

Regolamento Privacy

relativo alla protezione delle persone fisiche
con riguardo al trattamento dei dati personali,
nonché alla libera circolazione di tali dati

La missione principale degli Ordini a livello territoriale consiste nella tutela dell'interesse pubblico, in quanto garantiscono il cittadino circa la professionalità e la competenza dei professionisti che risultano iscritti.

L'Ordine ha l'obbligo di curare la formazione, la revisione e la pubblicazione dell'Albo, che è quindi la funzione preliminare rispetto a tutte le altre, quali:

- emissione di parere di congruità sulle parcelle
- tutela dell'esercizio professionale e del decoro, sia attraverso la repressione dell'esercizio abusivo della professione, sia attraverso il deferimento disciplinare e la celebrazione del relativo procedimento (Consiglio di disciplina)
- organizzare e facilitare l'obbligo di aggiornamento professionale degli iscritti individuare professionisti su richiesta di terzi

La tenuta dell'Albo e le altre attività che l'Ordine pone in essere, richiedono la predisposizione e il rispetto di presidi privacy da parte dell'Ordine, sia sotto il profilo organizzativo (Consiglio dell'Ordine) sia sotto il profilo operativo (Segreteria), con un'attenzione particolare al profilo disciplinare (Consiglio di Disciplina).

Ai sensi del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 e al Codice Privacy (D.Lgs 196/2003), con riferimento alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, il Consiglio dell'Ordine degli Architetti Pianificatori Paesaggisti e Conservatori della provincia di Lecco (definito d'ora in poi anche **Oappc Lecco**) delibera e adotta il seguente Regolamento.

1. OGGETTO E FINALITA'

Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività dell'**Oappc Lecco**.

2. DEFINIZIONI

"DATI PERSONALI": 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;

"DATI IDENTIFICATIVI": i dati personali che permettono l'identificazione della persona;

"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 organizzazione di carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"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. 14.11.2002 nr. 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;

"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

"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;

"RESPONSABILE DELLA PROTEZIONE DEI DATI": la persona esperta nella protezione dei dati, il cui compito è valutare e organizzare la gestione del trattamento di dati personali, e dunque la loro protezione, all'interno di un'azienda, di un ente o di una associazione, affinché questi siano trattati in modo lecito e pertinente;

"INCARICATI": i dipendenti e i consulenti dell'**Oappc Lecco**;

"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, l'**Oappc Lecco**, qualora riceva comunicazione di dati personali nell'ambito di un obbligo legale ai fini dell'esercizio della propria missione istituzionale non è considerato destinatario; il trattamento di tali dati 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 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.

3. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

L' **Oappc Lecco** garantisce che i dati personali sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**liceità, correttezza e trasparenza**);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (**limitazione della finalità**);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**minimizzazione dei dati**);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**esattezza**);
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**imitazione della conservazione**);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (**integrità e riservatezza**).

4. LICEITA' DEL TRATTAMENTO

Come previsto dall'art. 18 del Regolamento UE 679/16, l' **Oappc Lecco** nel raccogliere i dati personali dei propri iscritti non deve richiedere autorizzazione per il trattamento dei dati obbligatori in quanto necessari per l'espletamento della propria attività istituzionale, essendo compito di interesse pubblico.

Come previsto dall'art. 3 del R.D. 23.10.25 nr. 2537 l'Albo deve contenere di ogni singolo iscritto: cognome - nome - luogo e data di nascita - residenza - data e natura del titolo che abilita all'esercizio della professione con eventuale indicazione dell'autorità da cui il titolo stesso fu rilasciato - data di iscrizione. Sono pertanto questi dati obbligatori che ogni singolo iscritto deve fornire all'Ordine al momento dell'iscrizione e per i quali l'**Oappc Lecco** non è tenuto a richiedere alcun consenso per il trattamento.

Ogni iscritto può richiedere l'inserimento di dati ulteriori, purché pertinenti e non eccedenti rispetto all'attività professionale.

