Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali in conformità alla disciplina di cui al Regolamento UE 2016/679

Approvato con Determinazione del Direttore Generale n. __ del __/__/____

Sommario

INTRODUZIONE

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con abrogazione della direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Il nuovo regolamento UE, obbligatorio in tutti i suoi elementi e direttamente applicabile a ciascuno degli Stati membri a decorrere dal 25 maggio 2018, si fonda sul principio in forza del quale, la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale come previsto dall'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea ("Carta") e dall'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione Europea ("TFUE") che stabiliscono che "***ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano***".

Con il presente Regolamento l'Agenzia Sarda delle Entrate dà attuazione degli obblighi di legge e costituisce la cornice organizzativa e procedurale entro la quale vengono attuate le procedure operative, realizzati i modelli e gli allegati tecnici che sono adottati e aggiornati con atti interni, nel rispetto del presente Regolamento e della normativa vigente.

CAPO I - DISPOSIZIONI GENERALI

Art. 1 - Oggetto

1. Il presente Regolamento disciplina il trattamento dei dati personali effettuato dall'Agenzia Sarda delle Entrate (di seguito "Agenzia") in conformità al Regolamento (UE) 2016/679 (di seguito "GDPR") e al D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101 (di seguito "Codice Privacy").
2. Il Regolamento ha finalità di garantire il rispetto dei diritti e delle libertà fondamentali degli interessati, assicurare la liceità, correttezza e trasparenza dei trattamenti.
3. Il Regolamento disciplina altresì l'organizzazione interna dei trattamenti svolti con strumenti informatici, servizi digitali e banche dati, nonché i flussi di dati con altri enti pubblici o soggetti terzi, inclusi i casi di contitolarità e di affidamento a responsabili del trattamento.
4. Il Regolamento si applica a tutti i trattamenti di dati personali effettuati dall'Agenzia nell'esercizio delle proprie funzioni istituzionali, con mezzi automatizzati o manuali.
5. Sono soggetti al presente Regolamento:

a. il personale dipendente dell'Agenzia a qualunque titolo;
b. i collaboratori esterni e consulenti;
c. i soggetti designati quali Responsabili del trattamento ai sensi dell'art. 28 GDPR.

Art. 2 - Quadro normativo di riferimento

1. Il presente Regolamento tiene conto dei seguenti documenti:

- RGPD UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Codice in materia di dati personali (D. Lgs. n.196/2003) così come riformato dal D. Lgs. n. 101/2018;
- L. 241/90 e ssmmii;
- D. Lgs. 33/2013 e ss.mm.ii.
- D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale) e Linee guida AgID applicabili (formazione, gestione e conservazione dei documenti informatici; sicurezza ICT);

- Linee guida e provvedimenti del Garante in materia di trasparenza e pubblicazione online di atti contenenti dati personali;

Art. 3 - Definizioni

1. Il presente Regolamento utilizza le seguenti definizioni ai sensi dell'art. 4 RGPD:

«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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«Contitolari del trattamento»: due o più titolari del trattamento che determinino congiuntamente le finalità e i mezzi del trattamento;

«**Autorizzato al trattamento**»: la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del Titolare o del Dirigente/Funzionario EQ designato allo svolgimento di specifici compiti e funzioni connessi al trattamento;

«**Dirigente/Funzionario EQ Designato allo svolgimento di specifici compiti e funzioni connessi al trattamento»:** la persona fisica espressamente designata che, sotto la responsabilità del Titolare e nell'ambito della propria struttura organizzativa, svolge specifici compiti e funzioni connessi al trattamento dei 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;

«**Interessato**»: la persona fisica cui si riferiscono i dati personali oggetto di trattamento;

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

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

«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;

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

«Autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto

- il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
- oppure un reclamo è stato proposto a tale autorità di controllo.

2. Ai sensi dell'art. 2-*ter*, comma 4, D. Lgs. 196/03 e ss.mm.ii, si intende per:

«Comunicazione»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

«Diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 4 - Basi giuridiche del trattamento e disciplina del consenso

1. L'Agenzia Sarda delle Entrate è una pubblica amministrazione ai sensi dell'art. 1, c. 2, del D. Lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali trova il fondamento di liceità nella condizione prevista dall'art. 6, paragrafo 1 lett. e) del Regolamento (UE).
2. L'Agenzia tratta dati personali esclusivamente quando ricorre almeno una delle basi giuridiche di cui all'art. 6, par. 1, GDPR.
3. In qualità di autorità pubblica, i trattamenti dell'Agenzia trovano fondamento prevalentemente in:

Art. 6, par. 1, lett. c) GDPR: trattamento necessario per adempiere un obbligo legale;

Art. 6, par. 1, lett. e) GDPR: trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

4. I principali riferimenti normativi che legittimano i trattamenti dell'Agenzia sono:

a. Legge regionale n. 25/2016 istitutiva dell'ASE
b. Leggi regionali della Regione Autonoma della Sardegna in materia tributaria
c. Normativa nazionale e regionale in materia di riscossione e accertamento tributario.

5. Vengono integralmente recepiti nel regolamento le disposizioni del RGPD in ordine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

b) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

c) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

d) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;

e) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

6. Ai sensi dell'art. 6, par. 4, RGPD, laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, al fine di

verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo RGPD;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.
7. Il consenso dell'interessato, di cui al comma 5, lett. b), costituisce per l'Agenzia una base giuridica di carattere residuale. In ragione della natura pubblicistica del Titolare e dell'esercizio di funzioni di interesse pubblico e di pubblici poteri, il consenso non è utilizzato quale fondamento di liceità per i trattamenti connessi all'adempimento dei compiti istituzionali dell'Agenzia, per i quali trovano applicazione le condizioni di cui alle lettere a) e d) del medesimo comma 5. Il ricorso al consenso è ammesso esclusivamente per trattamenti che esulino dall'esercizio di pubblici poteri, nei soli casi in cui nessuna delle altre condizioni di liceità di cui all'art. 6, paragrafo 1, RGPD risulti applicabile, e a condizione che la manifestazione di volontà dell'interessato possa essere considerata genuinamente libera in ragione dell'assenza di squilibrio di potere tra le parti.
8. Nei casi in cui l'Agenzia faccia ricorso al consenso quale base giuridica del trattamento, sono rispettate le seguenti condizioni di validità ai sensi dell'art. 7 RGPD:
a) il consenso è prestato liberamente, per finalità specifiche, in forma informata e mediante una manifestazione di volontà inequivocabile dell'interessato, consistente in una dichiarazione o in un'azione positiva; non costituisce consenso valido il silenzio, le caselle pre-selezionate o l'inerzia dell'interessato;
b) il Titolare è in grado di dimostrare, in ogni momento, che l'interessato ha prestato il consenso al trattamento; a tal fine, la struttura competente cura la conservazione della documentazione attestante la raccolta del consenso, con indicazione della data, delle finalità e delle modalità della manifestazione di volontà;

c) qualora il consenso sia richiesto nell'ambito di una dichiarazione scritta che riguardi anche altre materie, la richiesta è presentata in forma chiaramente distinguibile dalle altre, con linguaggio semplice e accessibile; le clausole che non rispettano tale requisito sono prive di effetto;

d) l'interessato è informato, prima della prestazione del consenso, del diritto di revocarlo in qualunque momento; la revoca non pregiudica la liceità del trattamento basato sul consenso prima della revoca;

e) la prestazione del consenso non è condizionata all'erogazione di un servizio, qualora il trattamento cui il consenso si riferisce non sia necessario per la prestazione del medesimo servizio.

9. La revoca del consenso può essere esercitata dall'interessato mediante i medesimi canali previsti per l'esercizio dei diritti di cui all'art. 17 del presente Regolamento. Il Titolare garantisce che la revoca sia eseguibile con la stessa facilità con cui il consenso è stato prestato e dà seguito alla richiesta senza ingiustificato ritardo. La struttura competente per il trattamento aggiorna senza indugio il registro dei trattamenti e adotta le misure operative necessarie a cessare il trattamento dei dati per le finalità per le quali il consenso era stato rilasciato, fermo restando il trattamento eventualmente necessario in forza di altra base giuridica applicabile.

