Azienda Lombarda per l'Edilizia Residenziale delle province di Bergamo, Lecco e Sondrio

ALER BG-LC-SO






REGOLAMENTO PER LA DISCIPLINA DELLA PRIVACY ADOTTATO DA ALER BG-LC-SO IN ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679

Approvato con provvedimento del presidente n° 46 del 7 ottobre 2026

INDICE

Articolo 1. SCOPO ... 1
Articolo 2. RIFERIMENTI ... 1
Articolo 3. DEFINIZIONI ... 1
Articolo 4. PRINCIPI GENERALI ... 5
ARTICOLO 4.1. LICEITÀ DEL TRATTAMENTO ... 5
ARTICOLO 4.2. PRINCIPIO DI NECESSITÀ ... 6
ARTICOLO 4.3. PRINCIPIO DI PROPORZIONALITÀ ... 6
ARTICOLO 4.4. FINALITÀ DEL TRATTAMENTO ... 7
Articolo 5. RESPONSABILITÀ ... 7
Articolo 5.1. TITOLARE DEL TRATTAMENTO ... 7
ARTICOLO 5.2. REFERENTE PRIVACY ... 8
ARTICOLO 5.3. SOGGETTI DESIGNATI ... 8
ARTICOLO 5.4. SOGGETTI AUTORIZZATI ... 8
ARTICOLO 5.5. RESPONSABILI DEL TRATTAMENTO IN TRATTAMENTI ESTERNALIZZATI ... 9
ARTICOLO 5.6. COLLABORAZIONE CON ALTRI ENTI ... 9
ARTICOLO 5.7. RESPONSABILE PROTEZIONE DATI ... 9
ARTICOLO 5.8. AMMINISTRATORI DI SISTEMA E TRATTAMENTI INFORMATIZZATI ... 10
Articolo 6. INFORMATIVA ... 11
Articolo 7. CONDIZIONI PER IL CONSENSO ... 12
Articolo 8. DIRITTI DELL'INTERESSATO ... 13
Articolo 9. REGISTRO DEI TRATTAMENTI ... 13
Articolo 10. MISURE DI SICUREZZA ... 13
ARTICOLO 10.1. SICUREZZA ORGANIZZATIVA IN MATERIA DI PRIVACY ... 14
ARTICOLO 10.2. SICUREZZA DELLE IDENTITÀ ... 14
ARTICOLO 10.3. SICUREZZA DELLE RETI ... 15
ARTICOLO 10.4. SICUREZZA DEI SISTEMI INFORMATIVI ... 15
ARTICOLO 10.5. SICUREZZA FISICA ... 16
ARTICOLO 10.6. DISASTER RECOVERY E CONTINUITÀ OPERATIVA ... 16
Articolo 11. TRATTAMENTI NON INFORMATIZZATI ... 16
Articolo 12. TRASPARENZA E PRIVACY ... 16
Articolo 13. VALUTAZIONE D'IMPATTO (DPIA) ... 17
Articolo 14. DATA BREACH ... 19
Articolo 15. CESSAZIONE DEL TRATTAMENTO DATI ... 20
Articolo 16. TUTELA AMMINISTRATIVA E GIURISDIZIONALE ... 20
Articolo 17. NORMA DI RINVIO ... 20
Articolo 18. APPROVAZIONE ... 20
Articolo 19. PUBBLICITÀ ... 20
Articolo 20. ORGANIGRAMMA DELLA PRIVACY ... 21

Articolo 1. SCOPO

Il presente regolamento disciplina l'ordinamento degli uffici e delle sedi dell'Azienda Lombarda per l'Edilizia Residenziale delle province di Bergamo, Lecco e Sondrio (d'ora in poi "ALER BG-LC-SO", "ALER", "Ente" o "Azienda") in attuazione delle disposizioni del Regolamento europeo n. 679 del 27 aprile 2016 (di seguito "GDPR") e del "Codice in materia di protezione dei dati personali" approvato con D.Lgs. 30 giugno 2003, n.196, (di seguito denominato "Codice") come modificato dal D.Lgs. 101 del 10 agosto 2018 ed in particolare:

- la corretta gestione delle informazioni e dei dati all'interno di ALER BG-LC-SO nell'ambito di quanto definito dal GDPR e dal Codice;
- l'identificazione delle politiche da utilizzare per la privacy;
- l'individuazione dei trattamenti effettuati nell'ambito della gestione della privacy in conformità con quanto definito dal Regolamento UE n. 2016/679;
- le modalità di conduzione della valutazione d'impatto (DPIA) secondo quanto previsto dall'art. 35 del Regolamento UE n. 2016/679;
- la gestione dell'esercizio dei diritti degli interessati;
- la gestione e registrazione degli incidenti in materia di privacy e del conseguente Data Breach.