Il trattamento di dati ulteriori è lecito solo se:

- a) 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 soggetto l'**Oappc Lecco**;

I dati ulteriori, a richiesta dell'interessato, possono essere forniti a terzi dall'**Oappc Lecco** quando:

- a) attengono a speciali qualificazioni professionali non menzionate nell'Albo;
- b) attengono alla disponibilità ad assumere incarichi;
- c) attengono alla disponibilità a ricevere materiale informativo a carattere scientifico inerente anche convegni o seminari

5. CONDIZIONI PER IL CONSENSO

Per il trattamento di dati per i quali è previsto un consenso, l'**Oappc Lecco** raccoglie dall'interessato il consenso con una richiesta (*Allegato A*) redatta ai sensi dell'art. 7 del Regolamento UE 679/2016.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento inviando una comunicazione PEC all'indirizzo oappc.lecco@pec.aruba.it. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Il consenso è revocato con la stessa facilità con cui è accordato.

6. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

I dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica e i dati relativi alla salute della persona vengono trattati dall'**Oappc Lecco** solo dopo aver ricevuto esplicito consenso al trattamento degli stessi da parte dell'interessato.

L'**Oappc Lecco** non ha invece necessità di ricevere esplicito consenso al trattamento dei dati personali di cui al paragrafo precedente quando:

- a) le finalità sono relative all'assolvimento di obblighi e diritti specifici in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- b) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

- c) il trattamento è necessario per finalità di medicina del lavoro;
- d) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1 del Regolamento UE197/2016, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita.

7. DIRITTI DELL'INTERESSATO - INFORMAZIONI, COMUNICAZIONI E MODALITA' TRASPARENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

L'**Oappc Lecco** adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Nel sito <http://www.ordinearchitettilecco.it/> alla <http://www.ordinearchitettilecco.it/privacy/privacy> è consultabile l'informativa privacy.

8. DIRITTO DI ACCESSO DELL'INTERESSATO

L'interessato ha il diritto di ottenere dall'**Oappc Lecco** la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- c) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- d) l'esistenza del diritto dell'interessato di chiedere all'**Oappc Lecco** la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- e) il diritto di proporre reclamo a un'autorità di controllo;
- f) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

Qualora l'interessato presenti richiesta di accesso ai dati personali per una delle motivazioni sopraindicate, l'**Oappc Lecco** fornisce una copia dei dati personali oggetto di trattamento. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il termine per la risposta all'interessato è 1 mese.

La richiesta dovrà essere presentata utilizzando il modulo (*Allegato B*) reperibile nel sito <http://www.ordinearchitettilecco.it/privacy/privacy> inviandolo all'indirizzo PEC oappc.lecco@pec.aruba.it

Il diritto di ottenere una copia di cui al paragrafo precedente non deve ledere i diritti e le libertà altrui.

9. DIRITTO DI RETTIFICA

L'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Il termine per la risposta all'interessato è 1 mese.

La richiesta dovrà essere presentata utilizzando il modulo (Allegato B) reperibile nel sito <http://www.ordinearchitettilecco.it/privacy/privacy> inviandolo all'indirizzo PEC oappc.lecco@pec.aruba.it

10. DIRITTO ALLA CANCELLAZIONE ("DIRITTO ALL'OBLIO")

L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano, se sussiste uno dei motivi previsti dall'art. 17 del Regolamento UE 679/2016 e compilando il modulo (Allegato B) reperibile nel sito

<http://www.ordinearchitettilecco.it/privacy/privacy> inviandolo all'indirizzo PEC oappc.lecco@pec.aruba.it

Il termine per la risposta all'interessato è 1 mese.

11. DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Qualora l'interessato richieda la rettifica dei dati, o contesti l'esattezza dei dati personali o ravvisi la violazione dei diritti di liceità del trattamento, può chiedere la limitazione del trattamento, per il periodo necessario al Consiglio dell'**Oappc Lecco** per operare le opportune verifiche e/o rettifiche, compilando il modulo (Allegato B) reperibile nel sito

<http://www.ordinearchitettilecco.it/privacy/privacy> inviandolo all'indirizzo PEC oappc.lecco@pec.aruba.it

Prima che la limitazione al trattamento sia revocata, l'interessato riceverà l'informazione dall'**Oappc Lecco**.

