Politica generale per il trattamento dei dati personali

Istruzione operativa per l'attuazione del Regolamento UE 2016/679
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Approvato con Deliberazione dell'Amministratore Unico
del 14/06/2018 nr. 27

Documento	**IOPD 02-002**	**Politica generale per il trattamento e la protezione dei dati personali**

Revisione 1 del 21/05/2018

ARCA Jonica
(Agenzia Regionale per la Casa e l'Abitare di Taranto)
Via Pitagora, 144 - TARANTO - P.IVA: 00091580738
Centralino Tel. 099.45.39.411 - Fax 099. 45.35.992
PEO: info@arcajonica.gov.it - PEC: arcajonica@pec.it

Premessa

L'Ente tratta numerose informazioni personali, per tali intendendosi ai sensi di legge tutti i dati riferibili "*a persona fisica identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

Sotto il profilo qualitativo, oltre a dati cd. "comuni", si rinvengono informazioni di carattere "sensibile", dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale nonché dati personali idonei a rivelare provvedimenti giudiziari.

Inoltre l'Ente, per il trattamento dei dati personali, utilizza sia strumenti informatici (elaboratori) sia supporti cartacei o altri supporti di memorizzazione.

Oggetto

Il presente documento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'Ente **ARCA JONICA Taranto.**

Inoltre il presente documento descrive i ruoli, le responsabilità, le modalità di governo e di gestione operativa in materia di trattamento di dati personali adottati da **ARCA JONICA Taranto** in qualità di Titolare del trattamento (nel seguito anche "**Ente**") in ottemperanza al **Regolamento (UE) 2016/679 (RGPD).**

Campo di applicazione

L'ambito di applicazione del presente documento riguarda ARCA JONICA Taranto (di seguito indicata **"Ente")** che tratta dati personali sul territorio dello Stato italiano, anche in caso di trasferimento di dati personali da e verso l'estero (Paesi UE ed extra UE).

Destinatari e perimetro

Destinatario della presente Politica è tutto il personale di ogni ordine e grado di **ARCA JONICA Taranto** con riguardo alla gestione interna ed esterna dei dati personali.

Regole generali per il trattamento e la protezione dei dati personali

1. Principi generali

I dati personali devono essere sempre trattati in modo lecito e secondo correttezza sempre nel rispetto delle disposizioni del Regolamento UE 2016/679.

Tutto il personale che svolge detta attività (di seguito indicato come "**il Personale**") è tenuto ad attivarsi per far sì che i dati personali trattati siano sempre esatti e aggiornati.

I trattamenti non devono mai eccedere le finalità per le quali sono stati concepiti.

2. Principali definizioni

Nell'allegato 1 "**Glossario e definizioni**" sono riportate le principali definizioni richiamate nel presente documento.

3. Struttura organizzativa

Le norme sulla protezione dei dati personali individuano alcune figure organizzative obbligatorie:

3.1 Titolare del trattamento

L'Ente **ARCA JONICA Taranto,** rappresentato ai fini previsti dal RGPD dall'**Amministratore Unico**, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "**Titolare**").

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare 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. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

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.

Il Titolare, non avendo assegnato formalmente l'esercizio dei poteri del Titolare del trattamento ad alcun altro organo o Funzione aziendale, provvede a:

a) designare eventuali Responsabili del trattamento nelle persone dei Dirigenti/Responsabili delle singole strutture in cui si articola l'organizzazione, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della Protezione dei Dati (RPD);

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Organizzazione, relativamente alle banche dati gestite da soggetti esterni all'Organizzazione in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività aziendali;

d) decidere, in piena autonomia, in ordine alle finalità e alle modalità dei trattamenti dei dati personali, nonché agli strumenti utilizzati e al profilo della sicurezza;

e) nominare il personale "Addetti/Incaricati del trattamento", nei casi in cui questi non siano nominati dai Responsabili del trattamento.