Articolo 2. RIFERIMENTI

I riferimenti utilizzati per la gestione dei processi relativamente alla corretta gestione della privacy all'interno di ALER BG-LC-SO sono:

- REGOLAMENTO UE n. 2016/679: Regolamento Generale Sulla Protezione Dei Dati
- Decreto legislativo 10 agosto 2018, n. 101: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
- WP 248 rev.01 "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679"
- Provvedimento Garante Privacy n. 467 del 11 ottobre 2018 (pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

Articolo 3. DEFINIZIONI

- «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione,

diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; 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;
- «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

- «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Articolo 4. PRINCIPI GENERALI

ALER BG-LC-SO garantisce che il trattamento dei dati, a tutela delle persone fisiche, siano interlocutori siano utenti dei nostri servizi, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
ALER BG-LC-SO, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale, delle condizioni economiche e sociali dei cittadini che accedono ai nostri servizi e dei dati a loro associati.
Ai fini della tutela dei diritti e delle libertà degli utenti in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza di ALER BG-LC-SO, sono gestiti conformemente alle disposizioni del Codice, del GDPR, e del presente Regolamento.
I dati 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.
Le prescrizioni del presente Regolamento si fondano sui principi di liceità, necessità, proporzionalità e finalità.

Articolo 4.1. LICEITÀ DEL TRATTAMENTO

L'articolo 6 del GDPR indica espressamente che il trattamento dei dati è consentito solo quanto è lecito. In particolare secondo quanto riportato nel presente articolo, il trattamento dei dati effettuato all'interno di ALER BG-LC-SO è sempre legato allo svolgimento delle funzioni istituzionali ed al buon funzionamento dell'Ente, all'assolvimento di obblighi legali in capo all'amministrazione e in esecuzione di contratti posti in essere dall'Azienda con i soggetti interessati.

Infatti, l'art. 6 del GDPR, in odine alla liceità del trattamento, ha stabilito che il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetta ALER BG-LC-SO;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

ALER BG-LC-SO garantisce la liceità del trattamento indicando, per ogni trattamento effettuato ed individuato nel Registro dei Trattamenti, quale delle soprascritte sei condizioni ricorrono per i trattamenti effettuati.

Articolo 4.2. PRINCIPIO DI NECESSITÀ

I dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Il trattamento dei dati da parte di ALER BG-LC-SO deve essere sempre orientato verso un'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

In particolare, ALER BG-LC-SO garantisce l'esistenza di un nesso tra le finalità per cui i dati personali sono stati raccolti e le operazioni di trattamento effettuate. Non è consentito raccogliere dati non necessari e non pertinenti con le operazioni di trattamento effettuate.

Inoltre, i dati 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 sono 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.

Articolo 4.3. PRINCIPIO DI PROPORZIONALITÀ

Nel commisurare la necessità di trattare i dati all'interno di ALER BG-LC-SO, per poter esercitare in modo corretto le funzioni amministrative e istituzionali demandate dalla Regione Lombardia all'Azienda, va evitata la proliferazione di dati aggiuntivi, non necessari rispetto alle esigenze di

trattamento, e la rilevazione di dati per i quali non ricorra una effettiva esigenza di trattamento per l'esecuzione dei propri compiti istituzionali.
I dati trattati devono essere esatti e, se necessario, aggiornati. ALER BG-LC-SO adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

Articolo 4.4. FINALITÀ DEL TRATTAMENTO

Secondo quanto sopra riportato si evince che gli scopi perseguiti sono determinati, espliciti e legittimi in conformità con i principi prescritti dal Regolamento UE n. 2016/679.
I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con le finalità di seguito riportate. Un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali.
Infatti, i trattamenti sono compiuti da ALER per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
b) l'adempimento di un obbligo legale al quale è soggetta l'azienda nell'erogazione dei servizi di edilizia residenziale pubblica;
c) l'esecuzione di un contratto con soggetti interessati o per la conclusione dello stesso;
d) per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
e) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Tali finalità sono riportate per ogni trattamento effettuato nel Registro dei Trattamenti redatto in accordo con art. 30 del Regolamento.
Rientrano nelle finalità sopra riportate i trattamenti compiuti per:

a) l'esercizio delle funzioni attribuite dalla Regione Lombardia ad ALER BG-LC-SO che riguardano gli inquilini dei servizi di edilizia residenziale pubblica, i Comuni interessati dall'azione di ALER, gli interlocutori istituzionali, le associazioni a tutela degli inquilini;
b) la gestione dei progetti di edilizia residenziale pubblica e delle relazioni con fornitori e enti di controllo;
c) l'esercizio di ulteriori funzioni amministrative affidate dalla Regione Lombardia ad ALER BG-LC-SO per servizi connessi all'azione dell'Azienda, ovvero, per altri servizi in base a convenzione;
d) gestione dei condomini di edilizia residenziale pubblica;
e) la tutela in giudizio di ALER BG-LC-SO in caso di contenzioso.

