ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

Puglia Centrale

Agenzia Regionale per la Casa e l'Abitare

REGOLAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

in attuazione del Regolamento UE 2016/679 "Regolamento generale per la protezione dei dati"

APPROVATO CON DECRETO N.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

SOMMARIO

PREMESSA ..... - 4 -
CAPO I ..... - 4 -
DIPOSIZIONI GENERALI ..... - 4 -
Art. 1 ..... - 4 -
Oggetto del Regolamento ..... - 4 -
Art. 2 ..... - 4 -
Definizioni ..... - 4 -
Art. 3 ..... - 7 -
Finalità del trattamento ..... - 7 -
Art. 4 ..... - 7 -
Principi applicabili al trattamento ..... - 7 -
Art. 5 ..... - 8 -
Leicità del trattamento ..... - 8 -
Art. 6 ..... - 9 -
Consenso dell'interessato ..... - 9 -
Art. 7 ..... - 9 -
Trattamento dei dati particolari ..... - 9 -
Art. 8 ..... - 10 -
Trattamento dei dati giudiziari ..... - 10 -
CAPO II ..... - 12 -
DIRITTI DELL'INTERESSATO ..... - 12 -
Art. 9 ..... - 12 -
Informativa, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato ..... - 12 -
Art. 10 ..... - 13 -
Informativa per i dati da raccogliere presso l'interessato ..... - 13 -
Art. 11 ..... - 14 -
Informativa per i dati da ottenere da soggetti diversi dall'interessato ..... - 14 -
Art. 12 ..... - 15 -
Diritto di accesso dell'interessato ..... - 15 -
Art. 13 ..... - 16 -
Diritto di rettifica e integrazione ..... - 16 -
Art. 14 ..... - 16 -
Diritto alla cancellazione (diritto all'oblio) ..... - 16 -
Art. 15 ..... - 17 -
Diritto di limitazione di trattamento ..... - 17 -
Art. 16 ..... - 18 -
Diritto alla portabilità dei dati ..... - 18 -
Art. 17 ..... - 18 -
Diritto di opposizione ..... - 18 -
Art. 18 ..... - 19 -
Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione ..... - 19 -
CAPO III ..... - 20 -
SOGGETTI RESPONSABILI DEL TRATTAMENTO E DELLA SICUREZZA DEI DATI ..... - 20 -
Art. 19 ..... - 20 -
Titolare del trattamento ..... - 20 -
Art. 20 ..... - 21 -
Contitolari del trattamento ..... - 21 -
Art. 21 ..... - 22 -
Responsabili del trattamento ..... - 22 -

Art. 22 ..... **- 24 -**
Incaricati del trattamento ..... **- 24 -**
Art. 23 ..... **- 25 -**
Amministratore del sistema informatico ..... **- 25 -**
Art. 24 ..... **- 28 -**
Responsabile della protezione dei dati ..... **- 28 -**
Art. 25 ..... **- 31 -**
Trattamento di dati personali nei servizi esternalizzati ..... **- 31 -**
Art. 26 ..... **- 31 -**
Comunicazione interna di documenti contenti dati personali del trattamento ..... **- 31 -**
Art. 27 ..... **- 32 -**
Utilizzo di dati da parte dei componenti gli Organi Istituzionali di controllo interno ..... **- 32 -**
CAPO IV ..... **- 33 -**
SICUREZZA DEI DATI PERSONALI ..... **- 33 -**
Art. 28 ..... **- 33 -**
Misure per la sicurezza dei dati personali ..... **- 33 -**
Art. 29 ..... **- 34 -**
Registro delle attività di trattamento del Titolare ..... **- 34 -**
Art. 30 ..... **- 35 -**
Registro delle categorie di attività trattate dai responsabili ..... **- 35 -**
Art. 31 ..... **- 35 -**
Valutazioni di impatto sulla protezione dei dati ..... **- 35 -**
Art. 32 ..... **- 38 -**
Violazione dei dati personali ..... **- 38 -**
Art. 33 ..... **- 39 -**
Entrata in vigore, pubblicazione e divulgazione del Regolamento ..... **- 39 -**

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

PREMESSA

CAPO I
DIPOSIZIONI GENERALI

Art. 1
Oggetto del Regolamento

1. Il presente Regolamento disciplina le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo n. 679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" (RGPD), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali nonché alla libera circolazione di tali dati.
2. Per quanto non previsto nel presente Regolamento si rinvia al predetto Regolamento europeo 2016/679, alle vigenti fonti di diritto europee e nazionali della protezione dei dati personali, alle linee guida del Garante della Privacy, alle direttive impartite dal Titolare del trattamento, dai Responsabili del trattamento, dall'Amministratore del sistema informatico e dal Responsabile della protezione dei dati.

Art. 2
Definizioni
(artt. 4, 9 e 10 RGPD)

1. Ai fini del presente regolamento si intende per :
   a) «**ARCA**»: L'Agenzia Regionale per la Casa e l'Abitare Puglia Centrale, nella qualità di titolare del trattamento dei dati personali, le cui funzioni sono esercitate dall'Amministratore Unico, e del Direttore Generale nell'ambito delle rispettive competenze;
   b) «**Garante**»: l'Autorità di controllo ossia il Garante della Privacy;
   c) «**RGPD** o **REG. UE 2016/679**»: il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento generale sulla protezione dei dati";
   d) «**Codice**»: il d.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali";
   e) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (**C26, C27, C30**)
   f) «**dati particolari**»: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; (**C51)**

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

g) «**dati giudiziari**»: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
h) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (**C34**)
i) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (**C51**)
j) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (**C35**)
k) «**interessato**»: la persona fisica titolare dei dati personali oggetto di trattamento;
l) «**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;
m) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (**C67**)
n) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (**C24, C30, C71-C72**)
o) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (**C26, C28-C29**)
p) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (**C15**)
q) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. **(C74)** L'ARCA si configura come persona giuridica;
r) «**contitolari del trattamento**»: due o più titolari del trattamento che determinano congiuntamente, mediante un accordo interno, le finalità e i mezzi del trattamento. Ai fini del presente Regolamento, si intendono per contitolari i soggetti riportati nell'allegato A) che sarà oggetto ad aggiornamento in relazione al variare dei contitolari;
s) «**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. Ai