L'Organizzazione favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

3.2 Responsabile del trattamento

Nomina dei responsabili esterni

Nei casi in cui un soggetto terzo effettua trattamenti di dati personali per conto dell'Ente e non può essere considerato come autonomo Titolare o come soggetto autorizzato del trattamento (incaricato), questi è nominato come **Responsabile trattamento dati esterno** ai sensi dell'art. 28 del Regolamento UE 2016/679.

Relativamente alla formalizzazione della nomina conseguente a tutte le tipologie di accordi/contratti, ogni Responsabile di settore ha la responsabilità di garantire che tutti i contratti aventi per oggetto in via diretta o indiretta un trattamento dei dati in nome e per conto dell'Ente contemplino delle specifiche clausole, definite in accordo con il Responsabile Protezione Dati, in cui si prevede la nomina della controparte a Responsabile esterno del trattamento oggetto del contratto. In alternativa il contratto dovrà essere integrato con la lettera di designazione a Responsabile Trattamento dei dati esterno.

3.3 Soggetto autorizzato del trattamento (ex Incaricato)

L'Ente designa come "Soggetto autorizzato del trattamento" tutto il proprio personale; contestualmente all'assunzione, l'ufficio Risorse Umane fornisce l'informativa e la lettera di nomina a "Soggetto autorizzato del trattamento".

L'Ente può designare come soggetti autorizzati (Incaricati) anche persone fisiche (esterne all'Organizzazione ed eventualmente facenti parte di società terze) che, per esigenze legate alle attività contrattualizzate, partecipano ai trattamenti di dati personali di cui **l'Ente** è Titolare.

Ogni soggetto autorizzato deve attenersi alle istruzioni ricevute dal titolare o dal responsabile del trattamento.

3.4 Amministratori di sistema

L'Ente adotta le misure di sicurezza necessarie ad adempiere alle prescrizioni definite dal Garante nel Provvedimento[1] dedicato alla figura dell'Amministratore di Sistema.

L'Organizzazione ha definito specifiche procedure operative per disciplinare i seguenti aspetti:

- selezione e nomina degli Amministratori di Sistema (sia per il personale interno che per i consulenti), attribuzione privilegi, aggiornamento dell'elenco degli amministratori di sistema e relativa formazione obbligatoria
- modifica e revoca delle nomine degli Amministratori di Sistema e dei relativi privilegi prevedendo il successivo aggiornamento del suddetto elenco
- verifica dell'attività degli Amministratori di Sistema
- gestione dei contratti di outsourcing e introduzione in questi ultimi delle opportune clausole per gli adempimenti Privacy in materia di Amministratori di Sistema
- gestione delle richieste da parte degli interessati di consultazione dell'elenco degli Amministratori di Sistema.

Nell'ambito dell'Ente, Il Responsabile Protezione Dati provvede alla verifica almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

3.5 Responsabile della protezione dati (Data Protection Officer)

Il Titolare del trattamento ha designato il **Responsabile della protezione dei dati** / **Data Protection Officer** (in seguito indicato con "RPD" o "DPO") un dipendente interno.

Il Responsabile Protezione Dati - RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del 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 e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.
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 dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, 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

[1] Provvedimento Garante del 27 novembre 2008 - Gazzetta Ufficiale n. 300 del 24 dicembre 2008 (modificato in base al provvedimento del 25 giugno 2009), "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

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

f) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.
L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

Il Titolare del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Riservatezza dei dati

Il Personale deve sempre usare la massima discrezione sui dati personali di cui sia a conoscenza, curando attentamente la loro protezione.

Per assicurare tale discrezione è importante che gli spazi operativi destinati al ricevimento degli utenti, alla raccolta dei documenti ed alla loro conservazione siano opportunamente delimitati, per evitare il fortuito accesso da parte di terzi o di personale non interessato. Anche le comunicazioni tra colleghi di dati personali di terzi deve limitarsi a quanto necessario per l'espletamento del servizio.

E' vietata ogni comunicazione di dati all'esterno dei "soggetti titolari", salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati.

