti dal rispettivo Responsabile di livello centrale o regionale, assicurando la corretta attuazione e il monitoraggio operativo delle modalità, garanzie e limiti al trattamento dei dati personali definite nel rispetto della normativa in materia di protezione dei dati personali e delle prescrizioni del Sistema di Gestione.**

Essi inoltre sono tenuti a:

- attuare e monitorare a livello operativo le misure di sicurezza (tecnica e organizzativa) definite in materia di protezione dei dati personali;
- segnalare al Responsabile di livello centrale o di livello regionale di riferimento gerarchico, eventuali rischi rilevati nella protezione dei dati personali, anche derivanti dal concreto svolgimento dei processi organizzativi/trattamenti presidiati;
- attivare, d'intesa con il Responsabile di livello centrale o di livello regionale di riferimento gerarchico, la procedura di valutazione di impatto (DPIA), ai sensi dell'articolo 35 del Regolamento nei casi in cui un trattamento presenti un livello di rischio elevato per i diritti e le libertà degli interessati;
- proporre al RPD, attraverso il Responsabile di livello centrale o di livello regionale di riferimento gerarchico, aggiornamenti al Registro delle attività di Trattamento con riferimento alla definizione delle caratteristiche dei trattamenti e dei requisiti delle applicazioni sin dalla fase di progettazione, nel rispetto dei principi della "*privacy by default*" e della "*privacy by design*";
- supportare il corretto funzionamento del SGDP;
- evidenziare i fabbisogni formativi in materia di protezione dei dati;

- segnalare attraverso il Responsabile di livello centrale o di livello regionale di riferimento gerarchico, episodi di violazione dei dati (possibile *data breach*) secondo le modalità riportate nella procedura Gestione della violazione dei dati;
- rendicontare in merito allo stato di attuazione del sistema di protezione dei dati personali per gli ambiti di competenza.

Nell'ambito del SGDP, per la gestione e la manutenzione degli impianti di elaborazione o di sue componenti, sono state individuate delle figure professionali definite Amministratori di sistema (di seguito AdS). In base al provvedimento del Garante del 27 novembre 2008 e s.m.i., vengono considerati AdS anche gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

La designazione degli AdS, come prescritto dal provvedimento del Garante, è effettuata previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto della normativa in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza.

Può essere designato Amministratore di sistema, personale appartenente alla Direzione Tecnologie ed Innovazione. Possono essere altresì individuate altre specifiche figure professionali, anche esterne ad AdeR, di cui la Direzione Tecnologie e Innovazione si avvale per l'assolvimento di specifiche attività. La designazione quale AdS è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

La normativa pone in rilievo la particolare capacità di azione propria degli AdS e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, professionali e di condotta.

Inoltre nella lettera di designazione è indicato che, a norma del Provvedimento del 27 novembre 2008 e s.m.i., gli accessi degli AdS ai sistemi a cui sono preposti, saranno sottoposti a log, che il log sarà conservato per un periodo di almeno 6 mesi, che il Titolare o il Responsabile incaricato, anche attraverso l'analisi del log, verificheranno l'operato degli AdS.