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

fini del presente Regolamento, si intendono per responsabili del trattamento i Dirigenti dell'Agenzia e tutte le Aziende che, al fine del conseguimento degli obiettivi di piena efficacia ed efficienza dell'Agenzia, trattano autonomamente i dati. I soggetti sono riportati nell'allegato A) che sarà oggetto ad aggiornamento in relazione al variare dei responsabili del trattamento;

t) «**sub-responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali a cui fa ricorso il responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
u) «**incaricato del trattamento**»: chiunque, agendo sotto l'autorità del responsabile del trattamento o del titolare del trattamento, abbia accesso a dati personali essendo stato autorizzato al loro trattamento. Ai fini del presente Regolamento si intendono incaricati del trattamento tutti i Dipendenti che, in qualsiasi modo, partecipano al trattamento dei dati per l'espletamento delle funzioni di mandato;
l) «**responsabile della protezione dei dati**»: il dipendente del titolare o del responsabile del trattamento ovvero la persona fisica o giuridica estranea all'organizzazione del titolare o del responsabile del trattamento che svolge i compiti di cui all'art. 39 del REG. UE 2016/679 o ulteriori compiti affidati dal titolare del trattamento sulla base di un contratto di servizi (DPO);
m) «**amministratore del sistema**»: la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di basi di dati, di reti e di apparati di sicurezza e di sistemi *software* complessi. Ai fini del presente Regolamento, si intende amministratore del sistema il responsabile dell'Ufficio CED – Gestione Sistema Informatico amministrativo;
n) «**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 del trattamento;
o) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (**C31**)
p) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (**C32, C33**)
q) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (**C85**)
r) «**Unione**»: l'Unione Europea;
s) «**Stato**»: lo Stato italiano.

3. Per le definizioni non riportate nel precedente comma si rinvia all'elenco definizioni previste dall'art. 4 del RGPD.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

Art. 3
Finalità del trattamento
(art. 3 RGPD)

1. I trattamenti dei dati personali sono eseguiti dall'ARCA per le seguenti finalità di pubblico interesse, stabilite dalla fonti normative che rispettivamente le disciplinano:
   a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; rientrano in questo ambito i trattamenti dei dati personali compiuti per:
      - espletare le funzioni tecnico- amministrative in materia di edilizia residenziale pubblica e sociale;
      - espletare la gestione del patrimonio immobiliare di edilizia residenziale pubblica proprio e, su delega, di altri soggetti pubblici,
      - eseguire interventi di manutenzione, recupero e riqualificazione degli immobili di edilizia residenziale pubblica assegnati a nuclei familiari;
      - eseguire la gestione dei servizi attinenti al soddisfacimento delle esigenze abitative dei nuclei familiari;
      - l'esercizio di eventuali ulteriori funzioni amministrative per servizi di competenza regionale trasferiti, delegati o comunque affidati all'ARCA in base a disposizioni legislative.
   b) l'adempimento di un obbligo legale, civile e/o giudiziario al quale è soggetta l'ARCA;
   c) l'esecuzione di un contratto con riguardo ai soggetti interessati;
   d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4
Principi applicabili al trattamento
(art. 5 – C39, C74 - RGPD)

1. I dati personali sono trattati nel rispetto dei principi di : **(C39)**
   a) «**liceità, correttezza e trasparenza**»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
   b) «**limitazione delle finalità**»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, prf. 1 del RGDP, considerato incompatibile con le finalità iniziali;
   c) «**minimizzazione dei dati** »: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
   d) «**esattezza**»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

e) «**limitazione della conservazione**»: i dati personali sono 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'art. 89, prf. 1 del RGPD, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

f) «**integrità e riservatezza**»: i dati personali sono 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;

g) «**responsabilizzazione**»: il titolare del trattamento è competente per il rispetto dei principi di cui alla precedente lettera a), e deve essere in grado di comprovarlo. **(C74)**

2. Nelle ipotesi in cui disposizioni legislative, regolamentari o statutarie prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le opportune misure atte a garantire la riservatezza dei dati personali a norma del RGPD, del "Codice della privacy" di cui al d.lgs. 30 giugno 2003.n. 196, del "Codice della trasparenza" di cui al d.lgs. 14 marzo 2013, n. 33 e dei provvedimenti del Garante della Privacy.

Art. 5
Leicità del trattamento
(art. 6 – C40→C46 - RGPD)

1. Il trattamento dei dati personali effettuato dall'ARCA é lecito esclusivamente per lo svolgimento delle proprie funzioni istituzionali e se:
   a) l'interessato ha espresso il consenso al trattamento dei suoi dati personali per una o più specifiche finalità;
   b) il trattamento é necessario all'esecuzione di un contratto di cui l'interessato é parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato;
   c) il trattamento é necessario per adempiere un obbligo legale, civile e/o giudiziario al quale é soggetta l'ARCA;
   d) il trattamento é necessario per l'esecuzione di un compito di interesse pubblico di cui é investita l'ARCA;
2. La finalità del trattamento è necessaria per l'esecuzione di un compito svolto nel pubblico interesse di cui è investito il titolare del trattamento. Deve contenere: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX dello stesso RGPD (Rif. Manuale Gestione Documentale Decreto Arca n. 68/2016);

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

3. 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, il titolare del trattamento tiene conto, tra l'altro: (**C50**)
   a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
   b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
   c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 del RGPD, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del 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.

Art. 6
Consenso dell'interessato
(art. 7 - da C40 a C46 – RGPD)

1. L'ARCA richiede agli interessati il consenso per il trattamento dei loro dati personali esclusivamente quando il trattamento dei dati è effettuato nello svolgimento dei propri compiti istituzionali di interesse pubblico di cui è investita dalla vigente normativa.
2. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
3. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
4. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
5. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Art. 7
Trattamento dei dati particolari
(art. 9 RGPD)

1. Nell'esercizio della propria attività istituzionale, ARCA potrà trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (**C51**)

2. I casi in cui si potranno effettuare i trattamenti di cui al precedente comma, sono i seguenti: (**C51, C52**)
   a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri disponga che l'interessato non possa revocare il suddetto consenso;
   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
   d) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   e) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
   f) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (**C55, C56**)
   g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri, in conformità al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (**C53**)
   h) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del RGPD sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera g), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona, anch'essa soggetta all'obbligo di segretezza, in conformità al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (**C53**)

Art. 8
Trattamento dei dati giudiziari
(art. 10 RGPD)

1. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del RGPD deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato che preveda garanzie appropriate per i diritti e le libertà degli interessati.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