Ogni informazione, sia che si tratti di attività attuali sia che si tratti di attività future, ed ogni altro materiale utilizzato o prodotto dai prestatori d'opera (dipendenti, consulenti o incaricati di ditte esterne) in relazione al proprio impiego/attività, è di proprietà dell'Ente.

E' vietato copiare, diffondere, pubblicare, inviare notizie e/o informazioni tecniche che in qualche modo possano ridurre la sicurezza di funzionamento d'impianti o reti o che in qualche modo possano permettere di arrecare danni, anche di immagine, alla struttura dell'Ente.

E' fatto divieto ad ogni dipendente o collaboratore dell'Ente, salvo espressa autorizzazione, rilasciare comunicazioni o interviste a nome e per conto della stessa.

5. Trattamenti dei dati personali

Tutte i settori ed uffici dell'Ente sono responsabili di verificare, prima dell'effettivo trattamento, la necessità di operare su dati personali; nel caso si presenti tale fattispecie, le stesse funzioni coinvolgono il Responsabile Protezione dei Dati per concordare con questa le modalità di trattamento.

In particolare i casi che richiedono specifici presidi sono quelli relativi a:

- trattamenti di dati biometrici;
- trattamenti di dati sensibili e giudiziari;
- trattamenti di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo ("profilazione")
- trattamenti di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie

- trasferimento di dati personali verso Paesi extra Ue

6. Sicurezza del trattamento [2]

Il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

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

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

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

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.

Il Titolare e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

7. Registro delle attività di trattamento

Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, presso gli uffici della struttura organizzativa dell'Ente in forma telematica/cartacea.

Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto dell'Ente e degli eventuali Contitolari 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 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

8. Valutazioni d'impatto sulla protezione dei dati (DPIA)

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il

[2] NdR: l'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

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 DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, 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;
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 sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
e) trattamenti di dati su larga scala, tenendo conto: del numero di 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, come i dipendenti dell'Ente, 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 soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

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 monitora lo svolgimento della DPIA.

9. Violazione dei dati personali (Data Breach)

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'Organizzazione.

Il personale addetto al trattamento qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti di sicurezza che possano esporre a rischio di violazione dei dati (data breach) deve tempestivamente informare il Titolare, attraverso il Referente Privacy Interno.

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*, utilizzando la procedura operativa predisposta (**MOPD 07 Gestione Data Breach**).

Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione entro 24 ore.

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:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;

- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari,
- giudiziari).

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 verificatesi.

10. Riscontro delle richieste di accesso ai dati personali

Ogni responsabile di settore, in collaborazione del Responsabile Protezione Dati, ha la responsabilità di gestire le richieste da parte degli interessati pervenute all'Ente relativamente alle casistiche identificate dall'art. 15 e seguenti del Regolamento UE 2016/679.

Il Responsabile di settore, in collaborazione con il Responsabile Protezione Dati, deve assicurare che l'interessato riceva riscontro alla sua richiesta entro 30 giorni. A tal fine il Responsabile di settore è supportato:

- dall'ufficio competente;
- dagli esperti legali per definire il testo della risposta;
- dagli outsourcer per raccogliere i dati personali, eventualmente trattati dai sistemi informatici, necessari a fornire il riscontro richiesto.

Per la gestione dei diritti degli interessati utilizzare la procedura operativa predisposta (**MOPD 04 Gestione Diritti degli Interessati**).

11. Comunicazione e diffusione dei dati

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche, specie se a riguardo di dati sensibili:

- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative e regolamenti che consentano/rendano obbligatoria la divulgazione.