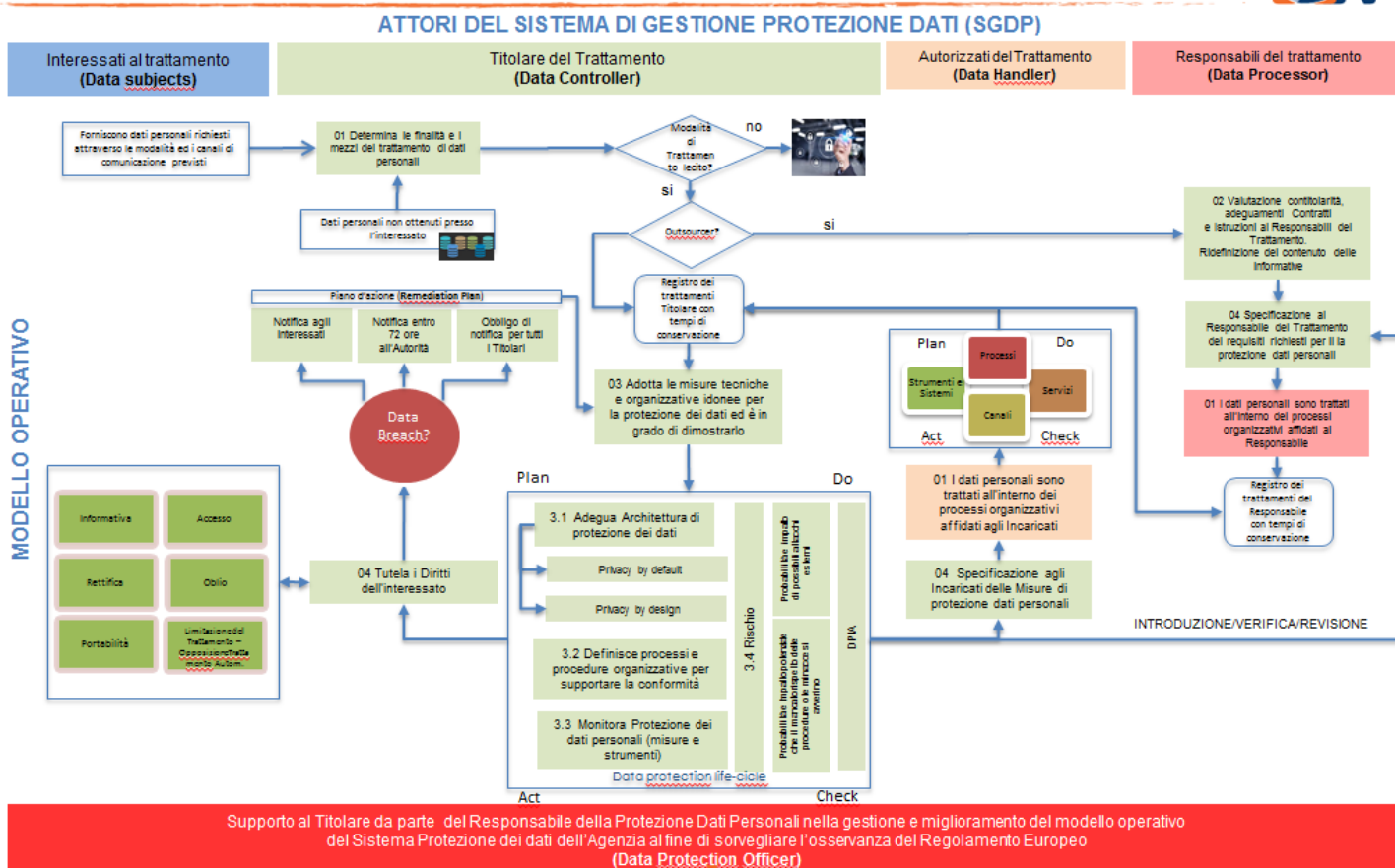
<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

## SEZIONE 3 – MODELLO OPERATIVO

Revisioni	Data Modifica	Descrizione delle modifiche	Natura delle modifiche
1.0	__/__/2018		

La rappresentazione seguente, illustra, in riferimento alle di figure di responsabilità in materia di protezione dati personali previste dal GDPR, il macro processo organizzativo di funzionamento relativo alla protezione dei dati adottato da Agenzia delle entrate – Riscossione, secondo l'approccio del miglioramento continuo.