Art. 5 - Trattamento di categorie particolari di dati personali di cui all'art. 9 RGPD

1. In ossequio alla previsione di cui all'art. 9, paragrafo 1, RGPD, rientrano nella nozione di "categorie particolari di dati personali", i dati idonei a rivelare: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. È vietato trattare i dati di cui al precedente comma a meno che non si verifichi uno dei seguenti casi:

a) il trattamento è necessario per motivi di interesse pubblico rilevante previsti dal diritto dell'Unione o nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Ai sensi dell'art. 2-*sexies*, comma 2, D. Lgs. 196/03 e ss.mm.ii., si considera rilevante l'interesse pubblico relativo a trattamenti effettuati dall'Agenzia nelle seguenti materie:

- accesso a documenti amministrativi e accesso civico;
- svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
- attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;
- attività di controllo e ispettive;
- concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
- rapporti tra i soggetti pubblici e gli enti del terzo settore;
- attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
- instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

b) L'interessato ha prestato il proprio consenso esplicito al trattamento di tali categorie particolari di dati personali per una o più finalità specifiche.

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

e) Il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato.

f) Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

g) Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro e per la valutazione della capacità lavorativa del dipendente.

h) Il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 6 - Trattamento di dati personali relativi a condanne penali e reati di cui all'art. 10 RGPD

1. Ai sensi dell'art. 10 del Regolamento (UE) 2016/679 e dell'art. 2-octies del D. Lgs. 30 giugno 2003, n. 196, rientrano nella nozione di «dati personali relativi a condanne penali e reati» i dati personali concernenti le condanne penali, i reati o le connesse misure di sicurezza.

2. Nei limiti delle finalità istituzionali dell'Agenzia, il trattamento è consentito, in particolare, nei seguenti casi:

a) adempimento di obblighi ed esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, atti normativi secondari e contratti collettivi;

b) verifica o accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalla legge o da atti normativi secondari;

c) accertamento, esercizio o difesa di un diritto in sede giudiziaria, ovvero svolgimento di investigazioni difensive ai sensi della L. 7 dicembre 2000, n. 397;

d) esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalla normativa vigente in materia;

e) adempimento di obblighi previsti dalla normativa in materia di comunicazioni e informazioni antimafia, di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nonché produzione della documentazione prescritta dalla legge per la partecipazione a procedure di affidamento di contratti pubblici;

g) tutela della vita o dell'incolumità fisica dell'interessato o di un terzo, nei casi in cui l'interessato non possa prestare il proprio consenso per ragioni fisiche o giuridiche;

h) ogni ulteriore caso espressamente previsto da disposizioni di legge o da atti normativi secondari di natura pubblicistica.

4. Per ciascuna attività di trattamento rientrante nel presente articolo, il titolare indica nel Registro dei trattamenti la specifica base normativa applicabile tra quelle di cui al comma 3, nonché le misure di garanzia adottate a tutela dei diritti e delle libertà degli interessati.

CAPO II - SOGGETTI DEL TRATTAMENTO

Art. 7 - Titolare del Trattamento

1. Il Titolare del trattamento dei dati è l'Agenzia Sarda delle Entrate nel suo complesso, in ossequio alla previsione di cui all'art. 4, Paragrafo 1, n. 7, RGPD.
2. L'Agenzia agisce per mezzo del suo legale rappresentante, individuato nel Direttore Generale.
3. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
4. Il Titolare mette in atto misure tecniche ed organizzative adeguate, per garantire ed essere in grado di dimostrare, che il trattamento di dati personali venga effettuato in modo conforme al RGPD, con particolare riferimento all'adozione delle misure di sicurezza di cui all'art. 32 RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD.
5. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa e di bilancio, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
6. Il Titolare adotta misure appropriate per fornire all'interessato le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato e le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.
7. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua una valutazione dell'impatto del trattamento

sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 RGPD, in ragione della natura, dell'oggetto, del contesto e delle finalità del medesimo trattamento, sulla base dell'elenco delle tipologie di trattamento da sottoporre a valutazione di impatto redatto dal Garante per la protezione dei dati personali.

8. Il Titolare, prima di procedere al trattamento, qualora la richiamata valutazione di impatto sulla protezione dei dati indichi che il trattamento possa presentare un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio, consulta preventivamente il Garante per la protezione dei dati personali in ossequio alla previsione di cui all'art. 36 RGPD.

9. Il Titolare provvede a:

a) a definire gli obiettivi per la protezione dei dati personali oggetto di trattamento, provvedendo all'inserimento degli stessi nei documenti di programmazione e pianificazione dell'Agenzia affinché sia garantita l'adozione delle necessarie e idonee misure tecniche e organizzative atte a garantire che il trattamento sia effettuato conformemente al Codice, al RGPD e al presente Regolamento;

b) in ossequio alle previsioni di cui all'art. 29 RGPD ed all'art. 2-*quaterdecies*, comma 1, D. Lgs. 196/03 a designare i Dirigenti dei Servizi in cui si articola l'organizzazione dell'Agenzia, in quanto preposti al trattamento dei dati afferenti ai procedimenti amministrativi di competenza dei Settori assegnati, contenuti nelle banche dati, cartacee e informatiche, custodite presso gli stessi, quali persone fisiche destinatarie di specifici compiti connessi al trattamento dei dati, attribuendo loro i compiti e le funzioni di cui al successivo art. 8;

c) nominare, con proprio atto, il Responsabile della Protezione dei Dati (DPO);

d) notificare al Garante per la protezione dei dati personali la violazione dei dati che rappresenti un rischio per i diritti e le libertà degli interessati, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza ai sensi del disposto di cui all'art. 33 RGPD;

e) comunicare all'interessato, senza ingiustificato ritardo, la violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà dello stesso interessato in conformità alle previsioni di cui all'art. 34 RGPD;

f) assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

10. Nel caso di esercizio associato di funzioni e servizi che comportino il

trattamento di dati personali, nonché nel caso in cui la gestione di funzioni o servizi sia affidata all'Agenzia da parte di altre Amministrazioni ed organismi statali o regionali, allorché due o più Titolari determinano congiuntamente le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. In questi casi, i contitolari determinano in modo trasparente, mediante un accordo interno, le responsabilità di ciascuno in merito all'osservanza degli obblighi in materia di tutela del diritto alla riservatezza, con particolare riferimento all'esercizio dei diritti dell'interessato, e alle rispettive funzioni in relazione agli obblighi di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD. Il richiamato accordo, il cui contenuto essenziale è messo a disposizione degli interessati, disciplina adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati; esso può individuare una delle Amministrazioni contitolari del trattamento quale punto di contatto per gli interessati.

Art. 8 – Attribuzione di specifici compiti e funzioni connessi al trattamento dei dati in capo al Dirigente

1. I Dirigenti sono, con provvedimento del Direttore Generale, designati allo svolgimento di specifici compiti connessi al trattamento dei dati personali in conformità alle previsioni di cui all'art. 2-*quaterdecies,* comma 1, del D. Lgs. n. 196/2003.

2. I Dirigenti destinatari del provvedimento di designazione assumono tutti gli obblighi, le responsabilità ed i poteri funzionali a garantire la correttezza e la conformità dei trattamenti alle prescrizioni di cui al RGPD in relazione ad ogni singola fase del trattamento, agli obblighi di informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, al fornire istruzioni alle persone autorizzate al trattamento in ossequio alle previsioni di cui all'art. 29 RGPD e all'art. 2-*quaterdecies*, comma 2, D. Lgs. 196/03 e ss.mm.ii.;