CAPO II
DIRITTI DELL'INTERESSATO

Art. 9
Informativa, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato
(art. 12 – C58, C60, C64 - RGPD)

1. L'ARCA adotta misure appropriate per fornire all'interessato tutte le informazioni di cui ai successivi articoli 10 e 11 e le comunicazioni di cui agli articoli da 12 a 18 e all'articolo 29 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente**,** purché sia evidentemente ottenuto il consenso dell'interessato e comprovata l'identità dello stesso; il mero rilascio dal copia del documento di identità da parte dell'interessato corrisponde alla raccolta del consenso informato ai fini del rilascio dell'informazione orale.
2. L'ARCA agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18. Nei casi di cui all'articolo 11, paragrafo 2, del RGPD, l'AGENZIA non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che l'ARCA dimostri che non è in grado di identificare l'interessato.
3. L'ARCA fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 12 a 18 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'ARCA informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. Se non ottempera alla richiesta dell'interessato, l'ARCA informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
4. Le informazioni fornite ai sensi degli articoli 10 e 11 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 12 a 18 e dell'articolo 29 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
   a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
   b) rifiutare di soddisfare la richiesta. Incombe all'ARCA l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
5. Fatto salvo l'articolo 11 del RGPD, qualora l'ARCA nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 12 a 17, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.
6. Le informazioni da fornire agli interessati, anche a mezzo di opportuna cartellonistica, a norma degli articoli 10 e 11 possono essere fornite in combinazione con icone standardizzate per dare,

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.

Art. 10
Informativa per i dati da raccogliere presso l'interessato
(art. 13 – C60, C62 - RGPD)

1. In caso di raccolta presso l'interessato di dati che lo riguardano, l'ARCA fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
   a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
   b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, l'ARCA fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
   a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento di dati non particolari e non giudiziari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento dei dati particolari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati particolari previsto dal paragrafo 1 dell'articolo 9 del RGPD, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora l'ARCA intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

4. I commi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Art. 11
Informativa per i dati da ottenere da soggetti diversi dall'interessato
(art. 14 – C60, C62 - RGPD)

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
   a) l'identità e i dati di contatto dell'ARCA;
   b) i dati di contatto del responsabile della protezione dei dati;
   c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   d) le categorie di dati personali in questione;
   e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
2. Oltre alle informazioni di cui al comma 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
   a) il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   b) l'esistenza del diritto dell'interessato di chiedere all'ARCA l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   c) qualora il trattamento di dati non particolari e non giudiziari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità oppure il trattamento dei dati particolari sia basato sul consenso espresso dall'interessato per una o più specifiche finalità e il diritto dell'Unione o dello Stato abbia disposto l'irrevocabilità del divieto di trattare gli stessi dati particolari previsto dal paragrafo 1 dell'articolo 9 del RGPD, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   d) il diritto di proporre reclamo a un'autorità di controllo;
   e) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
   f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. L'ARCA fornisce le informazioni di cui ai commi 1 e 2:
   a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
   b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati.

4. Qualora l'ARCA intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al comma 2
5. I commi da 1 a 4 non si applicano se e nella misura in cui:
   a) l'interessato dispone già delle informazioni;
   b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, del RGPD o nella misura in cui l'obbligo di cui al comma 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, l'ARCA adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
   c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
   d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o dello Stato, compreso un obbligo di segretezza previsto per legge.

Art. 12
Diritto di accesso dell'interessato
(art. 15 – C63, C64 - RGPD)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
   a) le finalità del trattamento;
   b) le categorie di dati personali in questione;
   c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
   d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
   f) il diritto di proporre reclamo a un'autorità di controllo;
   g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
   h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del RGPD e, almeno in tali casi, informazioni significative

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole, commisurato agli effettivi costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
3. Il diritto di ottenere una copia di cui al comma 2 non deve ledere i diritti e le libertà altrui.
4. L'istanza é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
5. Il Dirigente del settore competente per la materia relativa al trattamento dei dati ovvero un delegato di quest'ultimo, provvede a soddisfare la richiesta dell'interessato nel più breve tempo possibile e comunque non oltre trenta giorni.

Art. 13
Diritto di rettifica e integrazione
(art. 16 – C65 – art. 19 RGPD)

1. L'interessato ha il diritto di ottenere dall'ARCA la rettifica dei suoi dati personali inesatti nonché, tenuto conto delle finalità del trattamento, l'integrazione dei suoi dati personali incompleti, anche fornendo una dichiarazione integrativa. L'istanza di rettifica o integrazione é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
2. Alla rettifica ovvero all'integrazione dei dati richiesta dall'interessato provvede, senza ritardo e comunque entro cinque giorni lavorativi dalla data di arrivo della predetta istanza, il Responsabile del procedimento amministrativo cui ineriscono i dati da rettificare o integrare.
3. Dell'eseguita rettifica o integrazione ovvero della motivata inammissibilità é data tempestiva comunicazione all'interessato con raccomandata con avviso di ricevimento o con notifica a mani o tramite pec.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 14
Diritto alla cancellazione (diritto all'oblio)
(art. 17 – C65, C66 – art. 19 - RGPD)

1. L'interessato ha il diritto di ottenere dall'ARCA la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e l'ARCA ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

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

2. L'istanza é formulata dall'interessato per iscritto e inviata anche tramite posta elettronica.
3. L'ARCA, se ha reso pubblici dati personali ed è obbligato, ai sensi del comma 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
4. I commi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
   a) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
   b) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del RGPD nella misura in cui il diritto di cui al comma 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
   c) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
5. Il Responsabile del procedimento, relativo al trattamento dei dati oggetto della richiesta, deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, la rettifica del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 15
Diritto di limitazione di trattamento
(artt. 18 e 19 – C67 – RGPD)

1. L'interessato ha il diritto di ottenere dall'ARCA la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario all'ARCA per verificare l'esattezza di tali dati personali;

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché l'ARCA non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, del RGPD in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del comma 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del comma 1 è informato dall'ARCA prima che detta limitazione sia revocata.
4. Il Responsabile del procedimento relativo al trattamento dei dati oggetto della richiesta deve comunicare, con tempestività, a ciascuno dei destinatari cui sono stati trasmessi i dati personali la limitazione del trattamento effettuata, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato; e, inoltre, dà comunicazione all'interessato di tali destinatari qualora l'interessato lo richieda.