### GDPR (Gli Attori e il modello operativo del Sistema di gestione della Protezione dei Dati)

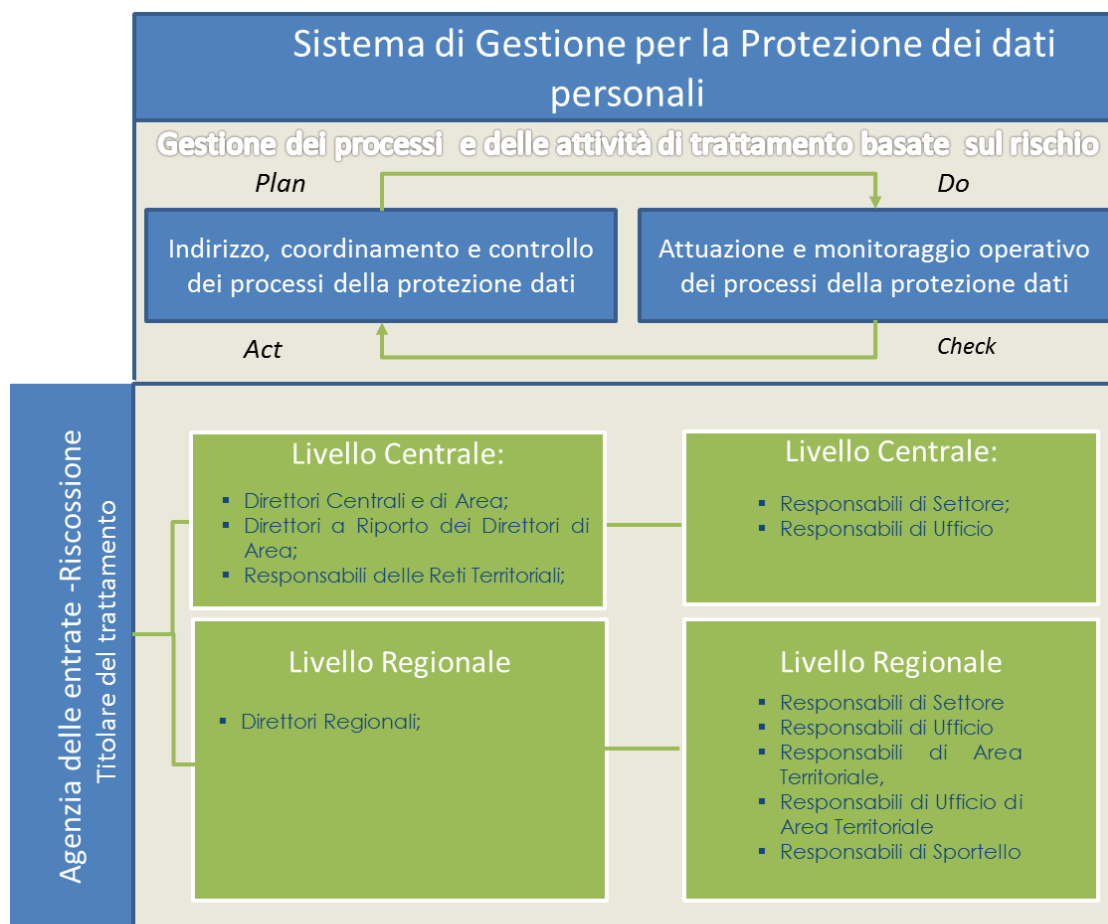


Agenzia delle Entrate-Riscossione ha definito, nel rispetto del Regolamento, gli elementi e le interazioni tra le componenti ed i processi della protezione dati personali compresi nel descritto

modello operativo che, dunque, è posto a fondamento del funzionamento del Sistema di Gestione per la protezione dei dati personali.

Tali processi, in coerenza con l'evoluzione della normativa e dei requisiti ad essa sottesi, saranno oggetto di progressiva implementazione secondo gli approcci già rappresentati nel presente Manuale e che si sintetizzano nella corretta valutazione dei rischi per la sicurezza dei dati personali e per i diritti e le libertà degli interessati, nonché attraverso la corretta e sistematica applicazione del ciclo Plan-Do-Check-Act (PDCA), utilizzato per presidiare il miglioramento continuo del Sistema di Gestione per la Protezione dei dati.

Con particolare riferimento alle modalità organizzative attraverso le quali la complessiva "accountability" di Agenzia delle entrate -Riscossione viene espressa, si riporta, di seguito, il seguente schema sinottico:



**Struttura Responsabile protezione dei dati e RPD**

### 3.1. Registro delle attività di trattamento

Il Regolamento prevede la tenuta da parte del Titolare (e di ciascun Responsabile esterno del trattamento) di un Registro delle attività di Trattamento (art. 30), quale parte integrante del sistema di gestione dei dati personali. L'Ufficio Privacy e Qualità cura la tenuta e l'aggiornamento del Registro per conto del RPD.

Il Registro delle attività di Trattamento prevede anche l'indicazione, mediante sezione dedicata o con distinto Registro, dei trattamenti svolti da Agenzia delle entrate-Riscossione in qualità di Responsabile esterno del trattamento, laddove sia stata designata sulla base di apposito contratto o altro atto giuridico (art. 28).

L'aggiornamento del Registro delle attività di Trattamento (anche con riferimento ai trattamenti effettuati in qualità di Responsabile esterno) deve avvenire sistematicamente e continuativamente laddove si rilevi una modifica dei trattamenti già registrati o nuovi trattamenti da effettuare.

Ciascun Responsabile di Struttura organizzativa, laddove rilevi, per quanto di competenza, l'esigenza funzionale di effettuare nuovi trattamenti non contemplati nel Registro, deve richiedere l'autorizzazione al Titolare, che valuta, attraverso il RPD, i dati trattati e le misure di sicurezza previste.

Fermo restando la necessità di garantire un sistematico e continuativo aggiornamento del Registro, l'Ufficio Privacy e Qualità provvede a richiedere, su impulso del Titolare o del RPD e comunque con cadenza trimestrale, alle strutture organizzative l'adeguatezza dei trattamenti già registrati, evidenziando:

- eventuali integrazioni o rettifiche nel caso di scostamenti tra quanto definito e l'effettiva operatività rilevata;
- la proposta di nuovi trattamenti da sottoporre alla valutazione del Titolare, con il supporto del RPD.

L'Ufficio Privacy e Qualità, allorché riceva una proposta di modifica dei trattamenti, ovvero di introduzione di nuovi, prima di interessare il RPD e il Titolare, verifica che la struttura apicale di livello centrale o regionale abbia effettuato le valutazioni di rischio e previsto adeguate misure di sicurezza.

Il Titolare, avvalendosi del RPD, autorizza la modifica del trattamento o l'introduzione di un nuovo trattamento mediante aggiornamento del Registro.

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

La versione aggiornata del Registro delle attività di Trattamento viene diffusa internamente all'Ente, a cura dell'Ufficio Privacy e Qualità, mediante pubblicazione nell'apposita Sezione dell'Intranet.

### 3.2. Informativa agli interessati

Il Regolamento, prevede l'obbligo di fornire, a fronte del trattamento dei dati personali, una apposita informativa all'interessato che illustra le informazioni sul trattamento e sui diritti esercitabili.