3. Con il provvedimento di nomina, ai Dirigenti sono, pertanto, specificatamente attribuiti i seguenti compiti e funzioni:

a) individuare nominativamente ed autorizzare al trattamento dei dati le persone che nell'ambito del Servizio/Settore/Ufficio di competenza siano preposte ad attività di

trattamento sotto l'autorità diretta del titolare, a ciò provvedendo con propria determinazione, impartendo loro apposite istruzioni organizzative ed operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29 RGPD e art. 2–*quaterdecies*, comma 2, D. Lgs. 196/03;

b) garantire che dette persone autorizzate siano opportunamente istruite e formate al trattamento con riferimento alla tutela del diritto protezione dei dati nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati, in conformità alle previsioni di cui all'art. 32, paragrafo 4 del RGPD;

c) nominare i Responsabili del trattamento in tutti i casi in cui si faccia ricorso a soggetti esterni, persone fisiche o giuridiche, mediante affidamento di contratti di appalto relativi a lavori, servizi, forniture o consulenze che abbiano ad oggetto o comportino attività di trattamento di dati per conto dell'Agenzia. Il medesimo provvedimento di nomina andrà adottato nei confronti di autorità pubblica, servizio o organismo che tratti dati personali per conto del titolare del trattamento. I trattamenti da parte dei Responsabili sono disciplinati mediante contratto ovvero altro atto giuridico che vincoli il Responsabile del trattamento al Titolare del trattamento ai sensi dell'art. 28 RGPD o ai Dirigenti designati;

d) rendere l'informativa agli interessati ai sensi degli artt. 12 e ss. RGPD, anche mediante adeguamento puntuale e tempestivo della modulistica resa disponibile dall'Agenzia. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato;

e) verificare e controllare che, nell'ambito del Servizio assegnato, il trattamento dei dati sia effettuato nel rispetto dei principi di cui all'art. 5 del RGPD e, in particolare, assicurare che i dati personali siano trattati in modo lecito, corretto e trasparente;

f) garantire, in caso di raccolta, che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità;

g) assicurare che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

h) adottare, tenuto conto dello stato dell'arte, della natura, dell'oggetto, del contesto, delle finalità del trattamento e, in particolar modo, del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche, tutte le misure tecniche ed organizzative,

ivi comprese la pseudonimizzazione e la cifratura dei dati personali, necessarie per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'articolo 32 del RGPD;

i) assistere il Titolare al fine di consentire allo stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del RGPD;

j) assistere il Titolare nel garantire il rispetto degli obblighi di sicurezza di cui all'art. 32 RGPD, mettendo in atto misure tecniche e organizzative adeguate in grado di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, ciascun Dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali provvede a formulare, al Direttore Generale, una proposta di adozione delle misure necessarie ed una stima dei costi preventivati per la realizzazione degli interventi proposti;

k) garantire l'adozione di adeguate misure di sicurezza in grado di assicurare il tempestivo ripristino della disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico; qualora a ciò non possa provvedere immediatamente e con i mezzi assegnati, ciascun Dirigente designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali provvede a formulare, all'organo di vertice, una proposta di adozione delle misure necessarie ed una stima dei costi preventivati per la realizzazione degli interventi proposti;

l) assicurare l'adozione di procedure volte a testare, verificare e valutare costantemente l'efficacia delle misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento;

m) informare senza ingiustificato ritardo il Titolare del trattamento, in caso di violazione dei dati personali;

n) assistere il Titolare nelle procedure di notifica di violazione dei dati personali al Garante per la protezione dei dati personali e di comunicazione di violazione dei dati personali all'interessato ai sensi degli artt. 33 e 34 del RGPD;

o) assistere il Titolare del Trattamento nell'effettuazione della Valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD, consultato il Responsabile della Protezione dei Dati (DPO), e nella successiva eventuale attività di consultazione preventiva del Garante per la protezione dei dati personali in conformità alla previsione di cui all'art. 36 del RGPD;

p) affiancare il Titolare, in conformità alle disposizioni di cui all'art. 30, paragrafo 1 e 2, del RGPD, nell'istituzione e aggiornamento del Registro delle attività di

trattamento, secondo quanto meglio definito dal successivo art. 17 del presente Regolamento. In particolare, con cadenza almeno annuale, ciascun Dirigente, provvede ad istituire le nuove eventuali schede relative a nuove categorie di trattamento e ad aggiornare le schede del Registro dei trattamenti di propria competenza.

q) garantire che il Responsabile della Protezione dei Dati (DPO) designato dal Titolare del trattamento, sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e riceva un adeguato affiancamento nell'esecuzione dei suoi compiti;

r) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa e per consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto incaricato;

s) informare immediatamente il Titolare qualora, a suo parere, un'istruzione impartita da quest'ultimo violi la normativa comunitaria o nazionale relativa alla protezione dei dati;

t) custodire e controllare i dati personali di competenza affinché sia ridotto al minimo il rischio di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

u) aggiornare sistematicamente la mappatura dei Procedimenti amministrativi di competenza del Servizio assegnato alla sua direzione e censire periodicamente le banche dati di pertinenza;

v) assicurare che il personale facente capo al Servizio di propria pertinenza si attenga, nel trattamento dei dati, al perseguimento delle finalità per le quali il trattamento è consentito e garantire che vengano compiute, in relazione a tale trattamento, solo le operazioni strettamente necessarie al perseguimento delle finalità istituzionali;

w) garantire la tempestiva emanazione, per iscritto, di direttive ed ordini di servizio rivolti al personale assegnato al Servizio di propria pertinenza, previo consulto del Responsabile della Protezione dei dati (DPO), necessari a garantire il rispetto della normativa in materia di trattamento dei dati personali;

x) vigilare sul rispetto da parte delle persone autorizzate al trattamento circa gli obblighi di corretta e lecita raccolta dei dati, di utilizzazione, di comunicazione nonché di diffusione degli stessi a mezzo pubblicazione all'Albo Pretorio On line (ai sensi dell'art. 32, L. 69/2009) ovvero nella Sezione del sito istituzionale dell'Agenzia denominata "Amministrazione Trasparente" (ai sensi del D. Lgs. 33/2013 e ss.mm.ii.).

y) vigilare sul rispetto del diritto alla riservatezza nell'ambito dei procedimenti di accesso documentale ai sensi e nei limiti degli artt. 22 e ss. L. 241/90, ovvero nei procedimenti di richiesta di accesso civico prevista dagli artt. 5, comma 2, e 5-bis, D. Lgs. 33/2013 di pertinenza del proprio Settore. Il medesimo obbligo di vigilanza troverà applicazione anche nelle richieste di informazioni formulate dai consiglieri regionali ai sensi delle disposizioni di cui all'art. 105 del Regolamento sul funzionamento del Consiglio Regionale della Sardegna.

z) comunicare tempestivamente al Titolare, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 RGPD, riguardanti l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

aa) disporre periodiche verifiche, anche per il tramite del Responsabile della Protezione dei Dati (DPO), sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati ed alla formazione ed istruzione dei dipendenti autorizzati al trattamento.

Art. 9 – Responsabile del Trattamento dei dati

1. In tutti i casi in cui l'Agenzia, nell'ambito dell'affidamento di un incarico, un servizio, un lavoro, una fornitura, una collaborazione o una consulenza, affidi all'esterno un trattamento di dati da effettuarsi per conto della stessa, il soggetto affidatario, sia esso persona fisica o persona giuridica, dovrà essere preventivamente individuato quale Responsabile del trattamento ai sensi dell'art. 28 RGPD.

2. In ossequio alla previsione di cui all'art. 8, comma 3, lett. c) del presente Regolamento, l'obbligo di provvedere all'esaustiva ed analitica disciplina dei trattamenti da parte dei Responsabili, necessari ad impartire agli stessi le istruzioni documentate sui trattamenti affidati, analiticamente contenute nel contratto o altro atto giuridico, è posto in capo ai singoli Dirigenti.

3. Per effetto delle previsioni di cui al precedente comma ed in conformità alle disposizioni di cui all'art. 28, paragrafo 3 del RGPD i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o altro atto giuridico adottato dal Direttore Generale o dal Dirigente competente.

4. Il contratto o altro atto giuridico ex art. 28 RGPD di cui al precedente comma deve includere almeno: oggetto, durata, natura, finalità, tipologia dati e categorie interessati,

obblighi e diritti del Titolare, misure di sicurezza, gestione sub-responsabili, assistenza su diritti interessati, assistenza su data breach, cancellazione, restituzione dati e verifiche. Ogni ricorso a sub-responsabili richiede autorizzazione preventiva o generale del Titolare e adeguate garanzie.