Articolo 5. RESPONSABILITÀ

ALER BG-LC-SO ha definito con apposito allegato al presente Regolamento un Organigramma della Privacy riportante la struttura organizzativa interna deputata alla gestione degli adempimenti previsti dal presente Regolamento. Si riportano di seguito le responsabilità connesse alle singole figure.

Articolo 5.1. TITOLARE DEL TRATTAMENTO

Ai sensi dell'articolo 4 comma 7 del GDPR, il Titolare del trattamento ("Titolare") è la persona giuridica dell'Ente, rappresentata dal Presidente in qualità di legale rappresentante dell'Ente.
Ai sensi dell'articolo 2-quaterdecies del Codice Privacy, il legale rappresentante può designare un proprio Delegato specificando nell'atto di designazione i compiti relativi alla protezione dei dati personali che intende delegare. In ALER BG-LC-SO, tale delega può essere conferita al Direttore Generale.

Articolo 5.2. REFERENTE PRIVACY

Il Titolare designa un Referente Privacy dell'Ente ("Referente Privacy"), con compiti di coordinamento e controllo operativi relativamente alla protezione dei dati nell'Ente.
Il Referente Privacy:

- collabora con le Aree e gli Uffici dell'Ente per la piena attuazione del GDPR in conformità al presente Regolamento;
- predispone i modelli previsti dal presente Regolamento;
- verifica con cadenza annuale l'effettiva attuazione di quanto previsto dal presente Regolamento, riferendone l'esito al Titolare;
- funge da riferimento per le relazioni col RPD/DPO e monitora l'attuazione delle sue raccomandazioni;
- informa l'Ente sull'evoluzione normativa che ha impatti sulla protezione dei dati personali e propone modifiche al presente Regolamento;
- svolge tutti gli altri compiti assegnatigli dal presente Regolamento.

Articolo 5.3. SOGGETTI DESIGNATI

Ai sensi dell'art. 2-quaterdecies comma 1 del Codice Privacy, Il Titolare attribuisce alle figure apicali di Area la responsabilità di applicare il presente Regolamento nell'ambito organizzativo di cui sono a capo.
La designazione specifica l'ambito di responsabilità del Soggetto Designato ed è valida fino a nuova designazione per il medesimo ambito.
La designazione include la nomina del Soggetto Designato a Responsabile interno del trattamento ai sensi dell'articolo 28 del GDPR.
Con la designazione, il Titolare autorizza in via generale il Soggetto Designato a ricorrere a Responsabili esterni del trattamento, così che il Soggetto Designato possa sottoscrivere contratti con soggetti esterni che trattano dati personali per conto dell'Ente.
In collaborazione con l'Ufficio Organizzazione e Risorse Umane, il Referente Privacy predispone il modello per la designazione dei Soggetti Designati e segnala la necessità di nuove designazioni.

Articolo 5.4. SOGGETTI AUTORIZZATI

Ai sensi dell'articolo 29 del GDPR e dell'articolo 2-quaterdecies comma 2 del Codice Privacy, sono Soggetti Autorizzati i dipendenti ed i collaboratori che trattano dati personali sotto l'autorità del Titolare o di un Soggetto Designato.
L'assegnazione di un soggetto ad una unità organizzativa lo autorizza, senza necessità di altri atti da parte del Titolare, a trattare i dati personali necessari ai procedimenti svolti in quell'unità

organizzativa e limitatamente alle proprie mansioni. L'assegnazione del soggetto ad una o più unità organizzative è documentata dall'Organigramma aziendale.
Ai sensi dell'articolo 29 del GDPR, il Titolare provvede all'istruzione del Soggetto Autorizzato mediante corsi inseriti nel Piano di Formazione dell'Ente, il disciplinare all'uso dei sistemi informatici predisposto dal Servizio Informatico, il Codice Etico e specifiche istruzioni dell'unità organizzativa cui il Soggetto è assegnato.