12. DIRITTO ALLA PORTABILITA' DEI DATI

La portabilità dei dati garantisce il diritto di ricevere dati personali e di trattarli secondo la volontà dell'interessato.

Ai sensi dell'articolo 20, paragrafo 1, lettera a), del RGPD, il diritto alla portabilità dei dati presuppone che il trattamento si basi:

- sul consenso dell'interessato, oppure
- su un contratto di cui è parte l'interessato

Ai sensi dell' articolo 20, paragrafo 1, sono portabili i dati personali che

- riguardano l'interessato, e-sono stati forniti dall'interessato a un titolare.

Inoltre, l'articolo 20, paragrafo 4, stabilisce che l'osservanza del diritto alla portabilità non deve ledere i diritti e le libertà altrui

Qualora l'interessato decida di ricevere un sottoinsieme dei dati personali trattati dall'**Oappc Lecco** che lo riguardano, può farne richiesta inviando una PEC all'indirizzo oappc.lecco@pec.aruba.it specificando i dati che intende ricevere.

Qualora l'interessato decida di trasmettere dati personali dall'**Oappc Lecco** a un altro titolare del trattamento può farne richiesta inviando una PEC all'indirizzo oappc.lecco@pec.aruba.it specificando i dati che intende trasmettere.

Ottemperando a una richiesta di portabilità l'**Oappc Lecco** non ha alcun obbligo specifico di verificare la qualità dei dati prima di trasmetterli

L'**Oappc Lecco** non sarà responsabile del trattamento effettuato dal singolo interessato o da un altro titolare che riceva i dati in questione.

13. UTILIZZAZIONE DEI DATI PUBBLICI

I dati personali, diversi da quelli sensibili o giudiziari, che sono presenti nell'Albo in conformità alla legge vigente possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'art. 19 commi 2 e 3 del Regolamento, anche mediante reti di comunicazione elettronica.

I dati "trasmettibili" senza consensi sono quelli ritenuti obbligatori dalla Legge.

Su richiesta dell'interessato, l'**Oappc Lecco** può fornire a terzi notizie o informazioni relative a speciali qualificazioni professionali non menzionate nell'Albo, ovvero la disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni e seminari.

14. ACCESSO AGLI ATTI E DATI PERSONALI

Nel caso in cui l'**Oappc Lecco** riceva una richiesta di accesso agli atti vertente su documenti che potrebbero rivelare dati personali, ad esempio parcelle, elaborati o ulteriori elementi lesivi della privacy del controinteressato, provvederà al mascheramento degli atti e permetterà il solo rilascio di fotocopie annotando pagine e numero di copie estratte.

L'**Oappc Lecco** rifiuta richieste di accesso civico sui dati e documenti ulteriori se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi pubblici:

- sicurezza e ordine pubblico, sicurezza nazionale, difesa e questioni militari, relazioni internazionali, politica e stabilità finanziaria, conduzione di indagini su reati e loro perseguimento, regolare svolgimento di attività ispettive.
- L'**Oappc Lecco** rifiuta richieste di accesso civico sui dati e documenti ulteriori se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:
- protezione dei dati personali, in conformità al Codice Privacy libertà e segretezza della corrispondenza
- interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

15. TITOLARE DEL TRATTAMENTO

L'Ordine degli Architetti, Pianificatori, Paesaggisti e Conservatori della Provincia di Lecco, rappresentato ai fini previsti dal Regolamento dal Presidente pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Presidente può delegare le relative funzioni al Responsabile della protezione dei dati in possesso di adeguate competenze.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del Regolamento: 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 Regolamento. 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 Regolamento, 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 Regolamento, qualora i dati personali siano raccolti presso lo stesso interessato;
- b) le informazioni indicate dall'art. 14 Regolamento, qualora i dati personali non stati ottenuti presso lo stesso interessato.