Art. 10 – Persone autorizzate al trattamento dei dati

1. Le persone autorizzate al trattamento dei dati sono le persone fisiche, dipendenti del Titolare, espressamente individuate ed autorizzate con atto determinativo adottato da ciascun Dirigente assegnatario delle risorse umane che trattino dati sotto l'autorità diretta e nell'ambito del Servizio di competenza.
2. In ossequio alle previsioni di cui all'art. 8, comma 3, lett. a) e b) del presente Regolamento, ciascun Dirigente individua e nomina, con propria determinazione, le persone autorizzate al trattamento dei Servizi/Settori/Uffici/ nei quali si articola la macrostruttura e le microstrutture dell'Agenzia, impartendo loro apposite istruzioni organizzative e operative per il corretto, lecito, pertinente e sicuro trattamento dei dati in ossequio alle previsioni di cui all'art. 29 RGPD e all'art. 2-*quaterdecies*, D. Lgs. 196/03 e ss.mm.ii.
3. Tenuto conto dei procedimenti amministrativi di pertinenza degli Uffici di assegnazione delle persone autorizzate al trattamento, del censimento delle Banche Dati cartacee e/o informatiche trattate dai singoli Uffici per la gestione dei procedimenti amministrativi di competenza, ciascun Dirigente, in quanto designato allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali, provvede a rilevare il fabbisogno formativo e, avvalendosi del Responsabile della Protezione dei Dati, ad istruire e formare le persone autorizzate al trattamento dei dati con riferimento alla tutela del diritto alla riservatezza, nonché alle misure tecniche e organizzative da osservarsi per ridurre i rischi di trattamenti non autorizzati o illeciti, di perdita, distruzione o danno accidentale dei dati.
4. La determinazione di individuazione degli autorizzati contiene le istruzioni e le regole tecniche e operative che le persone autorizzate al trattamento sono tenute a seguire nelle operazioni di trattamento dei dati personali assegnate nonché l'indicazione dei loro obblighi e delle loro responsabilità, con particolare riferimento a:

a. l'accesso alle banche dati informatiche;
b. la conservazione dei supporti informatici e/o cartacei contenenti dati personali;

c. la riservatezza ed il riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali;

d. la custodia ed il controllo dei dati personali affidati;

e. la conservazione dei dati in conformità alle misure di sicurezza adottate dall'Agenzia;

f. l'utilizzo della postazione di lavoro assegnata;

g. il collegamento ad Internet;

h. l'utilizzo dei supporti di memoria magnetici e ottici;

i. l'utilizzo della posta elettronica.

5. Le persone autorizzate sono tenute alla riservatezza con riferimento ai dati di cui siano venuti a conoscenza nell'esercizio delle funzioni istituzionali loro ascritte e provvedono al loro trattamento attenendosi scrupolosamente alle istruzioni impartite dal Dirigente designato, al quale rispondono.

6. In ossequio alle previsioni di cui all'art. 5 RGPD, le persone autorizzate devono assicurare che, nel corso del trattamento, i dati personali siano:

- trattati in modo lecito, corretto e trasparente;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione);
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

7. Le persone autorizzate sono beneficiarie di interventi formativi che prevedano richiami di aggiornamento periodici ai sensi delle disposizioni di cui agli artt. 29 e 32.4 del RGPD.

8. L'atto di autorizzazione dovrà contenere l'ambito di trattamento, i profili di accesso, le istruzioni operative, il richiamo all'obbligo di tutela del segreto d'ufficio,

la durata e le modalità di revoca. Alla cessazione del rapporto o del cambio mansione, i profili di accesso sono revocati senza ritardo.

Art. 11 – Persone autorizzate al trattamento dei dati, non dipendenti del Titolare

1. Le persone fisiche, non legate all'Agenzia da un contratto di lavoro subordinato, che abbiano accesso ai dati personali trattati per svolgere compiti di supporto agli stessi che comportino un trattamento di dati (a titolo meramente esemplificativo e non esaustivo: i tirocinanti, i volontari, i collaboratori e, tutti quei soggetti che operano temporaneamente all'interno della struttura organizzativa del Titolare), devono essere preventivamente individuate, con determinazione adottata dal Dirigente assegnatario, quali persone autorizzate al trattamento.
2. Le persone autorizzate sono soggette agli stessi obblighi cui sono sottoposti le persone autorizzate dipendenti del Titolare, in modo da garantire il pieno rispetto della tutela della riservatezza delle persone fisiche alle quali si riferiscono i dati oggetto di trattamento.
3. Le persone autorizzate sono beneficiarie di interventi formativi che prevedano richiami di aggiornamento periodici ai sensi delle disposizioni di cui agli artt. 29 e 32.4 del RGPD.
4. È acquisita specifica dichiarazione di riservatezza sottoscritta e sono impartite istruzioni scritte; al termine, è verificata la restituzione dei supporti e la disattivazione degli accessi.

Art. 12 - Procedura per affidamenti a fornitori e Data Processing Agreement (art. 28 RGPD)

1. La presente procedura si applica a tutti gli affidamenti, contratti, convenzioni o incarichi (a titolo esemplificativo: appalti di servizi/forniture, consulenze, manutenzione, assistenza tecnica, servizi informatici, cloud, gestione piattaforme, call center, postalizzazione, archiviazione, conservazione digitale) che comportino, anche potenzialmente, trattamenti di dati personali per conto dell'Agenzia.
2. Prima dell'affidamento, il Dirigente competente (o il RUP, se previsto) determina e documenta la corretta qualificazione privacy del rapporto, distinguendo almeno tra:

a) Responsabile del trattamento (art. 28 RGPD), quando il fornitore tratta dati per conto dell'Agenzia e secondo istruzioni documentate;

b) Titolare autonomo (art. 4 RGPD), quando il fornitore determina finalità e mezzi del trattamento in autonomia;

c) Contitolare (art. 26 RGPD), quando finalità e mezzi sono determinati congiuntamente;

d) Comunicazione di dati tra titolari (art. 6 RGPD), quando l'Agenzia comunica dati a un altro titolare per fini propri di quest'ultimo, sulla base di idonea base giuridica.

3. In caso di dubbio la valutazione è svolta con il supporto del Referente privacy e, ove necessario, del DPO.

4. Istruttoria preliminare e minimizzazione. Il Dirigente competente/RUP:

a) descrive finalità, categorie di dati, categorie di interessati, operazioni di trattamento, durata, sistemi e canali;

b) verifica la minimizzazione (riduzione dati e tempi), l'eventuale pseudonimizzazione/anonimizzazione, e le misure organizzative idonee;

c) verifica se il trattamento implica dati particolari (art. 9 RGPD) o dati relativi a reati/condanne (art. 10 RGPD) o trattamenti su larga scala o monitoraggi sistematici.

5. Prima della stipula, l'Agenzia acquisisce e valuta, in modo proporzionato al rischio:

a) informazioni sulle misure tecniche e organizzative (art. 32 RGPD) e, se pertinente, certificazioni/standard;

b) sedi e luoghi di trattamento e di conservazione;

c) eventuale ricorso a sub-responsabili e relativi ruoli;

d) gestione incidenti e tempi di notifica;

e) eventuali trasferimenti extra UE/SEE e basi giuridiche applicabili.

6. L'esito della valutazione è documentato nel fascicolo dell'affidamento.

7. Qualora il fornitore operi quale responsabile del trattamento, l'affidamento deve prevedere un Data Processing Agreement (clausole nel contratto principale o atto separato) contenente almeno quanto richiesto dall'art. 28, par. 3, RGPD, e in particolare:

a) oggetto, durata, natura e finalità del trattamento;

b) tipologie di dati personali e categorie di interessati;

c) obbligo di trattare i dati solo su istruzioni documentate dell'Agenzia;

d) obblighi di riservatezza del personale autorizzato;

e) misure di sicurezza (art. 32) adeguate al rischio;

f) disciplina dei sub-responsabili (autorizzazione preventiva o generale; obbligo di imporre condizioni equivalenti);

g) assistenza all'Agenzia per l'evasione delle richieste degli interessati;

h) assistenza per obblighi di sicurezza, DPIA, consultazione preventiva;

i) gestione e notifica delle violazioni di dati personali (data breach) e cooperazione;

j) restituzione o cancellazione dei dati a fine rapporto e cancellazione delle copie, salvo obblighi di legge;

k) messa a disposizione delle informazioni necessarie e diritto di audit/verifica dell'Agenzia;

l) divieto di uso dei dati per finalità proprie del fornitore e divieto di comunicazione a terzi non autorizzati.