12. Misure di sicurezza per il trattamento di dati personali effettuato senza strumenti elettronici

In particolare, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento effettuate senza l'ausilio di strumenti elettronici, gli Incaricati devono conservare gli atti, i documenti e ogni altro supporto contenente dati personali in ambienti controllati (ad esempio, locali, armadi o cassetti muniti di serratura), prelevandoli per il solo tempo necessario al loro utilizzo e restituendoli a chi ne ha la responsabilità e l'autorizzazione alla conservazione, al termine delle operazioni affidate. Nel dettaglio:

a) il materiale cartaceo contenente dati personali deve essere controllato e custodito con diligenza in modo da impedire che durante le quotidiane operazioni di lavoro terzi non autorizzati possano prenderne visione e, se il materiale contiene dati sensibili o giudiziari, esso dovrà essere conservato, sino alla restituzione, in contenitori muniti di serratura. Al termine del lavoro tutto il materiale dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura, in maniera che ad essi non accedano persone prive di autorizzazione;

b) l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato;

c) gli atti ed i documenti contenenti dati personali sensibili o giudiziari sono affidati agli Incaricati del trattamento esclusivamente per lo svolgimento dei relativi compiti assegnati in forma scritta: i medesimi atti e documenti sono controllati e custoditi dai predetti incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate

d) gli incaricati ammessi, a qualunque titolo, agli archivi contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, sono identificati e registrati: quando gli archivi non sono dotati di strumenti

elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate;

e) è obbligatorio distruggere o rendere inutilizzabili i documenti cartacei ed i supporti rimovibili, magnetici o ottici dismessi in modo da garantire che i dati ivi contenuti non possano più essere ricostruiti e/o utilizzati (anche parzialmente) da parte di terzi non autorizzati al trattamento: anche il materiale destinato al macero ed i supporti magnetici o ottici da eliminare devono essere trattati in modo che risulti tecnicamente impossibile recuperare, anche parzialmente, i dati contenuti negli stessi. Pertanto occorre prevederne la distruzione (se disponibili, con le apposite macchine "distruggi documenti/supporti" o con tecnologie similari, ad esempio i Cartbox in uso alla Società) in modo da garantire che i dati in essi contenuti non possano essere ricostruiti, anche parzialmente, o utilizzati;

f) tutte le stampe effettuate, contenenti dati personali, dovranno essere trattate in modo da evitare che terzi non autorizzati possano prenderne visione oppure accedervi e/o produrne copie.

Il responsabile di ogni settore/ufficio, verifica la corretta applicazione da parte degli incaricati di tutte le procedure previste in materia di trattamenti effettuati senza l'ausilio di strumenti elettronici finalizzate ad evitare accessi non autorizzati ai dati personali, anche se sensibili o giudiziari o trattamenti non consentiti.

Tale responsabile verifica in particolare che l'accesso agli archivi cartacei sia consentito al solo personale autorizzato e che la distruzione dei supporti cartacei che contengono dati personali venga effettuato in conformità alla normativa vigente, utilizzando ove possibile e se disponibili, le apposite apparecchiature "distruggi documenti".

13. Misure di sicurezza per il trattamento di dati personali effettuato con strumenti elettronici (Regole per l'utilizzo di strumenti informatici)

Il Titolare, I Responsabili e gli Incaricati al trattamento dei dati, qualora durante lo svolgimento della loro attività lavorativa utilizzino strumenti informatici devono rispettare quanto previsto dal "**POLITICA PER LA SICUREZZA E L'UTILIZZO DEGLI STRUMENTI INFORMATICI**" (Modello IOPD 02-003).

14. Smaltimento o riuso di apparecchiature elettriche ed elettroniche

Ogni Responsabile di settore è responsabile dell'adozione di opportune misure di sicurezza, anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, per garantire l'inesistenza o la non intelligibilità di dati personali sui supporti di memorizzazione destinati al reimpiego, al riciclaggio o allo smaltimento.

15. Verifiche periodiche

Oltre alla normale verifica delle attività operative in capo al Responsabile di Settore, sono previste verifiche periodiche in accordo con la normativa vigente al fine di **verificare il rispetto del presente Regolamento.**

L'Organizzazione si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno, che ledono diritti di terzi o che, comunque, risultino illegittime.

All'interno del Modello Organizzativo per la Protezione Dati previsto dall'Ente, le attività di valutazione delle misure organizzative, procedurali e tecniche sono in carico del Responsabile della Protezione dei Dati o altri professionisti esterni.

Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informativa nei confronti dei dipendenti e collaboratori.