In caso di raccolta di dati personali direttamente dall'interessato, ad esempio all'atto di presentazione di un'istanza ovvero di richiesta di un servizio da parte del contribuente, l'art. 13 del Regolamento indica le informazioni che devono essere fornite allo stesso nel momento in cui i dati sono ottenuti. Le informazioni da fornire all'interessato nel caso in cui i dati personali non siano stati ottenuti presso lo stesso (ma ad esempio forniti da terzi) sono indicati all'art. 14 del Regolamento.

L'informativa all'interessato nel caso di dati non ottenuti presso lo stesso va resa, ai sensi dell'art. 14 par. 3 (punti b) e c)) del Regolamento, 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, nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

### 3.3. Diritti degli interessati

Il Regolamento riconosce all'interessato, con riferimento ai propri dati personali trattati, una serie di diritti nei confronti del Titolare, quali diritto di accesso (art. 15), diritto di rettifica (art. 16), diritto alla cancellazione (art. 17), diritto di limitazione di trattamento (art. 18), diritto alla portabilità dei dati (art. 20), diritto di opposizione (art. 21) e diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22).

Con particolare riferimento al diritto di accesso, il Regolamento prevede che il Titolare fornisca all'interessato, a seguito di istanza, la conferma o meno che sia in corso un trattamento di dati personali che lo riguardano e, in tal caso, mette a disposizione, qualora ciò non leda i diritti e le libertà altrui, una "copia dei dati personali" oggetto di trattamento nonché le seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

- 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;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del Regolamento e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il termine per la risposta all'interessato è fissato, per tutti i diritti, in **1 mese dal ricevimento della richiesta**, prorogabile di ulteriori 2 mesi, se necessario, considerando la complessità e il numero delle richieste. La risposta all'interessato deve essere in forma scritta o con altri mezzi, anche, se del caso, con mezzi elettronici. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Per la presentazione ad Agenzia delle entrate-Riscossione dell'istanza per l'esercizio dei diritti dell'interessato i canali a disposizione sono i seguenti:

- per via telematica, secondo le modalità previste dall'art. 65 del D.lgs. 7 marzo 2005, n. 82, alla PEC [protezione.dati@pec.agenziaiscossione.gov.it](mailto:protezione.dati@pec.agenziaiscossione.gov.it) ;
- mediante posta, con allegata copia di idoneo e valido documento di riconoscimento, all'indirizzo Agenzia delle entrate-Riscossione, Struttura a supporto del RPD, Via Giuseppe Grezar n. 14 - 00142 Roma;
- mediante consegna a mano, allegando copia di idoneo e valido documento di riconoscimento, presso la sede di Agenzia delle entrate-Riscossione, in Roma, Via Giuseppe Grezar n. 14.

Eventuali istanze per l'esercizio dei diritti in argomento ricevute presso le sedi regionali e territoriali o presso gli sportelli dell'Agenzia devono essere oggetto di immediata protocollazione

e assegnazione all'Ufficio Privacy e Qualità, quale struttura a supporto del RPD (Responsabile protezione dati) da parte della struttura ricevente.

L'Ufficio Privacy e Qualità ricevuta l'istanza procede alla protocollazione della stessa, se pervenuta per via telematica, e alle seguenti attività:

- verifica di completezza della documentazione allegata e/o della presenza in seno all'istanza di richieste di natura diversa, da trasmettere alle strutture competenti;
- analisi di merito in relazione ai diritti che il richiedente intende esercitare.

Qualora dall'esito delle verifiche e dalle analisi effettuate si accerti la mancanza/incompletezza della documentazione, ovvero la non ricevibilità dell'istanza (per difetto di legittimazione del richiedente) l'Ufficio Privacy e Qualità procede, entro il termine previsto, con la richiesta di integrazione della documentazione oppure con un riscontro negativo informando l'interessato dei motivi dell'inottemperanza e della possibilità di proporre reclamo a una Autorità di controllo ovvero di proporre ricorso giurisdizionale.

È possibile prorogare il termine della risposta fino a due mesi in caso di istanze particolarmente complesse e, in tal caso, il RPD informa l'interessato di tale proroga motivandone il ritardo (art. 12).

L'Ufficio Privacy e Qualità si avvale delle informazioni già censite nel Registro delle attività di Trattamento e richiede, laddove necessario, alle Strutture organizzative che effettuano il trattamento le informazioni da fornire all'interessato. La richiesta dell'Ufficio contiene l'indicazione del termine massimo per l'evasione da parte della Struttura destinataria (di norma entro 10 giorni lavorativi dalla richiesta). A fronte delle informazioni acquisite, l'Ufficio Privacy e Qualità predispone la lettera di riscontro al richiedente ed i relativi allegati e la trasmette, previa protocollazione, all'interessato, nel rigoroso rispetto dei tempi previsti.

In caso di richiesta diversa dall'accesso ai dati personali (esempio rettifica, cancellazione, limitazione al trattamento, portabilità dei dati, opposizione, ecc.) il RPD valuta preliminarmente, coinvolgendo in primis la Direzione Centrale Affari Legali e il Responsabile di struttura apicale di livello centrale o regionale, owner del relativo processo dell'Agenzia, se sussistono le condizioni di applicabilità dei diritti. Tale valutazione deve tener conto della natura dei dati e dei trattamenti di cui viene richiesta la rettifica, cancellazione, ecc., delle norme contenute nel Regolamento e dei suggerimenti del Garante in materia, facendo salva, naturalmente, la speciale disciplina connessa al fine istituzionale dell'Agenzia, ovvero la sussistenza di motivi legittimi per la prosecuzione del trattamento.