Art. 16
Diritto alla portabilità dei dati
(art. 20 – C68 - RGPD)

1. Il diritto alla portabilità dei dati di cui all'articolo 20 del RGPD non si applica ai trattamenti svolti dall'ARCA necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio della attività istituzionale di cui é investita la stessa Agenzia.

Art. 17
Diritto di opposizione
(art. 21 – C69, C70 - RGPD)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano inerenti ad attività di profilazione che, peraltro, l'Agenzia non mette in atto durante le attività di trattamento. L'ARCA si astiene dal trattare ulteriormente i dati personali, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. L'opposizione é formulata dall'interessato per iscritto ed é inviata all'ARCA anche per posta elettronica.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

3. Da parte del Responsabile del procedimento relativo al trattamento dei dati oggetto dell'opposizione, il diritto di cui al comma 1, è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Art. 18
Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
(art. 22 – C71, C72 - RGPD)

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il comma 1 non si applica nel caso in cui la decisione:
   a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
   b) sia autorizzata dal diritto dell'Unione o dello Stato, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
   c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al comma 2, lettere a) e c), l'ARCA attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e riconosce all'interessato il diritto di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al comma 2 non si basano sulle categorie di dati particolari di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), del RGPD e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

CAPO III
SOGGETTI RESPONSABILI DEL TRATTAMENTO E DELLA SICUREZZA DEI DATI

Art. 19
Titolare del trattamento
(art. 24 – C74, C78 - RGPD)

1. L'ARCA è il titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee, gestite dagli uffici. Per il trattamento di dati l'ARCA può avvalersi anche di soggetti pubblici o privati esterni tramite un contratto di servizio o altro atto giuridicamente valido nel quale sono specificati le finalità e le modalità del trattamento, le categorie di dati da trattare, le responsabilità e i doveri facenti carico al soggetto che svolgerà il trattamento determinandone la qualifica di contitolare o responsabile del trattamento.
2. Le funzioni attribuite all'ARCA dalle norme vigenti, con particolare riguardo alla normativa regionale, sono esercitate nell'ambito delle precipue competenze. L'Amministratore Unico rappresenta l'ARCA nella qualità di titolare del trattamento; le specifiche attribuzioni di responsabilità sono parzialmente conferite, per le specifiche funzioni, al Direttore Generale e possono essere conferite, per delega funzionale, a un Dirigente e/o ai Responsabili del trattamento e/o all'Amministratore di Sistema, purché in possesso di adeguate competenze.
3. L'ARCA 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. L'ARCA mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
5. 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 da 15 a 22 del RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
6. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa 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.
7. Il Titolare adotta misure appropriate per fornire all'interessato:
   a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
   b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

8. 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, l'ARCA deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali ("DPIA" – *Data Process Impact Assessment*) ai sensi dell' art.35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 31.
9. L'Amministratore Unico provvede a:
   a) designare i Responsabili del trattamento;
   b) nominare il Responsabile della protezione dei dati;
   c) nominare l'Amministratore del sistema informatico;
   d) diramare le direttive necessarie per l'applicazione delle disposizioni del RGPD e del presente regolamento, sentiti il Direttore Generale, il Responsabile della protezione dei dati, l'Amministratore del sistema informatico e i Responsabili del trattamento.
10. Nelle convenzioni, nelle concessioni, nei contratti, negli incarichi professionali o in altri strumenti giuridici consentiti dalla legge con cui é affidata a soggetti esterni all'ARCA la gestione di attività e/o servizi per conto dell'Agenzia, é prevista espressamente la nomina degli stessi soggetti affidatari quali responsabili del trattamento dei dati personali connessi alle attività istituzionali affidate.
11. L'elenco dei Responsabili del trattamento e degli Uffici in cui si articola l'organizzazione dell'ARCA, é pubblicato in apposita sezione del sito istituzionale, aggiornato periodicamente e precisamente: sezione Amministrazione Trasparente – Altri Contenuti – Privacy.
12. L'ARCA favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli stakeholders rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 20
Contitolari del trattamento
(art. 26 – C79 - RGPD)

1. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'ARCA da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente e in modo trasparente, anche a mezzo di corrispondenza, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD.
2. L'intercorsa corrispondenza definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa europea, statale specificatamente applicabile. L'intesa di contitolarità può individuare un punto di contatto comune per gli interessati.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

Art. 21
Responsabili del trattamento
(art. 28 – C81 - RGPD)

1. L'ARCA si avvale di più Responsabili del trattamento, designati dall'Amministratore Unico. La designazione avviene formalmente nelle forme e nei modi consentiti dalla legge, ed esplicita le attribuzione delle funzioni, per le quali sono tassativamente previsti:
   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;
   - gli obblighi ed i diritti del Titolare del trattamento.

   Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra l'ARCA e ciascun responsabile designato.
2. Nel merito del trattamento dei dati personali, contenuti in tutte le banche dati esistenti nell'articolazione organizzativa, devono essere designati i Responsabili del Trattamento. Possono essere designati, altresì, Responsabili del trattamento i Dirigenti di settore, i funzionari cui é attribuita la Posizione Organizzativa, limitatamente alle banche dati di propria competenza, che abbiano una rilevante importanza per l'attività istituzionale dell'Agenzia.
3. Il Responsabile del trattamento deve essere in grado, anche attraverso una adeguata preventiva formazione, di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui al successivo articolo 28 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
4. L'ARCA può avvalersi, per il trattamento di dati, anche particolari, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2, stipulando atti giuridici in forma scritta, che specifichino la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
5. Gli atti che disciplinano il rapporto tra il Titolare del trattamento e il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, del RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
6. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare del trattamento e il Responsabile del trattamento primario, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD. Se il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile primario conserva, nei confronti del Titolare del trattamento, l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.
7. Le operazioni di trattamento possono essere effettuate solo da sub-responsabili o da incaricati che operano sotto la diretta autorità del Responsabile del trattamento attenendosi alle istruzioni

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

loro impartite per iscritto dallo stesso Responsabile, le quali istruzioni individuano specificatamente l'ambito del trattamento consentito.