Articolo 5.5. RESPONSABILI DEL TRATTAMENTO IN TRATTAMENTI ESTERNALIZZATI

ALER BG-LC-SO può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di riservatezza, integrità e disponibilità dei dati, 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.
Gli atti che disciplinano il rapporto tra ALER BG-LC-SO e il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, del GDPR.
In collaborazione col Referente Privacy, l'Ufficio "Appalti e Contratti" predispone modelli di clausole contrattuali e di atti separati per la designazione dei Responsabili esterni.
Con la collaborazione dei Soggetti Designati, il Referente Privacy tiene un elenco aggiornato dei fornitori pro tempore, che consente di conoscere nominativamente i destinatari dei dati personali indicati come categorie nei Registri delle attività di trattamento e nelle informative in materia di privacy.
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 od abbia un adeguato obbligo legale di riservatezza.

Articolo 5.6. COLLABORAZIONE CON ALTRI ENTI

Laddove la comunicazione di dati personali tra ALER BG-LC-SO ed altri enti pubblici non ricada nei casi previsti dall'articolo 2-ter del Codice Privacy, tale comunicazione è regolata da Convenzioni, che possono configurarsi come:

- un accordo di contitolarità ai sensi dell'articolo 26 del GPDR, qualora gli Enti definiscano congiuntamente finalità e mezzi del trattamento, oppure
- un contratto o atto giuridico equivalente ai sensi dell'articolo 28 del GPDR, qualora un Ente (Responsabile) svolga trattamenti di dati personali per conto di un altro Ente (Titolare).

Se la Convenzione non contiene le informazioni richieste dal GDPR, l'Ente propone agli altri Enti appositi accordi integrativi, col supporto del RPD/DPO.
Il Referente Privacy supporta il Titolare ed i Soggetti Designati all'analisi della casistica applicabile alle diverse collaborazioni dell'Ente e nella predisposizione degli eventuali accordi integrativi.

Articolo 5.7. RESPONSABILE PROTEZIONE DATI

Ai sensi dell'art. 37 e seguenti del GDPR, ALER si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD/DPO), 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.
Il Responsabile della protezione è designato con provvedimento del Presidente (titolare del trattamento) in favore del soggetto esterno scelto.
ALER BG-LC-SO, provvede tempestivamente, a che i dati identificativi e di contatto del Responsabile della protezione dei dati siano:

- pubblicati nel sito web istituzionale dell'Ente, rendendoli accessibili da un apposito link;
- comunicati al Garante della Privacy;
- comunicati ai componenti degli organi di governo regionale, a tutti i dirigenti dell'Azienda, ai componenti degli organi di controllo interni.

Sino alla designazione del nuovo RPD/DPO si intende prorogata di diritto la designazione del Responsabile della protezione dei dati in carica al momento della predetta proclamazione.
Nell'atto di designazione del RPC/DPO devono essere riportati i compiti che lo stesso è tenuto a svolgere, tra cui almeno i seguenti:

a) informare e fornire consulenza al Titolare del trattamento o ai Soggetti Designati del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa applicabile;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

ALER BG-LC-SO si impegna a:

a) mettere a disposizione del DPO adeguate risorse al fine di consentire l'ottimale svolgimento dei compiti e delle funzioni assegnate;
b) comunicare ogni scelta amministrativa e di indirizzo politico amministrativo che coinvolga anche potenzialmente attività di trattamento che, per numero di interessati o tipologia di dati, costituisca un potenziale rischio di riservatezza degli interessati;
c) adottare le indicazioni di adeguamento proposte dal DPO.

Il DPO fornisce il proprio parere, che può essere obbligatorio o facoltativo, in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano.

Articolo 5.8. AMMINISTRATORI DI SISTEMA E TRATTAMENTI INFORMATIZZATI

Su delega del Titolare, il Responsabile del Servizio Informatico designa uno o più Amministratori di Sistema, con i compiti definiti dal Provvedimento del Garante del 27 novembre 2008 e successivi. Designa altresì anche il Responsabile per la Sicurezza Informatica.

Le designazioni specificano l'ambito di responsabilità del singolo Amministratore di Sistema in termini di servizi e/o sistemi informatici amministrati. In caso di più Amministratori di Sistema, la designazione ne identifica uno principale, che coordina e verifica l'operatività degli altri.
In collaborazione col Servizio Informatico, il Referente Privacy predispone modelli di designazione degli Amministratori di Sistema e mette a disposizione del RPD/DPO le principali informazioni relative ai sistemi informatici ed alla sicurezza informatica.

Articolo 6. INFORMATIVA

ALER BG-LC-SO , al momento della raccolta dei dati personali, è tenuta a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal GDPR e dall'art 13 Codice, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico scaricabile dal sito istituzionale dell'ente.
L'informativa è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- diffusione sul sito istituzionale di ALER BG-LC-SO;
- apposita clausola inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il titolare;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alla procedura.