Ove sia necessario procedere alla rettifica, cancellazione o limitazione al trattamento, l'Ufficio Privacy e Qualità:

- richiede alle Strutture organizzative che effettuano il trattamento la rettifica, la cancellazione o la limitazione del trattamento dei dati personali dell'interessato e acquisisce conferma dell'avvenuto adeguamento dei relativi trattamenti;
- comunica a ciascuno dei destinatari a cui sono trasmessi i dati personali dell'interessato la rettifica, la cancellazione o la limitazione del trattamento richiesta, ove possibile ai sensi dell'art. 19 del Regolamento.

L'Ufficio Privacy e Qualità gestisce il **Registro delle istanze degli interessati**, anche attraverso l'applicativo aziendale di protocollazione (Docway), nel quale traccia tutte le istanze pervenute, con evidenza delle richieste effettuate (diritti esercitati), la relativa documentazione ed il relativo esito. Tale registro viene tenuto a disposizione del Titolare, dei Responsabili delle strutture organizzative interessate e, in caso di richiesta, del Garante.

### **3.4. Violazione dei dati personali (data breach)**

Il Regolamento (art. 33 e 34) introduce specifici adempimenti da assolvere in caso di violazione dei dati personali (c.d. *data breach*), definita (art. 4) come *"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"* trattati.

All'interno del Sistema di Gestione per la protezione dei dati personali è disponibile la procedura di *data breach* obbligatoria *erga omnes* in tutti i casi in cui si verifichi un evento riguardante una possibile violazione di dati personali. Ciò in quanto il Titolare del trattamento, è obbligato, in virtù delle disposizioni sopra richiamate, a notificare la violazione dei dati personali al Garante, 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, poi, la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, sarà necessario per il Titolare del trattamento informare della violazione anche gli interessati, senza ingiustificato ritardo, salvo ricorrano i casi di esclusione previsti dall'art. 34, paragrafo 3, del Regolamento. Per permettere al Titolare del trattamento di rispettare i tempi rapidi di azione previsti dal Regolamento, anche al fine di scongiurare eventuali misure sanzionatorie nei confronti dell'Agenzia, la procedura di *data breach*, contenuta nel Sistema di Gestione per la protezione dei dati personali, delinea il sistema di lavorazione delle segnalazioni.

Tutte le violazioni dei dati personali delle persone fisiche e le relative analisi di rischio (comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio) devono essere **annotate** in un **apposito Registro delle violazioni dei dati personali** per future consultazioni, anche da parte del Garante. Gli ulteriori adempimenti da porre in essere per la gestione delle violazioni (art. 33) sono definiti in relazione alla valutazione del rischio per i diritti e le libertà degli interessati.

### 3.5. Privacy by design e privacy by default

L'articolo 25 del GDPR introduce il cosiddetto principio della *privacy by design* prevedendo che il Titolare debba mettere 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 Regolamento e tutelare i diritti degli interessati, non solo al momento del trattamento ma anche "al momento di determinare i mezzi del trattamento".

Con questa previsione il Regolamento intende porre l'attenzione sull'opportunità che il processo di progettazione o aggiornamento di un servizio/processo che implichi un trattamento di dati personali prenda in adeguata considerazione le esigenze connesse alla protezione di questi dati sin dalle prime fasi di analisi.

L'adozione del principio della *privacy by design* consente di dare vita ad un processo di progettazione che non solo risulterà più efficace nella protezione dei dati ma anche più efficiente riducendo i costi e le inefficienze connesse alla necessità di realizzare interventi successivi mirati a rimediare a carenze di analisi.

Lo stesso articolo 25 introduce anche il principio della *privacy by default* affermando la necessità che il Titolare metta 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.

Dal punto di vista operativo, la responsabilità nell'attuazione del principio della *privacy by design* e della *privacy by default* investe chiunque, operando per conto del Titolare del trattamento, in qualità di owner del processo, progetti un nuovo servizio/processo o intervenga per modificare le modalità di esecuzione di un trattamento esistente.

In particolare, il Sistema di Gestione pone questa particolare responsabilità in capo ai Responsabili apicali di struttura di livello centrale / regionale, in quanto owner dei processi delle relative strutture, responsabili della progettazione delle modalità di esecuzione di tali processi e degli applicativi informatici di supporto.

Tuttavia, l'esigenza di dare vita ad un nuovo trattamento o di introdurre una modalità innovativa nell'esecuzione di un trattamento già censito e regolamentato potrebbe avvertirsi anche in strutture diverse da quelle apicale (livello centrale/regionale). In questi casi, la struttura apicale deve comunque ritenersi investita del ruolo di owner del processo e, pertanto, sarà chiamata ad effettuare, con il supporto della struttura che ha segnalato l'esigenza, una valutazione relativa al nuovo trattamento.