8. Il Responsabile del trattamento risponde, anche dinanzi al Titolare del trattamento, dell'operato del sub-responsabile del trattamento e degli incaricati del trattamento anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile e dell'incaricato del trattamento.
9. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza.
10. Il Responsabile del trattamento provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare del trattamento, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare deve provvedere:
    a) a tenere aggiornato il registro delle categorie di attività di trattamento svolte per conto del Titolare;
    b) ad adottare le misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti;
    c) ad autorizzare i dipendenti ad accedere ai dati personali al fine di svolgere il trattamento afferente i rispettivi compiti istituzionalmente assegnati;
    d) a sensibilizzare e formare il personale che partecipa ai trattamenti in materia di protezione dei dati personali, fornendo le istruzioni per il corretto trattamento dei dati personali, e a controllare che le attività di trattamento, con particolare riferimento alle operazioni di comunicazione e diffusione, svolte dagli incaricati siano conformi alle norme del RGPD;
    e) a collaborare con il Titolare al fine di definire la valutazione dell'impatto del trattamento sulla protezione dei dati personali, fornendo allo stesso ogni informazione di cui è in possesso;
    f) a informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso in cui il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.
    g) a curare le informative di cui agli articoli 13 e 14 del RGPD da fornire agli interessati, predisponendo la necessaria modulistica o determinando altre forme idonee di informazione inerenti ai trattamenti di competenza della propria struttura organizzativa, facendo, in presenza di dati particolari, espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento;
    h) a curare l'eventuale raccolta del consenso degli interessati per il trattamento dei dati particolari qualora il loro trattamento non sia previsto da una specifica norma di legge;
    i) adottare le misure necessarie per facilitare l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD;
    j) a stipulare gli accordi con altri soggetti pubblici o privati per l'esercizio del diritto di accesso alle banche-dati nei limiti previsti dalle disposizioni legislative e regolamentari.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

Art. 22
Incaricati del trattamento
(art. 29 – C81 - RGPD)

1. Gli incaricati del trattamento sono individuati nel personale ARCA, tra coloro che materialmente effettuano il trattamento dei dati relativi ai procedimenti propri dell'Agenzia e che, pertanto, hanno accesso a dati personali ovvero agiscano sotto l'autorità del titolare del trattamento o dei responsabili del trattamento.
2. Gli incaricati del trattamento non possono svolgere operazioni di trattamento dei dati personali se non istruiti in tal senso dal Titolare del trattamento.
3. I dipendenti sono designati incaricati del trattamento e autorizzati al trattamento dei dati personali con formale provvedimento (ordine di servizio) del Responsabile del trattamento competente per la struttura organizzativa apicale in cui sono inseriti gli stessi dipendenti; nel provvedimento sono indicati: i procedimenti amministrativi per lo svolgimento dei quali è indispensabile il trattamento dei dati personali; le finalità del trattamento; le categorie di dati personali da trattare; le operazioni di trattamento eseguibili, con particolare riferimento alla comunicazione e alla diffusione dei dati particolari e giudiziari; gli eventuali limiti al trattamento; le misure di sicurezza da adottare da parte degli stessi Incaricati. Le predette designazione e autorizzazione nonché le prefate indicazioni del trattamento possono essere stabilite anche con un atto distinto dal contratto individuale di lavoro. Tale atto deve essere notificato al dipendente interessato, il quale non può esimersi dalla sua accettazione e attuazione.
4. I dipendenti possono essere individuati quali incaricati del trattamento nominativamente ovvero con riferimento alla categoria di inquadramento o al profilo professionale o alla collocazione nell'organizzazione del settore o dell'ufficio.
5. I dipendenti incaricati del trattamento operano sotto l'autorità dei Responsabili del trattamento, attenendosi alle istruzioni impartite per iscritto, con particolare riferimento alla custodia degli atti e documenti analogici e digitali contenenti dati personali, particolari e giudiziari e alle relative misure di sicurezza.
6. Agli incaricati compete, in relazione al trattamento dei dati personali, provvedere:
   - al trattamento dei dati personali per lo svolgimento delle funzioni istituzionali dell'ARCA, in conformità alle disposizioni del RGPD;
   - la raccolta e la registrazione per gli scopi inerenti l'attività istituzionale svolta da ciascuno;
   - la verifica in ordine alla loro pertinenza, completezza e non eccedenza delle finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal responsabile del trattamento;
   - la conservazione, rispettando le misure di sicurezza predisposte al riguardo.
7. Per ogni operazione di trattamento è da garantire la massima riservatezza.
8. Nel caso di allontanamento anche temporaneo dalla propria postazione di lavoro, l'incaricato verifica che non vi sia possibilità per chiunque non sia autorizzato all'accesso ai dati di accedere alle banche-dati e/o ai dati personali per i quali è in corso un qualsiasi tipo di trattamento.
9. Le comunicazioni e le diffusioni a soggetti diversi dagli interessati devono essere svolte nel pieno rispetto delle norme che le disciplinano.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

10. Il flusso di dati tra Titolare del trattamento, Responsabili del trattamento, Incaricati del trattamento, Amministratore del sistema informatico e il Responsabile della protezione dei dati, Direttore Generale e componenti degli organi di controllo interno non costituisce "comunicazione" in senso tecnico quale operazione di trattamento; ne consegue che tale flusso non é soggetto ai limiti previsti per tale operazione di trattamento.

Art. 23
Amministratore del sistema informatico
(Garante Privacy provvedimento del 25.6.2009)

1. Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" come modificato con successivo provvedimento datato 25/06/2009, l'ARCA ha individuato l'amministratore del sistema informatico nel conferimento di Posizione Organizzativa incardinata nell'Ufficio CED. Tale responsabilità è determinata al fine di assicurare che il sistema informatico dell'Agenzia sia strutturato e gestito in modo da garantire le misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.
2. L'amministratore del sistema deve essere in possesso di titolo di studio specifico in informatica, almeno di laurea triennale e di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza.
3. Amministratore del sistema informatico può essere designato, con decreto dell'Amministratore Unico, un dipendente ARCA a tempo indeterminato inquadrato almeno nella categoria "D" ovvero, nel caso di mancanza di un dipendente, un soggetto esterno, persona fisica o soggetto giuridico. La designazione da parte dell'Amministratore del soggetto esterno può avvenire tra quanti abbiano partecipato a una apposita procedura ad evidenza pubblica nelle forme stabilite dalla legge e assolve ai suoi compiti in base a un contratto di servizio sottoscritto dal Dirigente preposto dell'ARCA. L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti é strettamente connessa agli obblighi di autonomia e indipendenza dell'Amministratore di sistema.
4. Il predetto provvede, tempestivamente, a che i dati identificativi e di contatto del Responsabile della protezione dei dati siano pubblicati nel sito web istituzionale dell'Agenzia.
5. Nell'atto, ovvero nel contratto di servizio, con cui é designato Amministratore di sistema il dipendente ARCA, o il soggetto esterno all'Agenzia, devono essere riportati, altresì, tutti gli adempimenti, sul piano delle procedure amministrative, dell'organizzazione, dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali, in riferimento alle fonti di diritto europee e nazionali, ai provvedimenti del Garante della Privacy, alle disposizioni regolamentari e alle direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati, per conformarsi alla disciplina del Codice