8. L'eventuale autorizzazione all'uso di sub-responsabili deve essere espressa nel DPA. In caso di autorizzazione generale, il responsabile informa l'Agenzia delle variazioni (aggiunta/sostituzione sub-responsabili) con congruo preavviso, consentendo all'Agenzia di opporsi per motivi legittimi. Il responsabile resta pienamente responsabile verso l'Agenzia dell'operato dei sub-responsabili.

9. Se il trattamento comporta trasferimenti di dati verso Paesi terzi o accessi da Paesi terzi, o l'uso di servizi cloud con potenziale accesso extra UE/SEE, il Dirigente competente/RUP verifica, con supporto del Referente privacy, la base giuridica del trasferimento (artt. 44–49 RGPD) e la disponibilità di garanzie adeguate, incluse eventuali clausole contrattuali standard e misure supplementari proporzionate al rischio.

10. Il DPA deve prevedere che il responsabile informi l'Agenzia senza ingiustificato ritardo e, salvo motivata impossibilità, entro un termine massimo predefinito (es. 24 ore) dalla conoscenza della violazione, fornendo tutte le informazioni necessarie per le valutazioni di notifica/comunicazione ai sensi degli artt. 33 e 34 RGPD e cooperando alle attività di contenimento e ripristino.

11. Il DPA (o le clausole privacy nel contratto) è predisposto sulla base di modelli standard dell'Agenzia. L'atto è sottoposto al DPO per parere di conformità. La sottoscrizione avviene secondo le competenze interne (DG o soggetto legittimato),

su proposta del Dirigente competente.

12. Durante l'esecuzione contrattuale, il Dirigente competente:

a) aggiorna le istruzioni documentate;

b) verifica periodicamente il rispetto delle misure e degli obblighi del DPA, anche tramite evidenze documentali;

c) valuta la necessità di audit o verifiche, in particolare per trattamenti ad alto rischio, dati particolari/penali, cloud o fornitori critici;

d) gestisce, in coordinamento con privacy/DPO, eventuali non conformità e azioni correttive.

13. Alla cessazione del contratto o dell'incarico, il responsabile:

a) restituisce i dati e/o li cancella secondo le istruzioni dell'Agenzia;

b) fornisce attestazione documentata dell'avvenuta cancellazione e della cancellazione delle copie, salvo obblighi legali di conservazione;

c) disattiva gli accessi e restituisce credenziali, dispositivi e supporti eventualmente assegnati.

14. Tutta la documentazione (qualificazione del rapporto, due diligence, DPA, istruzioni, evidenze di controllo, incidenti, attestazioni di cancellazione) è conservata nel fascicolo dell'affidamento secondo i tempi di conservazione applicabili.

Art. 13 - Responsabile della Protezione dei dati (DPO)

1. Il Responsabile della protezione dei dati (DPO), è individuato, in ossequio alla previsione normativa di cui all'art. 37, paragrafo 5 e 6 RGPD ed in conformità alle disposizioni dettate dal Provvedimento del Garante Privacy n. 9589104 del 29/04/2021 recante "*Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*", qui interamente richiamato, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati che caratterizzano lo specifico settore di appartenenza dell'Agenzia, in quanto la liceità del trattamento dei dati personali in questo ambito dipende dalla corretta applicazione delle regole di volta in volta previste dalla disciplina di settore, nonché della capacità del DPO di dare corretto adempimento ai compiti di cui all'art. 39 del Regolamento. Per quanto concerne la conoscenza di norme e prassi in materia di protezione dei dati personali, essa può essere dimostrata, in primo luogo, attraverso una documentata esperienza professionale e/o anche attraverso la partecipazione ad

attività formative specialistiche (ad esempio, master, corsi di studio e professionali, specie se risulta documentato il livello di acquisizione delle conoscenze). Analogamente, la conoscenza specialistica sarà dimostrata dalle attività, dalle esperienze lavorative e professionali svolte, risultanti, ad esempio, dal curriculum e dalle autocertificazioni presentate. Particolare valore potrà assumere l'eventuale esperienza del candidato in organizzazioni simili a quella del titolare.

2. La funzione di DPO può essere esercitata in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'Agenzia. In tal caso, è indispensabile che le persone fisiche appartenenti alla persona giuridica che operano quali DPO dell'Agenzia possiedano tutti i requisiti richiesti dall'art. 37, paragrafo 5, RGPD e, in particolare, abbiano maturato approfondita conoscenza con riferimento alle Amministrazioni Pubbliche e, segnatamente, alla Regione Autonoma della Sardegna, agli Enti, Agenzie ed Aziende collegati o dipendenti, alla loro organizzazione, alle norme e procedure amministrative applicabili.

3. I compiti attribuiti al DPO sono indicati in apposito contratto di servizi. Il DPO esterno è tenuto a procedere sistematicamente nell'aggiornamento della propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, da comprovare documentalmente.

4. Il DPO può essere altresì individuato tra le risorse umane dell'Agenzia, nella figura di un dipendente in possesso di competenze e professionalità adeguate alla natura dell'incarico, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dei dati all'interno dell'organizzazione dell'Agenzia. Il Titolare del trattamento provvede affinché il DPO interno mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

5. In ossequio alla previsione di cui all'art. 37, paragrafo 3, RGPD, è possibile l'affidamento dell'incarico di DPO ad un unico soggetto, anche esterno, designato da più Enti mediante esercizio associato della funzione.

6. Il DPO è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) informare e fornire consulenza al Titolare del trattamento, ai Dirigenti designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali ed alle Persone autorizzate al trattamento in merito agli obblighi derivanti dal

RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati personali;

b) partecipare alle riunioni di coordinamento dei Dirigenti e del personale del comparto che abbiano per oggetto questioni inerenti la protezione dei dati personali;

c) provvedere alla formazione dei Dirigenti e del personale del comparto in merito agli obblighi derivanti dal RGPD in conformità alle disposizioni vigenti;

d) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché l'osservanza delle politiche adottate dal Titolare del trattamento o dai Dirigenti in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

e) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'art. 35 RGPD. In particolare, il Titolare e/o i Dirigenti, si consulta/no con il DPO in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

f) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare al Garante;

g) tenere, il Registro delle attività dei trattamenti di cui al successivo art. 17, sotto la responsabilità del Titolare del trattamento;

h) fornire supporto tecnico-giuridico e vigilare circa l'applicazione dei principi in materia di protezione dei dati personali in relazione alle attività rilevanti ai fini del trattamento realizzate dalle seguenti figure:

a. Social media manager;
b. Responsabile per la transizione alla modalità digitale;
c. Responsabile per Responsabile della gestione documentale e degli archivi;
d. Responsabile della conservazione;

e. Responsabile della sicurezza informatica;

f. Amministratore di Sistema.

7. Il Titolare del trattamento ed i Dirigenti assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine provvedono a:

a) mettere a disposizione del DPO le risorse umane e materiali preordinate a consentirgli l'ottimale svolgimento dei compiti e delle funzioni assegnate, garantendogli l'accesso ai dati personali ed ai trattamenti;

b) garantire al DPO il supporto dell'Amministratore di Sistema Informatico dell'Agenzia per la risoluzione di tutte le problematiche relative alla protezione dei dati personali che abbiano una incidenza diretta o indiretta sulle attività di trattamento effettuate con l'ausilio di strumenti informatici;

c) fornire al DPO tutte le informazioni in merito al trattamento dei dati personali ed alle correlate misure di sicurezza adottate dall'Agenzia al fine di consentire allo stesso DPO di fornire all'Agenzia una consulenza funzionale con riferimento alle problematiche oggetto di analisi. Il parere del DPO sulle decisioni che impattano sulla protezione dei dati è obbligatorio, ma non vincolante. Nel caso in cui la decisione assunta determini condotte difformi da quelle raccomandate dal DPO, è necessario che il Titolare del trattamento o i Dirigenti motivino specificamente detta decisione;

d) consultare tempestivamente il DPO qualora si verifichi una violazione dei dati o altro incidente in grado di avere rilevanza sui dati personali trattati dall'Agenzia.

8. Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

9. La figura di DPO è incompatibile con qualunque figura deputata a determinare le finalità o i mezzi del trattamento all'interno dell'Agenzia; in particolare, risultano con la stessa incompatibili:

a) la funzione di Responsabile per la prevenzione della corruzione e per la trasparenza;

b) la funzione di Dirigente o di personale del comparto con funzioni che determinino la finalità e i mezzi di trattamento, secondo quanto previsto dall'art. 38, par. 6 RGPD).