Dal punto di vista operativo, l'approccio *privacy by design* dà luogo a un percorso di progettazione dei nuovi servizi/processi che si sviluppa nelle seguenti fasi:

1. Coinvolgimento del RPD e degli *stakeholders*
2. Analisi delle caratteristiche del trattamento
3. Valutazione dei rischi e definizione delle misure di sicurezza
4. Aggiornamento del Registro delle attività di trattamento

### **3.5.1. Coinvolgimento del RPD e degli *stakeholders***

Sin dalla prima fase di analisi dell'esigenza, il Responsabile apicale owner del processo (di livello centrale/ regionale) deve coinvolgere il RPD affinché questi possa esprimersi circa le modalità di trattamento dei dati personali gestiti nell'ambito del processo oggetto di progettazione e le misure di sicurezza da predisporre. In questa fase, il RPD può anche dare istruzioni circa la necessità di un suo eventuale coinvolgimento nelle fasi successive all'analisi.

Inoltre, l'owner deve coinvolgere, sin dall'inizio della progettazione, anche tutti gli altri *stakeholders*, interni o esterni all'Agenzia, che potrebbero avere un ruolo nella definizione del progetto, anche a prescindere dal fatto che siano previsti trattamenti dei dati personali (ad esempio: il Responsabile della sicurezza informatica, il Responsabile della gestione documentale, ecc.).

Nell'ambito del processo di progettazione e realizzazione di nuovi servizi, informatici o che prevedono interventi di natura logistica, la richiesta funzionale, predisposta dall'owner del processo deve includere anche una prima indicazione dei trattamenti di dati personali previsti.

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

Dal punto di vista della protezione dei dati personali è fondamentale che in questa fase siano coinvolte, o rappresentate, tutte le strutture che parteciperanno al trattamento in quanto idonee a fornire informazioni circa le modalità del trattamento, gli strumenti utilizzati e, quindi, favorire l'individuazione e la successiva attuazione delle misure di sicurezza.

La progettazione di servizi informatici che prevedono trattamenti di dati personali è curata dalla Direzione Tecnologie e Innovazione - Settori *Demand&Delivery*; la progettazione di servizi di natura logistica o di natura documentale sono curate attraverso il coinvolgimento, secondo competenza, della Direzione Approvvigionamenti e Logistica e della Direzione Produzione Ruoli e Gestione Documentale

### 3.5.2. Descrizione delle caratteristiche del trattamento

L'owner del processo, nel caso in cui il servizio/processo oggetto di progettazione preveda il trattamento di dati personali, deve quindi procedere ad un'analisi delle caratteristiche del trattamento finalizzata ad individuare, in particolare, le tipologie di dati trattati, le categorie di soggetti interessati, la tipologia di trattamento, gli strumenti che si prevede di utilizzare per il trattamento, le modalità di archiviazione dei dati, i tempi di conservazione dei dati.

Da questo punto di vista, il Registro delle attività di trattamento rappresenta un importante strumento di supporto in quanto individua, innanzitutto, i trattamenti di dati personali già censiti dall'Agenzia e, per ciascuno di essi, elenca le principali caratteristiche significative ai fini della protezione dei dati. Il confronto con il Registro permette di verificare facilmente se l'oggetto della progettazione dia luogo ad un "nuovo" trattamento non previsto nel Registro (e, quindi, da aggiungere) oppure si configuri una modifica delle caratteristiche di un trattamento già censito nel Registro che, in questo caso, dovrà essere aggiornato.

In particolare, nella fase di analisi e classificazione del trattamento, l'owner deve raccogliere le seguenti informazioni:

- Nome del trattamento
- Descrizione del trattamento
- Referente del trattamento
- Struttura dell'Agenzia referente per il trattamento
- Processo di riferimento per il trattamento, individuato facendo riferimento ai Processi dell'Agenzia
- Tipologia di trattamento, indicando se il trattamento è supportato da servizi ICT o se si tratta di un trattamento interamente manuale

- Strumenti di trattamento, indicando gli applicativi ICT utilizzati
- Modalità di archiviazione dei dati, specificando se saranno utilizzati archivi fisici o logici e fornendo i dettagli per la loro individuazione
- Finalità del trattamento, indicando gli scopi del trattamento che devono essere determinati, espliciti e legittimi, al fine di poter determinare modalità di trattamento ed evitare la raccolta di dati eccedenti e superflui rispetto alle finalità del trattamento contravvenendo ai principi della privacy by default
- Descrizione della finalità del trattamento
- Fondamenti di liceità del trattamento, in quanto il trattamento deve trovare fondamento in un'idonea base giuridica
- Categorie di soggetti interessati
- Descrizione degli interessati
- Categorie di dati personali oggetto del trattamento
- Descrizione dei dati personali
- Origine dei dati personali, precisandola modalità di raccolta e quindi se il dato viene fornito direttamente dall'interessato, da terze parti, da fonti pubbliche o da altre fonti
- Destinatari della comunicazione e relativa categoria di soggetto (persona fisica o giuridica, autorità o altro organismo) che riceve comunicazione dei dati personali, a prescindere dal fatto che si tratti o meno di un terzo
- Trasferimento di dati extra UE, indicando se il dato trattato è destinato ad essere trasferito in un Paese terzo e, nel caso, in quale specificando le garanzie e autorizzazioni previste dagli articoli 45 e 46 del Regolamento
- Termini per la cancellazione dei dati