L'informativa contiene il seguente contenuto minimo:

- l'identità e i dati di contatto del Titolare e, ove presente, del suo rappresentante;
- i dati di contatto del DPO di ALER BG-LC-SO ;
- le finalità del trattamento;
- i destinatari dei dati;
- la base giuridica del trattamento;
- l'interesse legittimo del Titolare se quest'ultimo costituisce la base giuridica del trattamento;
- se il Titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto dell'interessato di chiedere al Titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo all'autorità di controllo;

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

Nel caso di dati personali non raccolti direttamente presso l'interessato:

a) il titolare deve informare l'interessato in merito a:
   - ✓ le categorie di dati personali trattati;
   - ✓ la fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;
b) l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del titolare è predisposta apposita informativa per il personale dipendente.

Articolo 7. CONDIZIONI PER IL CONSENSO

Femi restando i casi, disciplinati dalla normativa vigente, nei quali può essere legittimamente effettuato il trattamento senza consenso, nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica la disciplina del GDPR la quale prevede che:

- qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
- se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante;
- il consenso deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto;
- l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.

La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Per i dati sensibili il consenso deve essere esplicito e in forma scritta. Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione.

Il consenso dei minori è valido a partire dai 16 anni, fermo restando il diverso limite di età, comunque non inferiore a 13 anni, previsto dalla normativa nazionale; prima del limite di età previsto dalla normativa nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci.
In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.
Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, predisposta da ALER BG-LC-SO, previa consegna e presa d'atto dell'informativa.

Articolo 8. DIRITTI DELL'INTERESSATO

In ogni momento gli interessati potranno esercitare i propri diritti nei confronti di ALER BG-LC-SO , quale Titolare del trattamento, ai sensi dell'artt. 15-22 del Regolamento UE 2016/679, ed in particolare i diritti di accesso, rettifica, integrazione e, nei casi consentiti la portabilità dei dati conferiti, oltre ad ottenere la cancellazione, la limitazione o l'opposizione al trattamento dei dati per motivi legittimi e di opporsi al processo decisionale automatizzato, inclusa la profilazione.
I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
Le istanze sono presentate ai Responsabili dei Settori di riferimento, in qualità di Responsabili del trattamento nel proprio settore di riferimento.
Al fine di garantire la protezione delle informazioni personali dell'interessato, ALER BG-LC-SO potrebbe aver bisogno di richiedere ulteriori informazioni specifiche, che confermino l'identità dell'interessato richiedente e garantirne così il diritto di accesso alle informazioni (o a esercitare uno qualsiasi degli altri diritti) solamente a persone aventi il diritto di ricevere tali comunicazioni. Si tratta di un'altra misura di sicurezza idonea alla protezione dei dati personali.

Articolo 9. REGISTRO DEI TRATTAMENTI

ALER BG-LC-SO tiene un registro delle attività di trattamento svolte sotto la propria responsabilità ex articolo 30 del Regolamento UE n.679/2016 ("Registro del Titolare").
Il Referente Privacy predispone lo schema del Registro, ne aggiorna il contenuto con la collaborazione dei Soggetti Designati e del Servizio Informatico, lo verifica annualmente, e lo mette a disposizione del RPD/DPO e del Garante, in caso di richiesta.
Se l'Ente svolge attività come Responsabile del trattamento per conto di altri Titolari, viene istituito anche il Registro delle attività del Responsabile ("Registro del Responsabile"), con caratteristiche e modalità analoghe a quelle previste per il Registro del Titolare.

Articolo 10. MISURE DI SICUREZZA

ALER BG-LC-SO ha adottato, a norma dell'art. 32 del R.E. 2016/679 tutte le misure tecniche ed organizzative capaci di garantire un livello di sicurezza adeguato al rischio.

Le misure di sicurezza adottate in materia di privacy e data protection permettono di assicurare il controllo, la prevenzione dei rischi e la sicurezza nei seguenti ambiti:

- Sicurezza delle Identità
- Sicurezza delle Reti
- Sicurezza dei Sistemi informativi
- Sicurezza Organizzativa in materia di privacy
- Sicurezza Fisica
- Disaster Recovery e continuità operativa

Articolo 10.1. SICUREZZA ORGANIZZATIVA IN MATERIA DI PRIVACY

Il sistema di gestione della privacy di ALER BG-LC-SO ha definito un sistema di governo delle informazioni, con definizione di ruoli e responsabilità all'interno dell'Organizzazione ed i controlli a presidio della corretta esecuzione dell'attività in compliance con quanto definito dal Regolamento Europeo n. 2016/679.

Le misure definite nel sistema di sicurezza delle informazioni ed il rispetto dei requisiti previsti dalle suddette norme assicura il rispetto della compliance in materia anche di privacy e la riduzione dei rischi in materia di sicurezza informativa.