10. Il DPO opera in posizione di autonomia nello svolgimento dei compiti attribuiti;

in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare ad una specifica questione attinente alla normativa in materia di protezione dei dati.

11. Il DPO non può essere rimosso o penalizzato dal Titolare del trattamento e dai Dirigenti per l'adempimento dei propri compiti.

12. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare del trattamento ed ai Dirigenti designati allo svolgimento di specifici compiti e funzioni connessi al trattamento di dati personali.

Art. 14 – Referente Privacy

L'Agenzia individua, con provvedimento del Direttore Generale di durata triennale, rinnovabile, il referente privacy che funga da punto di contatto tra il DPO e le diverse articolazioni aziendali, garantendo la continuità dei flussi informativi e lo svolgimento delle attività che richiedano il supporto del DPO.

CAPO III – PRINCIPI

Art. 15 - Principi e responsabilizzazione

1. Vengono integralmente recepiti, nell'organizzazione interna del Titolare, i principi del RGPD, per effetto dei quali, i dati personali sono:

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

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

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati in base al c.d. principio di "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 base del principio di "esattezza";

e) conservati in una forma che consenta l'identificazione degli interessati per un arco

di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "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 in base ai principi di "integrità e riservatezza";

2. Il Titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

Art. 16 – Informativa all'interessato

1. Il Titolare del trattamento e ciascun Dirigente assicurano, anche avvalendosi dei dipendenti assegnati che, al momento della raccolta dei dati personali, agli interessati sia fornita apposita informativa secondo le modalità previste dall'art. 13, RGPD, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

2. L'informativa è fornita, in linea di principio, per iscritto, anche in formato elettronico, soprattutto nel contesto di servizi resi in modalità *online*.

3. L'informativa può essere fornita con le seguenti modalità:

a) attraverso apposita modulistica resa disponibile agli interessati;

b) attraverso avvisi agevolmente accessibili al pubblico, posti nei locali di accesso agli Uffici dell'Agenzia ovvero diffusi attraverso pubblicazione sul sito istituzionale dell'Agenzia;

c) attraverso apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti e di altri soggetti chiamati a prestare la loro attività per conto dell'Agenzia;

d) in sede di pubblicazione dei bandi, degli avvisi, delle lettere d'invito.

4. L'informativa contiene il seguente contenuto minimo:

a) l'identità ed i dati di contatto del Titolare;

b) i dati di contatto del DPO;

c) le indicazioni in merito alle finalità del trattamento;

d) la base giuridica del trattamento;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) l'eventuale intenzione del Titolare di trasferire i dati personali ad un Paese terzo o a un'organizzazione internazionale;

g) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;

h) l'esistenza del diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;

i) qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualunque momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

j) l'indicazione in merito al fatto che la comunicazione dei dati personali sia un obbligo legale o contrattuale, ovvero un requisito necessario per la conclusione di un contratto, ovvero se l'interessato abbia l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione dei dati;

k) il diritto di proporre reclamo al Garante per la protezione dei dati personali;

l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

5. 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 ritenuta utile.

6. Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato, ciascun Dirigente, anche avvalendosi dei dipendenti assegnati agli Uffici/Servizi ricompresi nell'Area Organizzativa ascritta alla sua direzione, fornisce all'interessato le seguenti informazioni:

a) l'identità ed i dati di contatto del Titolare;

b) i dati di contatto del DPO;

c) le indicazioni in merito alle finalità del trattamento;

d) la base giuridica del trattamento;

e) le categorie di dati personali trattati;

f) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

g) l'eventuale intenzione del Titolare di trasferire i dati personali ad un Paese terzo o a un'organizzazione internazionale;

h) il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;

i) l'esistenza del diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;

j) qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualunque momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

k) il diritto di proporre reclamo al Garante per la protezione dei dati personali;

l) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

m) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

7. L'informativa, nei casi di cui al precedente comma 6, deve essere fornita entro un termine ragionevole dall'ottenimento dei dati personali e, al più tardi, entro un mese. Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, l'informativa deve essere fornita al più tardi al momento della prima comunicazione all'interessato. Nel caso sia invece prevista la comunicazione ad altro destinatario, l'informativa deve essere fornita non oltre la prima comunicazione dei dati personali.

Art. 17 - Diritti dell'interessato e revoca del consenso

1. L'Agenzia garantisce l'esercizio dei diritti dell'interessato previsti dagli artt. 12–22 del Regolamento (UE) 2016/679 (di seguito "RGPD"), assicurando modalità di presentazione delle istanze semplici, accessibili e idonee a consentire la corretta identificazione del richiedente.

2. Le istanze possono essere presentate mediante i canali istituzionali dell'Agenzia (a titolo esemplificativo: posta elettronica/PEC, sportello, modulistica pubblicata sul sito istituzionale), indicando almeno: i dati identificativi del richiedente, un recapito per le comunicazioni, l'oggetto della richiesta e ogni elemento utile a individuare il trattamento cui si riferisce.

3. L’Agenzia può richiedere informazioni ulteriori, ove necessarie per confermare l’identità dell’interessato o per meglio circoscrivere la richiesta, nel rispetto del principio di minimizzazione. Qualora la richiesta sia presentata da un delegato o rappresentante, l’Agenzia acquisisce idonea documentazione comprovante i poteri di rappresentanza.

4. Le istanze sono prese in carico senza ingiustificato ritardo e comunque entro i termini di cui all’art. 12 RGPD. L’Agenzia fornisce riscontro all’interessato entro un mese dal ricevimento della richiesta; tale termine può essere prorogato, in relazione alla complessità e al numero delle richieste, di ulteriori due mesi, dandone comunicazione motivata all’interessato entro un mese dal ricevimento.

5. L’istruttoria è curata dalla struttura competente per materia e/o dal dirigente responsabile del trattamento cui l’istanza si riferisce, in coordinamento con il Referente privacy. Il Responsabile della Protezione dei Dati (DPO) è coinvolto, ove necessario, per supporto e parere sugli aspetti interpretativi e di conformità.

6. L’esercizio dei diritti è gratuito. Qualora le richieste siano manifestamente infondate o eccessive, anche per il loro carattere ripetitivo, l’Agenzia può: (a) addebitare un contributo spese ragionevole, tenendo conto dei costi amministrativi sostenuti, oppure (b) rifiutare di soddisfare la richiesta. In tali casi l’Agenzia motiva adeguatamente la decisione e informa l’interessato della possibilità di proporre reclamo al Garante per la protezione dei dati personali e di adire le opportune sedi giurisdizionali.

7. Nel dare seguito alle richieste di accesso, rettifica, cancellazione, limitazione, portabilità e opposizione, l’Agenzia valuta l’applicabilità del diritto richiesto alla luce della base giuridica del trattamento, delle finalità perseguite e degli eventuali obblighi di legge o regolamentari di conservazione e trattamento. In particolare, la cancellazione o la limitazione possono non essere accordate quando il trattamento sia necessario per adempiere un obbligo legale o per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri, ovvero per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria, fermo restando l’obbligo di motivare il riscontro.

8. Qualora l’evasione dell’istanza implichi la comunicazione di dati personali riferiti a terzi, l’Agenzia adotta misure idonee a tutelare i diritti e le libertà altrui, anche mediante oscuramento/selezione dei dati non pertinenti, secondo criteri di proporzionalità e minimizzazione, e nel rispetto delle discipline applicabili in materia di accesso ai documenti amministrativi e trasparenza.

9. L’Agenzia assicura la tracciabilità delle istanze e degli esiti mediante un registro interno delle richieste, contenente almeno: data di ricezione, tipologia di diritto esercitato, struttura competente, attività istruttorie svolte, esito e data di riscontro. Il registro è conservato per il tempo necessario alle finalità di rendicontazione e controllo interno e comunque nel rispetto dei principi di limitazione della conservazione e minimizzazione.

10. L'interessato ha il diritto di revocare in qualunque momento il consenso al trattamento dei propri dati personali nei casi in cui il trattamento sia fondato esclusivamente su tale base giuridica. La revoca non pregiudica la liceità del trattamento effettuato sulla base del consenso prima della revoca medesima. Qualora il trattamento trovi fondamento anche in una diversa condizione di liceità ai sensi dell'art. 6, paragrafo 1, RGPD, l'Agenzia ne dà comunicazione all'interessato contestualmente al riscontro sulla revoca, indicando la base giuridica alternativa e le conseguenze sul trattamento in corso.