### 3.5.3. Valutazione dei rischi e delle misure di sicurezza

Completata la classificazione del trattamento con l'individuazione delle principali caratteristiche dei dati che ne sono oggetto, l'owner del processo effettua una valutazione dei rischi connessi alla tipologia di dati personali trattati al fine di individuare le misure di sicurezza, tecniche e organizzative, da porre in essere per ottenerne una mitigazione.

La metodologia per effettuare la valutazione dei rischi (e la Valutazione d'impatto) e per individuare le misure di sicurezza è descritta nella procedura "Metodologia per il *Data Protection Impact Assessment*".

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

In sede di valutazione del rischio potrebbe emergere la necessità di attivare la Valutazione d'impatto sulla protezione dei dati, prevista dall'articolo 35 del Regolamento per i casi in cui un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'attivazione della Valutazione d'impatto richiede il coinvolgimento obbligatorio del DPO che fornisce il suo parere.

#### 3.5.4. Aggiornamento del Registro delle attività di trattamento

Conclusa con esito positivo la valutazione del rischio, l'owner del processo, secondo le modalità organizzative precedentemente descritte, evidenzia la necessità di aggiornare il Registro delle attività di trattamento trasmettendo tutti i dati raccolti in fase di classificazione del trattamento, le risultanze della valutazione dei rischi (e dell'eventuale Valutazione di impatto) e le misure di sicurezza individuate per il trattamento, proponendo la modifica e/o integrazione al Registro all'Ufficio Privacy e Qualità.

#### 3.6. Data Protection Impact Assessment (DPIA)

La valutazione d'impatto sulla protezione dei dati o "*Data Protection Impact assessment*" (di seguito anche: "DPIA") è una procedura, da effettuarsi prima di procedere con un trattamento di dati personali, finalizzata a descrivere un tale trattamento di dati personali, valutarne la necessità e la proporzionalità ed a gestire gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo.

Qualora un trattamento (o un insieme di trattamenti simili), allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento presenti un rischio elevato per i diritti e le libertà degli interessati, l'art. 35 del Regolamento prevede l'obbligo di effettuare una valutazione di impatto del trattamento sulla protezione dei dati personali.

Laddove la valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, Se a seguito della valutazione di impatto, considerando anche le misure di sicurezza adottate/da adottare per attenuare il rischio, il rischio del trattamento risulti comunque elevato, il RPD consulta il Garante ai sensi dell'art. 36 del Regolamento (consultazione preventiva), secondo le tempistiche ivi previste.

Il Titolare, per il tramite dei Responsabili apicali delle strutture centrali / regionali (con il coinvolgimento delle strutture di diretto riporto gerarchico) in quanto owner dei processi

dell'Agenzia, effettua l'attività di valutazione (tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento) dei rischi per i diritti e le libertà delle persone relativi al trattamento e delle relative misure di sicurezza con il supporto delle seguenti strutture: Direzione Tecnologie e Innovazione, per le misure di sicurezza adottate o da adottare per gli strumenti di trattamento utilizzati.

- Direzione Approvvigionamenti e Logistica e Direzione Produzione Ruoli e Gestione Documentale, per le misure di sicurezza connesse all'utilizzo di archivi fisici dislocati sulle sedi dell'Agenzia ovvero gestiti a livello centrale
- Direzione Organizzazione e Processi, per le misure organizzative adottate o da adottare in riferimento alle attività di trattamento.

Il Responsabile apicale per la valutazione dei rischi coinvolge, secondo le previsioni del Regolamento, il RPD che opera con il supporto dell'Ufficio Privacy e Qualità.

La metodologia DPIA è oggetto di uno specifico documento.

### **3.7. Verifica e monitoraggio della compliance del Sistema**

Tra le funzioni che l'articolo 39 del GDPR attribuisce al Responsabile per la Protezione dei Dati figura anche la sorveglianza sul corretto adempimento delle disposizioni del Regolamento, delle norme e dalle procedure dell'Agenzia in materia di protezione dei dati.

Per consentire al RPD di svolgere questa funzione, il Sistema di gestione della protezione dei dati dell'Agenzia prevede la possibilità di introdurre strumenti che permettano al RPD di raccogliere elementi informativi in grado di dimostrare il grado di *compliance*.

D'altra parte, l'introduzione del principio di *accountability* richiede che gli stessi attori del Sistema, ai diversi livelli di responsabilità, siano coinvolti in attività di presidio e monitoraggio della *compliance*.