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare effettua una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35 Regolamento, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

6. Il Titolare, inoltre, provvede a:

- a) designare il Responsabile del trattamento
- b) nominare il Responsabile della protezione dei dati

16. RESPONSABILE DEL TRATTAMENTO

Una Consigliere è nominato Responsabile del trattamento della banca dati in possesso dell'Ordine. Il Responsabile offre garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 18 (sicurezza del trattamento) rivolte a garantire che i trattamenti siano effettuati in conformità al Regolamento.

Il Titolare 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 cui al comma precedente, stipulando atti giuridici in forma scritta, che specificano 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 il Titolare ed il Responsabile del trattamento contengono in particolare quanto previsto dall'art. 28, p. 3, del Regolamento; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

E' consentita la nomina di un sub-responsabile del trattamento da parte del Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

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.

Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

17. RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD/DPO)

Il Responsabile della protezione dei dati è di seguito indicato con **"DPO"**

Il Titolare ed il Responsabile del trattamento provvedono affinché il **"DPO"** mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione.

Il **"DPO"** 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 Regolamento e dalle altre normative relative alla protezione dei dati. In tal senso il **"DPO"** 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 Regolamento 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 **"DPO"** in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al Regolamento;
- 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 Regolamento, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del **"DPO"** è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
- f) la tenuta del registro di cui al successivo art. 19;
- g) 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 **"DPO"**. Il Titolare ed il Responsabile del trattamento assicurano che il **"DPO"** sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il **"DPO"** 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 **"DPO"** 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 **"DPO"**, è necessario motivare specificamente tale decisione;
 - il **"DPO"** deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
 - Nello svolgimento dei compiti affidatigli il **"DPO"** deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il **"DPO"**:
- a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.
- Il **"DPO"** dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

La figura di **“DPO”** è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;
- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il Titolare ed il Responsabile del trattamento forniscono al **“DPO”** le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al **“DPO”**:

tempo sufficiente per l'espletamento dei compiti affidati al **“DPO”**;
supporto adeguato in termini di infrastrutture (attrezzature, strumentazione);
comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

Il **“DPO”** opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati. Il **“DPO”** non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il **“DPO”** riferisce direttamente al Titolare ed al Responsabile del trattamento.

Nel caso in cui siano rilevate dal **“DPO”** o sottoposte alla sua attenzione decisioni incompatibili con il Regolamento UE e con le indicazioni fornite dallo stesso **“DPO”**, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

18. SICUREZZA DEL TRATTAMENTO

Il Titolare e il Responsabile del trattamento mettono 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.

Le misure tecniche ed organizzative adottate dal Servizio cui è preposto il Responsabile del trattamento sono:

sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
misure antincendio; sistemi di rilevazione di intrusione; 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 Regolamento UE in materia di protezione dei dati personali è dimostrata attraverso l'adesione al codice di condotta approvato e disponibile al link

[Http://www.ordinearchitettiLecco.it/sites/ordinearchitettiLecco.it](http://www.ordinearchitettiLecco.it/sites/ordinearchitettiLecco.it)

Il Titolare e il 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.

I nominativi ed i dati di contatto del Titolare, del Responsabile del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Ordine, sezione Amministrazione trasparente.

19. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

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'Ordine;
- 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, come da precedente art.6.

Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 15, presso gli uffici dell'Ordine in forma telematica/cartacea, secondo lo schema allegato C al presente Regolamento.

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

20. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, attua una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del Regolamento, 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.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, pp. 4-6, Regolamento.

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, Regolamento, 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, concernenti aspetti riguardanti la situazione economica, le preferenze o gli interessi personali, il comportamento;
- b) decisioni automatizzate che producono significativi effetti giuridici o di analogia 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) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- e) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative.

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 garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'Ordine.

Il Titolare si consulta con il **"DPO"** anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare sono documentate nell'ambito della DPIA. Il **"DPO"** monitora lo svolgimento della DPIA. Il Responsabile del trattamento assiste il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il **"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:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, Regolamento;
- 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.

21. VIOLAZIONE DEI DATI PERSONALI

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'Ordine.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del Regolamento, sono i seguenti:

- danni 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.

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. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati; riguardare categorie particolari di dati personali; comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze); comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito); impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 Regolamento, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del Regolamento.

22. Rinvio

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