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

dell'amministrazione digitale di cui al decreto legislativo n. 82/2005 e ss.mm.ii.; in particolare la cura dei seguenti adempimenti:

a) gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per i Responsabili e gli Incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzati;
d) verificare costantemente che il Titolare del trattamento abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari, redigendo entro il 30 settembre di ogni anno una apposita relazione da inviare all'Amministratore Unico di ARCA e al Responsabile per la protezione dei dati, in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;
e) suggerire al Titolare del trattamento, ai Responsabili del trattamento l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati atte a che i dati personali, oggetto di trattamento, siano custoditi e controllati, anche in relazione alle conoscenze acquisite, in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

   Più specificamente, l'Amministratore di sistema dovrà:

   1) assegnare e gestire il sistema di autenticazione informatica e quindi, fra le altre, generare, sostituire e invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le password e i codici identificativi personali da assegnare ai Responsabili e agli Incaricati del trattamento dei dati, svolgendo anche la funzione di custode delle copie delle credenziali; più specificamente dovrà:
      - custodire le password personali degli incaricati del trattamento di dati personali con elaboratori elettronici e preservare con estrema attenzione il "cartellino delle credenziali di autenticazione";
      - nel caso in cui il Responsabile del trattamento abbia la necessità indifferibile di accedere a un elaboratore in caso di assenza o impedimento dell'incaricato che lo utilizza abitualmente, consentire al Responsabile del trattamento con una nuova password l'accesso all'elaboratore sul quale egli possa intervenire unicamente per necessità di operatività e sicurezza del sistema informativo; informare l'Incaricato del trattamento, allorché rientri in servizio, e consegnargli una nuova password

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

diversa da quella consegnata al Responsabile del trattamento durante la sua assenza, che lo stesso incaricato provvederà a variare al primo accesso al sistema.

2) procedere, più in particolare, alla disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva ai soggetti interessati l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali per oltre 6 (sei) mesi;
3) dotare e attivare nonché aggiornare adeguati programmi antivirus, firewall e altri strumenti software o hardware atti a garantire la massima misura di sicurezza e protezione dei dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici, e utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento e il funzionamento degli stessi;
4) aggiornare periodicamente, con frequenza almeno annuale (oppure semestrale se si trattano dati particolari o giudiziari), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
5) curare l'adozione e l'aggiornamento delle predette misure di sicurezza;
6) impartire a tutti i soggetti che comunque svolgano trattamento dei dati, istruzioni organizzative dirette al salvataggio quotidiano dei dati; prendere, pertanto, tutti i provvedimenti necessari a evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up; assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
7) adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
8) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza;
9) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati allorché si provveda al loro reimpiego.

6. All'Amministratore del sistema informatico è :
   a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema, a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;
   b) obbligato a dare tempestiva comunicazione al Titolare e ai Responsabili del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware sia dei software eventualmente rilevati;
   c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

7. Il Responsabile della protezione dei dati procederà, entro il mese di settembre di ogni anno, alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Art. 24
Responsabile della protezione dei dati
(artt. 37, 38, 39 – C97 - RGPD)

1. L'ARCA si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD), interno o esterno all'Agenzia, in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.
2. Il Responsabile della protezione è designato con decreto dell'Amministratore Unico.
3. Responsabile della protezione dei dati può essere designato un dipendente a tempo indeterminato dell'Agenzia, inquadrato in una categoria non inferiore alla D) ovvero un soggetto esterno, persona fisica o soggetto giuridico. La designazione da parte dell'Amministratore Unico del soggetto esterno avviene tra quanti abbiano partecipato ad una apposita procedura ad evidenza pubblica, nelle forme stabilite dalla legge, e assolve i suoi compiti in base a un contratto di servizio sottoscritto dal Dirigente preposto. L'assenza di conflitti di interesse, anche potenziali con l'esercizio dei propri compiti, é strettamente connessa agli obblighi di indipendenza del RPD.
4. Il Dirigente preposto alla sottoscrizione del contratto provvede, tempestivamente, a che i dati identificativi e di contatto del Responsabile della protezione dei dati siano:
   - pubblicati nel sito web istituzionale dell'Agenzia, e in particolar modo, rendendoli accessibili alla sezione Amministrazione Trasparente – Altri Contenuti – Privacy;
   - comunicati al Garante della Privacy;
   - comunicati ai componenti degli organi di governo, a tutti i dirigenti e dipendenti, ai componenti degli organi di controllo interni.
5. Sino alla designazione del nuovo RPD si intende prorogata di diritto la designazione del Responsabile della protezione dei dati in carica al momento della predetta proclamazione. Tale proroga é valida anche a seguito della nomina di un Commissario che sostituisca tutti gli organi di governo dell'Agenzia, salvo che lo stesso Commissario non ritenga necessario designare un nuovo Responsabile della protezione dei dati ovvero sostituire il Responsabile in carica all'atto della sua nomina.
6. Nell'atto di designazione del soggetto interno all'Agenzia ovvero nel contratto di servizio relativi all'affidamento dell'incarico di RPD devono essere riportati i compiti che lo stesso é tenuto a svolgere, tra cui almeno i seguenti:
   a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati; in tal senso il RPD può indicare al Titolare e/o ai Responsabili del

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD, di altre disposizioni dell'Unione o dello Stato relative alla protezione dei dati nonché delle politiche del titolare del trattamento o dei responsabili del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dai Responsabili del trattamento;
d) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD; il Titolare del trattamento, in particolare, si consulta con il RPD 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;
e) verificare e relazionare, entro il mese di settembre di ogni anno, riguardo alle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
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 del RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione.

7. Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. A tali fini il RPD procede a mappare le aree di attività e ne valuta il grado di rischio in termini di protezione dei dati, determinandone un elenco in ordine decrescente di gravità in modo da definire un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare e ai Responsabili del trattamento.
8. Il Titolare del trattamento e i Responsabili del trattamento si assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Responsabili del trattamento che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve ricevere tempestivamente, tramite posta elettronica, dal Titolare e dai Responsabili del trattamento tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da essere edotto sulla evoluzione della gestione in materia e da poter rendere una consulenza idonea, scritta od orale;
- é obbligatorio richiedere il parere del RPD sulle decisioni che impattano sulla disciplina e sulla prassi da seguire nell'Agenzia in materia di protezione dei dati; qualora la decisione assunta determini condotte difformi dal parere del RPD, è necessario motivare specificamente tale decisione;
- il RPD, consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente, con proprio parere indica quali provvedimenti debbano essere adottati per porre rimedio ovvero per prevenire il ripetersi di tali violazioni.

9. Il RPD è tenuto a manifestare il proprio dissenso alle decisioni o ai provvedimenti o ai comportamenti incompatibili con il RGPD adottati o tenuti dai componenti degli organi di governo e di controllo nonché degli organi di gestione e dei dipendenti ogni qual volta ne venga a conoscenza, dandone comunicazione all'Amministratore Unico, al Direttore Generale, ai Responsabili del trattamento interessati dai rilievi e, ove necessario, all'Amministratore del sistema informatico. I Responsabili del trattamento, qualora non condividano i rilievi formulati dal RPD, comunicano a quest'ultimo, all'Amministratore Unico e al Direttore Generale le proprie osservazioni. Il RPD dirama le direttive utili a prevenire il ripetersi delle violazioni rilevate.
10. Il Titolare del trattamento e i Responsabili del trattamento sostengono il Responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 del RGPD, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. In particolare é assicurato al RPD:
    - supporto attivo per lo svolgimento dei compiti da parte dei Responsabili del trattamento, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della redazione e approvazione degli atti di programmazione (Bilancio, Piano della performance, Piano della formazione, etc.);
    - tempo necessario e sufficiente per l'espletamento dei compiti affidati al RPD, in particolar modo qualora designato all'interno dell'Agenzia;
    - supporto adeguato in termini di risorse strumentali (sede e attrezzature) e umane (dipendenti) costituite in gruppo di lavoro che lo coadiuvi nell'espletamento dei suoi compiti;
    - accesso garantito ai settori funzionali dell'Agenzia così da fornirgli supporto, informazioni e input essenziali.
11. Il titolare del trattamento e i responsabili del trattamento si assicurano che il Responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti.
12. Il Responsabile della protezione dei dati non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

13. Il Responsabile della protezione dei dati riferisce direttamente al Titolare del Trattamento.
14. Gli interessati possono contattare direttamente il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento
15. Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o dello Stato.
16. Il Responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il Titolare del Trattamento pone in atto azioni tali da assicurare che lo svolgimento dei compiti e delle funzioni del RPD non diano adito a un conflitto di interessi.

Art. 25
Trattamento di dati personali nei servizi esternalizzati

1. Nella ipotesi che a soggetti pubblici o privati esterni siano affidati, tramite delega o concessione o contratto, lo svolgimento di compiti e/o servizi di competenza dell'ARCA, da cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve prevedere norme specifiche attraverso le quali si provvede: a nominare il legale rappresentante del soggetto, pubblico o privato ovvero la persona fisica, affidatario, quale responsabile esterno del trattamento dei dati personali per la durata dell'affidamento; a obbligare il soggetto affidatario a osservare le prescrizioni di cui al RGPD e alle altre fonti di diritto dell'Unione e dello Stato in materia di protezione dei dati personali; a consentire le verifiche sul rispetto delle predette disposizioni normative.
2. Nelle ipotesi di trattamento dei dati personali di cui al precedente comma, il Responsabile del trattamento della struttura organizzativa dell'ARCA competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza.
3. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, é determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento.
4. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal responsabile esterno del trattamento e dal soggetto interno che svolge ciascuna verifica.

Art. 26
Comunicazione interna di documenti contenenti dati personali del trattamento

1. La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a) del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo ovvero all'interno della struttura organizzativa di ARCA, per ragioni d'ufficio e nell'ambito delle specifiche competenze dei servizi, non è soggetta a limitazioni particolari, salvo quelle espressamente previste da leggi e regolamenti.

2. Il Responsabile del trattamento può, tuttavia, disporre, con adeguata motivazione, le misure necessarie per la protezione dei dati personali, qualora la comunicazione sia riferita a dati particolari e/o giudiziari.

Art. 27
Utilizzo di dati da parte dei componenti gli Organi Istituzionali e di controllo interno

1. L'Amministratore Unico nonché i componenti degli organi di controllo interno hanno diritto di accedere a documenti amministrativi detenuti da ARCA e contenenti dati personali, nei limiti e con le modalità previsti dalle disposizioni di legge e di regolamenti.
2. Le notizie e le informazioni così acquisite devono essere utilizzate esclusivamente per le finalità pertinenti alle rispettive competenze, rispettando il divieto di divulgazione dei predetti documenti nonché l'obbligo della segretezza del loro contenuto.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

CAPO IV
SICUREZZA DEI DATI PERSONALI

Art. 28
Misure per la sicurezza dei dati personali
(art. 32 – C83 - RGPD)

1. Il Titolare e i Responsabili del trattamento nonché l'Amministratore del sistema informatico e il Responsabile della protezione dei dati provvedono, per quanto di rispettiva competenza, all'adozione e alla dimostrazione di attuazione concreta di misure tecniche e organizzative adeguate per garantire un livello di sicurezza correlato 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 e 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 con cui sono trattati 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 e organizzative che possono essere adottate dal Settore cui è preposto ciascun Responsabile del trattamento:
   - sistemi di autenticazione, autorizzazione e 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; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
5. Il Titolare e i Responsabili del trattamento nonché l'Amministratore del sistema informatico e il Responsabile della protezione dei dati provvedono, per quanto di rispettiva competenza, a impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi e i dati di contatto del Titolare e dei Responsabili del trattamento nonché dell'Amministratore del sistema informatico e del Responsabile della protezione dei dati sono pubblicati sul sito web istituzionale dell'ARCA, sezione "Amministrazione Trasparente – Altri Contenuti – Privacy".