Ferma restando la possibilità, per il RPD, di introdurre ulteriori strumenti e metodi per esercitare le funzioni previste dall'articolo 39, il Sistema prevede i seguenti strumenti, a disposizione rispettivamente dello stesso RPD e dei Responsabili apicali delle strutture organizzative centrali, per verificare il grado di *compliance* raggiunto dall'organizzazione:

- Sistemi di audit
- Documenti del riesame

<b>Titolo Documento:</b> Manuale del Sistema di Gestione della Protezione dei dati personali	<b>Codice Documento:</b> Manuale SGPD	<b>Revisione N°:</b> 1.0
<b>TIPO DOCUMENTO:</b> Manuale	<b>Data di Autorizzazione:</b> 11/06/2018	<b>Status:</b> in vigore

Questi strumenti consentono di far affluire verso il RPD elementi informativi in grado di produrre una valutazione sullo stato di attuazione del Sistema di protezione dei dati personali dell'Agenzia delle entrate Riscossione e, quindi, di poter riferire in tal senso, sia al Titolare che all'Autorità Garante.

### 3.7.1. Sistemi di audit

Il Responsabile per la Protezione dei Dati pianifica, sulla base degli elementi informativi in suo possesso, un Piano di audit attraverso il quale può verificare, mediante un accesso diretto alle strutture dell'Agenzia, lo stato di adeguamento del Sistema di protezione dei dati personali.

Il Piano di audit può:

- avere ad oggetto tutti i trattamenti (o un campione di trattamenti) svolti presso una determinata struttura, allo scopo di verificare il grado di *compliance* complessivamente raggiunto da tale struttura;
- riguardare una porzione limitata di trattamenti da verificare su più strutture (anche individuate a campione) per valutare il grado di *compliance* raggiunto complessivamente sui trattamenti oggetto dell'indagine.

Per la conduzione degli audit, il RPD si avvale del supporto dell'Ufficio Privacy e Qualità.

Al termine di ciascun audit viene prodotto un Rapporto di audit nel quale vengono indicati eventuali non conformità e azioni di miglioramento nella protezione dei dati. Il Rapporto viene rilasciato al Responsabile della struttura presso la quale è stato condotto l'audit e viene trasmesso al Responsabile apicale di livello centrale e/o regionale della struttura owner.

### 3.7.2. Documenti di riesame

Periodicamente, con cadenza almeno trimestrale, secondo le indicazioni fornite dal RPD, i Responsabili apicali delle strutture di livello centrale/regionale, con il supporto delle strutture a loro diretto riporto, trasmettono all'Ufficio Privacy e Qualità e al RDP un documento nel quale viene fornita evidenza dello stato di attuazione del Sistema di protezione dei dati nella struttura di riferimento.

Il documento presenta una serie di elementi informativi, che possono essere raccolti anche mediante strumenti forniti dal RDP (es. schede di rilevazione, *check list*, ecc.) che consentano, in particolare, di:

- dare evidenza della corretta implementazione delle modalità di trattamento dei dati e delle misure di sicurezza indicate dalle norme, dalle procedure organizzative e dal Registro delle attività di trattamento in tutte le articolazioni interne della struttura di riferimento;
- fornire un riepilogo delle segnalazioni di violazioni dei dati promosse dalla struttura dettagliando, per ciascuna segnalazione, le azioni poste in essere per il contenimento della violazione, anche a seguito delle indicazioni ricevute dal RPD, dall'Ufficio Privacy e Qualità;
- rendicontare la gestione delle richieste di accesso ai dati personali che hanno interessato la struttura;
- dare evidenza delle iniziative adottate attivate per la sensibilizzazione del personale ai principi del GDPR e della partecipazione dei dipendenti alle iniziative formative avviate in materia di protezione dei dati.
- dare evidenza della corretta implementazione delle modalità di trattamento dei dati e delle misure di sicurezza indicate dalle norme, dalle procedure organizzative e dal registro delle attività di trattamento

### **3.8. Relazione sullo stato di attuazione del sistema di protezione dei dati**

Il Responsabile Protezione Dati predispone annualmente una Relazione sullo stato di attuazione del Sistema di protezione dei dati nella quale viene data evidenza:

- della sintesi delle risultanze contenute nei documenti trasmessi dai Responsabili apicali delle strutture centrali;
- delle risultanze del piano di audit;
- delle segnalazioni di violazione di dati pervenute dalle strutture dell'Agenzia o da altre fonti e delle azioni intraprese di conseguenza;
- delle notifiche di violazioni all'autorità di controllo;
- delle Valutazioni di impatto sulla protezione dei dati attivate dalle strutture dell'Agenzia;
- dei casi in cui si è fatto ricorso alla consultazione preventiva di cui all'articolo 36 del Regolamento;
- delle richieste di accesso ai dati provenienti dagli interessati.

La Relazione può contenere indicazioni e pareri per il miglioramento del Sistema di gestione della protezione dei dati e viene trasmessa al Titolare.