ALER BG-LC-SO ha adottato tra le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio valutato i seguenti strumenti previsti dall'articolo 32 comma 1 punto a) del Regolamento UE n. 2016/679:

- formazione generale e specifica del personale in materia di privacy;
- adozione di policies di gestione del sistema di trattamento dati e di sicurezza dei sistemi informativi;
- adozione di una serie di controlli e monitoraggi in grado di presidiare i trattamenti a rischio;
- pseudonimizzazione dei dati cartacei, ove possibile;
- pseudonimizzazione dei dati degli interessati su supporti informatici, ove possibile: quest'attività è effettuata attraverso l'attività di indicizzazione dei documenti relativi agli utenti effettuati per cui i dati sono archiviati attraverso codici univoci che non permettono di essere attribuiti ai soggetti interessati;
- crittografia: è applicata una cifratura dei dati sulle copie di backup salvate su supporto digitale esterno. I dati sono crittografati utilizzando un algoritmo di cifratura a blocchi considerato uno standard per la crittografia simmetrica.

Articolo 10.2. SICUREZZA DELLE IDENTITÀ

ALER BG-LC-SO ha adottato delle policies che consentono di identificare e riconoscere le persone che utilizzano e trattano i dati, fra cui in modo particolare i dati personali.

La responsabilità individuale nei trattamenti è fondamentale per poter prevenire e correggere comportamenti che, sia per errore che per volontà, possano minare l'integrità, la disponibilità e la riservatezza dei dati.

La creazione di un sistema in grado di gestire correttamente l'abbinamento fra l'identità dei soggetti e le attività che gli stessi svolgono nell'ambito delle informazioni non solo è da deterrente per ogni

attività dolosa ma contribuisce a creare ed elevare consapevolezza e responsabilità, che sono alla base della sicurezza delle informazioni e del principio di accountability espresso dal GDPR.
Le credenziali di accesso per gli operatori di ALER BG-LC-SO sono basate su una logica di profilazione degli utenti in base all'assetto organizzativo ed al ruolo ricoperto dal soggetto autorizzato rispettando comunque il principio del minimo privilegio.
A ciascun incaricato è affidato l'utilizzo e l'accesso ad un PC, ove necessario per l'esecuzione della propria attività lavorativa, dotato di un sistema di autenticazione informatica. In particolare, è previsto l'utilizzo da parte degli Incaricati di apposite credenziali di autenticazione che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
Ciascun Incaricato è reso edotto del fatto che le credenziali di autenticazione sono personali:

- devono essere memorizzate;
- non devono essere comunicate a nessuno;
- non devono essere trascritte.

Le "credenziali di autenticazione" consistono in:

- un codice per l'identificazione dell'incaricato ("user id") non assegnabile, neppure successivamente nel tempo, ad altro incaricato;

associato a,

- una parola chiave riservata conosciuta solamente dal medesimo ("password"), composta da almeno 8 (otto) caratteri (qualora il sistema preveda meno caratteri: il massimo consentito), non contenente riferimenti agevolmente riconducibili all'incaricato.

Le password devono essere conformi ai requisiti di complessità definiti dai sistemi medesimi.
ALER BG-LC-SO provvede periodicamente alla pulizia degli account per la disattivazione delle credenziali inutilizzate nel periodo, o riferite ad incaricati che hanno perso le qualità per accedere ai dati personali.
Sono state adottate policies di sicurezza anche nei casi di smarrimento delle password: IT, in quanto amministratore di sistema, procede con reset password; in caso di necessità improrogabili di accedere ad un account, l'accesso viene operato da IT nella sua funzione di amministratore di sistema.

Articolo 10.3. SICUREZZA DELLE RETI

Le reti, attraverso i dispositivi di accesso, consentono agli utilizzatori (fra cui anche gli stessi elaboratori) di poter accedere al patrimonio informativo.
Le misure di sicurezza delle reti sono attuate adottando misure volte a proteggerne la riservatezza, l'integrità e disponibilità delle informazioni in transito attraverso la stessa rete.
ALER BG-LC-SO adotta delle misure che consentono di ridurre i rischi legati alle reti (segregazione degli ambienti, autenticazione anche per gli accessi alla rete).

Articolo 10.4. SICUREZZA DEI SISTEMI INFORMATIVI

Le politiche di sicurezza dei sistemi includono tutte quelle misure di sicurezza volte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni aziendali elaborate e contenute all'interno delle architetture IT in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale

delle stesse, di accesso non autorizzato o di effettuazione di operazioni non consentite (articolo 32 comma 1 punto. B del Regolamento UE n. 679/20016).
L'infrastruttura di rete di ALER BG-LC-SO è oggetto di una continua attività di monitoraggio e aggiornamento dei sistemi HW e SW, potendo così definire logicamente l'organizzazione del network aziendale sia in termini di dominio che di sicurezza e classificazione logica dei sistemi.