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

7. I responsabili del trattamento provvedono, nell'ambito dei propri poteri di controllo, a effettuare periodiche verifiche sulla corretta applicazione della normativa in materia di trattamento dei dati personali nell'ambito delle articolazioni organizzative cui sono preposti, in accordo con i controlli specifici effettuati dal responsabile della protezione dei dati.
8. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati particolari e giudiziari per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art. 29
Registro delle attività di trattamento del Titolare
(art. 30 – C82 - RGPD)

1. E' istituito il Registro delle attività di trattamento svolte dal Titolare del trattamento, sul quale sono annotate almeno le seguenti informazioni:
   a) il nome e i dati di contatto dell'ARCA, dell'Amministratore Unico ai sensi del precedente art.2, eventualmente del Contitolare del trattamento, del RPD;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno eventualmente comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è tenuto dal Titolare in forma telematica, e conterrà, altresì, il Registro delle categorie delle attività trattate dai Responsabili del trattamento di cui al successivo art. 30; nello stesso possono essere inserite ulteriori informazioni, tenuto conto delle dimensioni organizzative dell'Agenzia. E' facoltà del Titolare del trattamento, sentiti i Responsabili del trattamento, l'Amministratore del sistema informatico e il Responsabile della protezione dei dati, estrapolare dal predetto schema i dati attinenti ai rischi rilevati, alla loro ponderazione e alle rispettive misure individuate, annotandoli in un distinto apposito registro.
3. Il Titolare del trattamento può delegare la tenuta del predetto Registro unitario, e dell'eventuale distinto Registro dei rischi e delle misure, a ciascun Responsabile del trattamento ovvero a un solo Responsabile interno, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque l'obbligo di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro.
4. Il Registro deve essere aggiornato annualmente entro il termine e in conformità alle direttive diramate dal Responsabile della protezione dei dati, il quale é tenuto a comunicare, entro trenta giorni successivi al predetto termine, le eventuali inadempienze all'Amministratore Unico per le eventuali responsabilità dirigenziali e disciplinari che ne conseguono.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

Art. 30
Registro delle categorie di attività trattate dai responsabili
(art. 30 – C82 - RGPD)

1. Il Registro dei trattamenti contiene, altresì, l'elenco delle categorie di attività trattate da ciascun Responsabile del trattamento, nel quale sono annotate le seguenti informazioni:
   a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;
   b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;
   c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Detto Registro, tenuto in formato informatico, é compreso nel Registro unitario, nel quale sono annotati anche i dati di cui al Registro delle attività di trattamento del Titolare, di cui al precedente articolo 29.

Art. 31
Valutazioni di impatto sulla protezione dei dati
(artt. 35 e 36 – C84, C89, C93, C94, C95, C96 - RGPD)

1. Nel caso in cui una tipologia 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 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
   La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. 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'at. 35, paragrafi 4-6, del RGDP.
3. Fermo restando quanto indicato dall'art. 35, paragrafo 3, del RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
   a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
   b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati particolari o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del RGDP;
e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento presenti almeno due delle criticità sopra indicate occorre, in via generale, condurre una DPIA, salvo che il Titolare, sentito il Responsabile della protezione dei dati e l'Amministratore del sistema informatico, ritenga motivatamente che non si configuri un rischio elevato. Il Titolare può motivatamente ritenere che per un trattamento che presenti anche solo una delle criticità sopra elencate, sia comunque necessario la conduzione di una DPIA.

4. Il Titolare del trattamento garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA al Responsabile della protezione dei dati ovvero ad altro soggetto, interno o esterno all'ARCA.
   Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD, se gli viene affidata tale incombenza da parte del Titolare del trattamento, provvede allo svolgimento della DPIA ovvero, se non gli compete la predetta incombenza, monitora lo svolgimento della DPIA.
   I Responsabili del trattamento collaborano e assistono il Titolare del trattamento e il Responsabile della protezione dei dati nella conduzione della DPIA, redigendo per quanto di competenza il Registro unitario di cui ai precedenti articoli 29 e 30 e fornendo ogni informazione necessaria.
   L'Amministratore del sistema informatico fornisce il necessario supporto al Titolare per lo svolgimento della DPIA.
5. Il Responsabile della protezione dei dati può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

L'Amministratore del sistema informatico può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:
   a) 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, del RGDP;
   b) 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;
   c) se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

   Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o dal RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE, rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.
7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:
   a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. 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) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
      - delle finalità specifiche, esplicite e legittime;
      - della liceità del trattamento;
      - dei dati adeguati, pertinenti e limitati a quanto necessario;
      - del periodo limitato di conservazione;
      - delle informazioni fornite agli interessati;
      - del diritto di accesso e portabilità dei dati;
      - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
      - dei rapporti con i responsabili del trattamento;
      - delle garanzie per i trasferimenti internazionali di dati;
      - consultazione preventiva del Garante privacy;
   c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischio, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
   d) individuazione delle misure previste per affrontare e attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

8. Il Titolare del trattamento può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.
9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale.
10. 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.
11. E' pubblicata sul sito istituzionale dell'Agenzia, nella sezione "Amministrazione Trasparente – Altri Contenuti – Privacy", una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 32
Violazione dei dati personali
(artt. 33 e 34 – C85, C86, C87, C88 - RGPD)

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'ARCA.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato a informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
   a) danni fisici, materiali o immateriali alle persone fisiche;
   b) perdita del controllo dei dati personali;
   c) limitazione dei diritti, discriminazione;
   d) furto o usurpazione d'identità;
   e) danno economico o sociale;
   f) decifratura non autorizzata della pseudonimizzazione;
   g) pregiudizio alla reputazione;
   h) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

ARCA Puglia Centrale - Prot. n. 0019228 del 02/07/2018 13:00 - PARTENZA

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatasi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (a esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento;
   - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33.
6. Il Titolare del trattamento deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art. 33
Entrata in vigore, pubblicazione e divulgazione del Regolamento

1. L'efficacia del presente regolamento decorre dal giorno in cui diviene esecutivo il decreto con cui é stato approvato.
2. Il presente Regolamento, divenuto esecutivo, è pubblicato sul sito web istituzionale dell'ARCA, nella Sezione "Amministrazione Trasparente – Altri Contenuti – Privacy".
3. Il presente regolamento è trasmesso, per opportuna conoscenza, all'Organo di Vigilanza sulla regolarità contabile finanziaria ed economica dell'Agenzia (Collegio dei Sindaci), all'Organismo Indipendente di Valutazione (OIV), al Direttore Generale, ai Dirigenti, ai Responsabili di P.O., agli incaricati di Alta Professionalità ed a tutti i Dipendenti.