11. La revoca del consenso è esercitata dall'interessato mediante i medesimi canali istituzionali previsti al comma 2 del presente articolo. L'Agenzia garantisce che la revoca sia eseguibile con la stessa facilità con cui il consenso è stato originariamente prestato. In particolare:

a) qualora il consenso sia stato acquisito mediante modulo cartaceo o digitale, l'Agenzia mette a disposizione, attraverso i medesimi canali di raccolta, un apposito modulo di revoca ovvero indica le istruzioni per esercitare tale diritto senza necessità di giustificazione e senza oneri per l'interessato;

b) qualora il consenso sia stato acquisito in forma elettronica, attraverso interfacce digitali o sistemi informativi dell'Agenzia, la funzione di revoca è accessibile con modalità di pari semplicità rispetto a quella di prestazione del consenso, senza che siano frapposti passaggi aggiuntivi o ostacoli tecnici;

c) la richiesta di revoca non è subordinata all'indicazione delle motivazioni e non può essere condizionata alla preventiva verifica di requisiti ulteriori rispetto all'identificazione del richiedente.

12. L'Agenzia dà seguito alla revoca senza ingiustificato ritardo e comunque entro i termini di cui all'art. 12 RGPD, applicabili in quanto compatibili. La struttura competente per il trattamento, ricevuta la richiesta di revoca:

a) cessa il trattamento dei dati per le finalità coperte dal consenso revocato con effetto immediato, salvo che la cessazione immediata non sia tecnicamente praticabile per

ragioni documentate, nel qual caso il termine non può comunque essere superiore a quindici giorni dalla ricezione della richiesta;

b) aggiorna il registro delle attività di trattamento di cui all'art. 19 del presente Regolamento, annotando la revoca, la data di ricezione e la data di effettiva cessazione del trattamento;

c) verifica se i dati personali trattati sulla base del consenso revocato debbano essere cancellati ai sensi dell'art. 17, paragrafo 1, lett. b), RGPD ovvero se sussista una diversa base giuridica che ne legittimi la conservazione, dandone motivata comunicazione all'interessato nel riscontro;

d) informa le eventuali strutture interne o i responsabili del trattamento esterni che abbiano avuto accesso ai dati sulla base del consenso revocato, affinché adottino le corrispondenti misure operative.

L'esito delle attività di cui al presente comma è comunicato all'interessato nel riscontro scritto, con indicazione delle misure adottate e, ove applicabile, delle ragioni per cui la conservazione dei dati prosegua in forza di altra base giuridica.

13) Resta fermo il diritto dell'interessato di proporre reclamo al Garante per la protezione dei dati personali e di adire le competenti sedi giurisdizionali ai sensi degli artt. 77–79 RGPD.

Art. 18 – Formazione e sensibilizzazione del personale

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il Titolare del trattamento promuove, all'interno dell'Agenzia, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore del diritto alla riservatezza dei dati, al fine di migliorare la qualità dei servizi resi nei confronti degli interessati.

A tale riguardo, il presente regolamento riconosce nell'attività di formazione ed informazione, resa nei confronti del personale uno degli strumenti essenziali per la responsabilizzazione e la sensibilizzazione dei diversi soggetti coinvolti nel trattamento di dati personali.

2. Al fine di assicurare la conoscenza capillare delle disposizioni contenute nel RGPD e nel presente Regolamento, al momento dell'ingresso in servizio è consegnata ad ogni dipendente una specifica comunicazione, che richiama l'apposita clausola inserita nel

contratto di lavoro, contenente i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale.

Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.

3. Il presente Regolamento è pubblicato sul sito istituzionale dell'Agenzia, nella Sezione Amministrazione Trasparente, Sotto Sezione di I Livello "Altri Contenuti", Sotto Sezione di II Livello "Privacy".

4. Il Titolare organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, con cadenza annuale, in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione dei rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso illegittimo ai dati conservati e trattati dai dipendenti dell'Agenzia.

Gli interventi formativi ed informativi, sono altresì finalizzati a rendere edotto tutto il personale dirigenziale e del comparto, sulle misure di sicurezza adottate dall'Agenzia ai sensi dell'art. 32 RGPD al fine di assicurare l'integrità, la riservatezza, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

5. La formazione in materia di tutela del diritto alla riservatezza e prevenzione dei rischi di violazione dei dati personali viene integrata con la formazione in tema di trasparenza e di diritto di accesso, con particolare riguardo al corretto bilanciamento tra il diritto alla protezione dei dati personali e le contrapposte esigenze di trasparenza dell'azione amministrativa, nonché di diritto di accesso ai documenti amministrativi (di cui agli artt. 22 e ss. L. 241/90) e di diritto di accesso civico generalizzato (di cui all'art. 5, comma 2, D. Lgs. 33/2013), nei diversi ambiti in cui opera il Titolare.

6. La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento imprescindibile per il trattamento dei dati personali e criterio di misurazione e valutazione della performance organizzativa ed individuale.

7. La formazione è tracciata e documentata; sono previsti moduli obbligatori differenziati per profili di rischio e un richiamo periodico almeno annuale per i ruoli con accesso a dati particolari/penali o a banche dati.

Art. 19 - Registro delle attività dei trattamenti

1. Il Titolare del trattamento istituisce, in forma scritta, il Registro delle attività di trattamento e di tutte le categorie di attività relative al trattamento, svolte sotto la propria responsabilità, secondo quanto previsto dall'art. 30, paragrafo 1, del RGPD.

2. Il Registro delle attività dei trattamenti reca almeno 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, del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) le categorie dei trattamenti effettuati da parte delle singole articolazioni dell'Agenzia;

d) una descrizione delle categorie di interessati e delle categorie di dati personali;

e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

f) 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 di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

h) il richiamo alle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. Il Titolare assicura la tenuta e l'aggiornamento del Registro tramite il Referente privacy. Il DPO fornisce supporto nella elaborazione e nell'aggiornamento del registro dei Trattamenti, svolge funzioni di verifica e consulenza, senza assumere la responsabilità operativa della tenuta. Ciascun Dirigente ha comunque la responsabilità di fornire prontamente e correttamente al Responsabile per la Protezione dei Dati, ogni elemento, dato e informazione necessari alla regolare formazione, tenuta e all'aggiornamento del Registro delle attività dei trattamenti.

4. Su richiesta, il Titolare del trattamento o il Dirigente, mettono il registro a disposizione del Garante.

5. Il registro è tenuto in forma scritta, anche in formato elettronico, e deve essere periodicamente aggiornato, con cadenza almeno annuale e, in ogni caso, ogniqualvolta vi siano delle modifiche che richiedono la loro trascrizione nel registro dei trattamenti (modalità di trattamento, finalità, categorie di dati, categorie di interessati, ecc.).

6. Il registro delle attività dei trattamenti è adottato con provvedimento del Titolare del trattamento e, successivamente, con cadenza annuale, con analogo provvedimento sono adottate le revisioni del Registro delle attività dei trattamenti che, danno conto

delle eventuali modifiche/integrazioni e novità intercorse con riferimento alle categorie di dati trattati, alle modalità di trattamento, alle finalità, alle categorie di interessati, nonché alle misure di sicurezza tecniche ed organizzative di cui all'art. 32 RGPD.

CAPO IV – PUBBLICITA' E DIFFUSIONE SUL WEB DI DOCUMENTI CONTENENTI DATI PERSONALI

Art. 20 - Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

1. I Dirigenti, in sede di pubblicazione sul sito istituzionale dell'Agenzia nelle Sezioni "Albo pretorio on-line" e "Amministrazione Trasparente", di dati personali contenuti in atti e provvedimenti amministrativi per i quali un'espressa previsione normativa ne preveda l'obbligo di pubblicazione, assicurano il rispetto dei principi di pertinenza e minimizzazione di cui all'art. 5, paragrafo 1, lett. c), RGPD.
2. La pubblicazione di un atto sul sito istituzionale dell'Agenzia costituisce un'operazione di diffusione dei dati personali in esso eventualmente contenuti; detta circostanza impone all'Agenzia di valutare preventivamente, di volta in volta, quali siano le informazioni personali la conoscenza delle quali sia realmente rilevante rispetto alle specifiche finalità perseguite con la pubblicazione medesima.