Articolo 10.5. SICUREZZA FISICA

Le misure di sicurezza fisica presso le sedi operative di ALER BG-LC-SO prevedono:

- tutti gli archivi e database sono custoditi in contenitori/stanze chiuse con chiavi detenute dai responsabili di trattamento o dai responsabili di sistema;
- conformità degli impianti elettrici;
- misure di prevenzione e riduzione dei rischi da incendio: in tutte le sedi sono presenti estintori in funzione del rischio incendio valutato. Sugli estintori sono effettuati periodicamente gli interventi di manutenzione, revisione e collaudo;
- reception in grado di monitorare gli accessi alle sedi operative.

Articolo 10.6. DISASTER RECOVERY E CONTINUITÀ OPERATIVA

ALER BG-LC-SO sta attivando salvataggi in cloud, tramite adesione al Polo Strategico Nazionale (PSN) dei server e di tutti gli applicativi office; è dotata di unità esterne (QNAP) per il salvataggio dei dati che garantiscono misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio valutato che assicurino la capacità dell'Organizzazione di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (articolo 32 comma 1 punto del Regolamento UE n. 679/20016).

Articolo 11. TRATTAMENTI NON INFORMATIZZATI

Nell'ambito di propria responsabilità, ogni Soggetto Designato:

- verifica che le modalità operative dei trattamenti non informatizzati offrano un livello adeguato di protezione dei dati personali, con particolare attenzione all'accesso fisico ad uffici, archivi e stampanti, alla presenza di documenti contenenti dati personali negli spazi comuni (corridoi, sale ristoro, etc.), al rischio di ascolto di conversazioni riservate e ad ogni altra situazione che possa comportare rischi di violazioni di dati personali;
- segnala al Titolare ed al Referente Privacy le situazioni a rischio rilevate e propone misure tecniche ed organizzative per ridurre il rischio;
- provvede tempestivamente all'attuazione delle misure approvate e finanziate.

Il Responsabile dell'Ufficio Protocollo definisce le regole di accesso controllato e tracciato agli archivi centrali e le regole di scarto della documentazione cartacea.

Articolo 12. TRASPARENZA E PRIVACY

ALER BG-LC-SO ha degli obblighi di trasparenza previsti dal D.l.gs 33/2013 (Amministrazione Trasparente) e dagli obblighi di pubblicità legale previsti per le pubblicazioni sul sito istituzionale dell'Ente.

La base giuridica per il trattamento di dati personali in materia di trasparenza è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi dell'art. 6 comma 1, lett. e) del GDPR, «è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento».
Nel pubblicare tali dati, ALER BG-LC-SO deve valutare i dati necessari da pubblicare nel rispetto degli obblighi di trasparenza previsti dalla normativa applicabile sull'Ente (principio di necessità e di indispensabilità). Tale verifica viene effettuata dal Responsabile della Prevenzione della Corruzione e per la Trasparenza di ALER BG-LC-SO in quanto destinatario degli obblighi di pubblicazione. ALER BG-LC-SO pubblica solo i dati pertinenti rispetto all'obbligo di pubblicazione (principio di pertinenza e non eccedenza).
È, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" (art. 22, comma 8, del Codice) e "la vita sessuale" (art. 4, comma 6, del d. lgs. n. 33/2013).
La pubblicazione di dati ulteriori, rispetto a quelli obbligatori, nell'ottica di una maggiore trasparenza ed una riduzione del rischio di corruzione, è vincolata sempre alla richiesta di parere al RPD/DPO al fine di valutare se è prevalente l'interesse pubblico rappresentato dalla maggiore trasparenza dell'ente o il pregiudizio verso i soggetti interessati.

Articolo 13. VALUTAZIONE D'IMPATTO (DPIA)

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, ALER BG-LC-SO , prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del GDPR considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.
Ciò in coerenza con quanto previsto dall'art. 35 par. 1 GDPR secondo il quale "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*".
Per una più precisa identificazione di quando l'effettuazione di una DPIA, risulta obbligatoria si fa riferimento alle Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248) ed al provvedimento del Garante Privacy n. 467 del 11 ottobre 2018 (pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) che ha individuato, così come previsto all'art. 35 comma 4 del GDPR, le tipologie di trattamenti per i quali la DPIA è un adempimento obbligatorio.
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 del GDPR;
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, attraverso il Soggetto Designato, sentito il RPD/DPO, ritenga motivatamente che non può presentare un rischio elevato.