16. Sanzioni

È fatto obbligo a tutti i Dipendenti e collaboratori dell'Ente di osservare le disposizioni portate a conoscenza con le presenti Istruzioni Operative. Il mancato rispetto o la violazione delle regole sopra ricordate é perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

La presente Politica è stata redatta tenendo conto della normativa vigente e dei Provvedimenti generali emanati dal Garante della Privacy. Per qualsiasi eventuale ulteriore indicazione, valgono oltre alla presente politica le disposizioni della normativa vigente.

Tutti gli dipendenti e collaboratori possono proporre, quando ritenuto necessario, integrazioni al presente documento. Le proposte vanno esaminate dal Titolare tramite il Responsabile Protezione Dati.

La presente Politica è soggetta a revisione con frequenza periodica o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente o collaboratore ovvero messo a disposizione per ogni soggetto autorizzato all'utilizzo della rete aziendale.

Con l'entrata in vigore del presente Politica, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

18. Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

Allegato 1: GLOSSARIO E PRINCIPALI DEFINIZIONI

Abbonato	Qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;	D.Lgs. 196/03
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;	GDPR
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità	D.Lgs. 196/03
Autorità di controllo	l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;	RGPD
Autorità di controllo interessata	un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;	RGPD
Banca di dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti	D.Lgs. 196/03
Blocco	La conservazione dei dati personali con sospensione temporanea di ogni altra operazione del trattamento;	D.Lgs. 196/03
Chiamata	La connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;	D.Lgs. 196/03
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;	D.Lgs. 196/03
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile	D.Lgs. 196/03
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;	GDPR
Credenziali di autenticazione	I dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica	D.Lgs. 196/03
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;	RGPD
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;	RGPD
Dati giudiziari	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;	D.Lgs. 196/03

Dati identificativi	i dati personali che permettono l'identificazione diretta dell'interessato;	D.Lgs. 196/03
Dati relativi al traffico	qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;	D.Lgs. 196/03
Dati relativi all'ubicazione	ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;	D.Lgs. 196/03
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;	GDPR
Dati sensibili	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;	D.Lgs. 196/03
Dato anonimo	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile	D.Lgs. 196/03
Dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale	RGPD
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;	RGPD
Diffusione	l dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;	D.Lgs. 196/03
Evidenza	Nell'ambito della ISO 19011 sono definite evidenze dell'audit le registrazioni, dichiarazioni di fatti o altre informazioni, che sono pertinenti ai criteri dell'audit e verificabili. Possono essere qualitative o quantitative	ISO 19011
Gruppo imprenditoriale	un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;	RGPD
Impresa	la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica	RGPD
Incaricati	le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;	D.Lgs. 196/03
Interessato	La persona fisica cui si riferiscono i dati personali	D.Lgs. 196/03
Limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;	RGPD
Misure minime	il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;	D.Lgs. 196/03
Norme vincolanti d'impresa	le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;	RGPD

Obiezione pertinente e motivata	un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione	RGPD
Organizzazione internazionale	un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati	RGPD
Parola chiave	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;	D.Lgs. 196/03
Politica (Policy)	Descrive, ad alto livello, la posizione di una organizzazione rispetto ad un determinato argomento. La policy, comportando un'assunzione di rischio, deve essere approvata dal top management	
Procedura	Una procedura descrive, con il livello di dettaglio adeguato, come un'organizzazione realizza uno specifico obiettivo. E' possibile che un'organizzazione si doti di un impianto documentale con procedure a diverso livello di dettaglio, dalle più generiche alle istruzioni operative. La modalità, il formato, la responsabilità di creazione e gestione, le modalità di revisione devono essere formalmente definite.	
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;	RGPD
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti	D.Lgs. 196/03
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;	RGPD
Rappresentante	la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;	RGPD
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;	RGPD
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;	RGPD
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;	RGPD

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;	RGPD
Trattamento transfrontaliero	a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro	RGPD
Stabilimento principale	a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;	RGPD
Servizio della società dell'informazione	il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio	RGPD
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;	RGPD