A questo fine, si osserva che:

- la "diffusione" di dati personali – ossia "il dare conoscenza dei dati personali a soggetti indeterminati" mediante la pubblicazione sul proprio sito istituzionale - da parte dei "soggetti pubblici" è ammessa unicamente quando la stessa sia prevista da una specifica norma di legge o di regolamento ovvero da atto amministrativo generale (art. 2-*ter*, comma 1, D. Lgs. 196/03 e ss.mm.ii.);
- laddove l'Amministrazione riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento sul proprio sito web istituzionale è necessario selezionare i dati personali da inserire in tali documenti, verificando, caso per caso, se ricorrano i presupposti per l'oscuramento di determinate informazioni;
- è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria (cd. "principio di pertinenza e minimizzazione" di cui all'art. 5, paragrafo 1, lett. c), RGPD).

- è sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale" (art. 2-*septies*, comma 8, D. Lgs. 196/03 e ss.mm.ii. e art. 7-*bis*, comma 6, D. Lgs. 33/2013) nonché "la situazione di disagio economico sociale degli interessati" (art. 26, comma 4, D. Lgs. 33/2013).

3. Una volta trascorso l'arco temporale previsto dalle singole discipline per la pubblicazione degli atti e dei documenti sul sito web dell'Amministrazione, l'Agenzia provvederà, senza indugio, alla loro defissione.

4. L'Agenzia adotta una procedura di oscuramento/redazione e misure tecniche per ridurre la diffusione indiscriminata (es. limitazione indicizzazione da motori di ricerca, gestione cache, controllo metadati dei file, pubblicazione di versioni 'redatte').

5. Sono disciplinati separatamente le pubblicazioni in Albo pretorio online e le pubblicazioni in Amministrazione Trasparente, con tempi e finalità proprie.

CAPO V - SICUREZZA DEI DATI PERSONALI

Art. 21 – Sicurezza del trattamento

1. Il Titolare e ciascun Dirigente mettono in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono:

- la pseudonimizzazione;
- la minimizzazione;
- la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate da ciascun designato, previa consultazione con il Responsabile della Protezione dei dati e con l'Amministratore di Sistema dell'Agenzia:

- sistemi di autenticazione;
- sistemi di autorizzazione;
- sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio;
- sistemi di rilevazione di intrusione;
- sistemi di sorveglianza;
- sistemi di protezione con videosorveglianza;
- registrazione accessi;
- porte, armadi e contenitori dotati di serrature e ignifughi;
- sistemi di copiatura e conservazione di archivi elettronici;
- ulteriori misure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al RGPD è dimostrata attraverso l'adozione delle misure di sicurezza adeguate al rischio in ossequio alle previsioni di cui all'art. 32 RGPD, ovvero attraverso l'adesione a codici di condotta approvati o ad altri meccanismi di certificazione approvati.

Art. 22 -Valutazioni d'impatto sulla protezione dei dati

1. La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.

2. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGPD, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

3. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, paragrafi 4, 5 e 6 RGPD. A questo

proposito si richiama integralmente l'Allegato 1 al Provvedimento del Garante Privacy n. 467 dell'11/10/2018 ed i successivi provvedimenti contenenti gli elenchi delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto.

4. La DPIA è avviata dal dirigente competente prima dell'avvio o modifica sostanziale del trattamento; è redatta con supporto del Referente privacy e con coinvolgimento tempestivo del DPO, che fornisce parere in merito e ne sorveglia lo svolgimento. La DPIA è approvata dal Titolare e riesaminata in caso di variazioni rilevanti.

5. L'Amministratore di Sistema e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare ed al Responsabile della Protezione dei Dati (DPO) per lo svolgimento della DPIA.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, RGPD;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base giuridica nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

7. La DPIA, condotta prima di dar luogo al trattamento, contiene almeno:

a) la descrizione sistematica del contesto, dei trattamenti previsti e delle finalità del trattamento. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (*hardware*, *software*, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) la valutazione dei rischi per i diritti e le libertà degli interessati, con particolare riguardo alla probabilità e alla gravità dei rischi rilevati;

d) l'individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento al RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 23 - Consultazione preventiva

1. Il Titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del DPO, il Garante Privacy qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

Art. 24 – Procedura operativa per la gestione delle violazioni (Data Breach) e notifica al Garante

1. Per "violazione di dati personali" (data breach) si intende qualsiasi violazione di sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trattati dall'Agenzia. La procedura si applica a ogni evento, anche solo potenziale o sospetto.

2. Chiunque venga a conoscenza di un possibile incidente deve segnalarlo entro 4 ore al Dirigente competente e al Referente privacy, fornendo descrizione dell'evento, tempi e sistemi coinvolti.

3. Il Responsabile del Trattamento è obbligato a informare il Titolare senza ingiustificato ritardo e comunque entro 24 ore dalla conoscenza, cooperando per il ripristino.

4. Il Dirigente competente attiva immediatamente il supporto ICT e il Referente privacy. Il DPO è coinvolto tempestivamente per fornire un parere sulla qualificazione dell'evento. Entro 24 ore dalla presa in carico, viene effettuata una valutazione documentata per determinare la gravità del rischio per i diritti e le libertà delle persone fisiche (come ad es. nel caso di furto d'identità, perdite finanziarie,

danni reputazionali, dati sensibili o di persone vulnerabili).

5. Se la valutazione evidenzia un rischio per i diritti e le libertà, l'Agenzia notifica la violazione al Garante entro 72 ore dal momento in cui ne è venuta a conoscenza. Qualora non sia possibile fornire tutte le informazioni contestualmente, esse sono fornite in fasi successive. La notifica deve contenere:

a) Natura della violazione e numero approssimativo di interessati/registrazioni;

b) Nome e recapiti del DPO;

c) Probabili conseguenze e misure adottate o proposte per attenuare gli effetti.

6. L'Agenzia documenta ogni violazione (anche quelle non notificate), indicando circostanze, effetti e misure correttive. Tale registro è conservato per finalità di accountability e verifica di conformità.

Art. 25 – Comunicazione della violazione agli interessati

1. Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Agenzia comunica la violazione agli interessati senza ingiustificato ritardo, con linguaggio chiaro e semplice.

2. La comunicazione deve descrivere la natura della violazione e contenere almeno:

a) I recapiti del DPO o del punto di contatto;

b) Le probabili conseguenze;

c) Le misure adottate e le raccomandazioni pratiche per gli interessati (es. cambio password, attenzione a phishing).

3. La comunicazione avviene con canali idonei a raggiungere effettivamente l'interessato (PEC, e-mail, raccomandata, area riservata), garantendo la tracciabilità e rispettando il principio di minimizzazione dei dati.

4. La comunicazione all'interessato non è richiesta se:

a) I dati erano protetti da misure tecniche adeguate (es. cifratura) che li rendono inintelligibili;

b) L'Agenzia ha adottato misure successive tali da scongiurare il sopraggiungere del rischio elevato;

c) La comunicazione richiederebbe sforzi sproporzionati (in tal caso si procede con una comunicazione pubblica o misura equivalente).

5. Qualora il Titolare non abbia provveduto, il Garante può richiedere di effettuare la comunicazione dopo aver valutato la probabilità del rischio elevato.

6. Ogni decisione relativa alla comunicazione (inclusa la motivazione in caso di mancata comunicazione) deve essere registrata nel Registro interno delle violazioni di cui all'Art. 22.

Art. 26 - Disposizioni finali

1. Per quanto non espressamente previsto e disciplinato dal presente Regolamento si applicano le disposizioni di cui al Regolamento UE 2016/679, al D. Lgs. 196/03 (così come riformato e modificato dal D. Lgs. 101/18), nonché le Linee guida ed i provvedimenti del Garante Privacy, e le Linee Guida del Comitato europeo per la protezione dei dati personali.
2. Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.
3. Gli allegati tecnici e le procedure operative di attuazione sono aggiornati con determinazione del Titolare del Trattamento, sentito il DPO, in funzione dell'evoluzione normativa, tecnologica e organizzativa.