Il Titolare, attraverso il Soggetto Designato competente, può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Soggetto Designato dell'area interessata è il soggetto incaricato dell'effettuazione della DPIA ed è responsabile della stessa. Il Soggetto Designato può affidare la conduzione materiale della DPIA ad altro soggetto esterno ad ALER BG-LC-SO che abbia competenze riconosciute in materia di privacy.

Il RPD/DPO 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.

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 GDPR;
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 il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;

d) 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.

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

- Ruoli e responsabilità in materia di trattamento dei dati.
- Una descrizione dell'oggetto della valutazione che riporti: finalità e descrizione del trattamento, categorie di interessati e di dati trattati, periodo di conservazione dei dati, soggetti autorizzati al trattamento, tipo di trattamento, eventuali comunicazioni dei dati trattati, supporti elettronici e fisici impiegati, condizione di liceità, limitazione delle finalità.
- Descrizione del principio di minimizzazione ed esattezza dei dati, necessarietà e proporzionalità.
- Informativa e Diritti dell'interessato.
- I criteri che hanno reso necessario la DPIA (presenza di almeno due criteri o di un criterio a particolare rischio).
- Valutazione del rischio ed identificazione delle contromisure.
- Rischio residuo valutato.

Il Titolare deve consultare il RPD/DPO prima approvare la DPIA e consultare il Garante se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato o nei casi in cui la legislazione stabilisce l'obbligo di consultare l'Autority.

Articolo 14. DATA BREACH

Ai sensi del GDPR, uno degli obblighi fondamentali per ALER BG-LC-SO, nella qualità di Titolare del Trattamento, e dei Responsabili di trattamento designati, è quello della sicurezza nel trattamento dei dati personali.

In particolare, secondo il GDPR, la sicurezza è una tematica che include anche quelle della riservatezza, integrità e disponibilità dei dati e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

L'art. 33 del GDPR disciplina il Data Breach prevedendo espressamente un obbligo di notifica e comunicazione in capo al Titolare, in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati. All'atto della notifica all'autorità di controllo, il Titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. In effetti l'autorità di controllo può ordinare al Titolare del trattamento di informare le persone fisiche interessate dalla violazione. La comunicazione della violazione alle persone fisiche interessate consente al Titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione come previsto dall'art. 34 del Regolamento Europeo 2016/679 (GDPR). Allo stesso tempo, va ricordato che la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione al Titolare del trattamento ai sensi dell'articolo 83.

Ogni dipendente di ALER deve segnalare tempestivamente al Soggetto Designato dell'unità organizzativa cui è assegnato le situazioni di potenziale violazione di dati personali, fornendo ogni dettaglio utile alla valutazione. In assenza del Soggetto Designato, il dipendente la segnala al Referente Privacy.
Se la segnalazione non riguarda il proprio ambito, il Soggetto Designato interpellato inoltra senza indugio la segnalazione al Soggetto Designato nel cui ambito è presumibilmente avvenuta la violazione. Se la segnalazione riguarda generalmente i sistemi informatici, deve essere inoltrata al Responsabile del Servizio Informatico. Il soggetto così identificato (Soggetto Designato o Responsabile del Servizio Informatico) assume il ruolo di Responsabile della Segnalazione. Le modalità di gestione degli obblighi inerenti al Data Breach sono riportate all'interno di specifiche procedure adottate da ALER che assicurano il rispetto degli obblighi in caso di Data Breach.

Articolo 15. CESSAZIONE DEL TRATTAMENTO DATI

In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:

- distrutti con sistemi che rendono indisponibili i dati in modo definitivo;
- ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- conservati per fini esclusivamente istituzionali.

La cessione dei dati in violazione di disposizioni di legge in materia di trattamento dei dati personali, determina la loro inutilizzabilità, fatta salva l'applicazione di sanzioni disciplinari ed amministrative, e, ove previsto dalla vigente normativa, l'avvio degli eventuali procedimenti penali.

Articolo 16. TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 77 e seguenti del GDPR relativo alla protezione delle persone fisiche.
In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali, così come individuato dal precedente art. 5.

Articolo 17. NORMA DI RINVIO

Per quanto non disciplinato dal presente Regolamento si rinvia:

a. al Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
b. al D.l.gs 196/2003 e successive modificazioni;
c. alle leggi nazionali e regionali applicabili.

Articolo 18. APPROVAZIONE

Il Regolamento è adottato da apposito Provvedimento del Presidente di ALER BG-LC-SO.

Articolo 19. PUBBLICITÀ

Il Regolamento, una volta approvato verrà pubblicato sul sito internet istituzionale di ALER BG-LC-SO e diffuso a tutto il personale dell'Azienda.

Articolo 20. ORGANIGRAMMA DELLA PRIVACY

- Organigramma della Privacy

