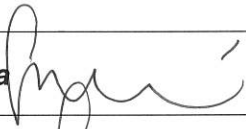




REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Redatto ai sensi dell'art. 30 del Regolamento UE 679/2016

Data di emissione:	24 giugno 2021	Firma 
Ultimo aggiornamento:	23 settembre 2026	Firma 

INDICE

FINALITÀ DEL TRATTAMENTO.....	7
DATI DI CONTATTO DEL TITOLARE E DEL RESPONSABILE DELLA PROTEZIONE DEI DATI	7
1. ELENCO DEI TRATTAMENTI DI DATI	8
1 Dati degli iscritti	9
2 Dati dei fornitori	11
3 Dati dei dipendenti e collaboratori.....	13
2. RUOLI, COMPITI E RESPONSABILITÀ	16
2.1 Gli incaricati del trattamento	16
2.2 Responsabile del trattamento	17
2.3 Responsabile della protezione dei dati	17
3. ANALISI DEI RISCHI E MISURE DI SICUREZZA	19
3.1 Comportamenti degli operatori.....	19
3.2 Eventi relativi agli strumenti	19
3.3 Eventi relativi al contesto	22
4. MISURE ADOTTATE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI	27
5. RIPRISTINO DISPONIBILITÀ DEI DATI	29
6. ELENCO DEGLI AGGIORNAMENTI.....	31

Lo scopo del presente documento è delineare il quadro di sicurezza del **sistema informativo** di:

**ORDINE DEGLI ARCHITETTI PIANIFICATORI PAESAGGISTI E
CONSERVATORI DELLA PROVINCIA DI TRIESTE**

VIA GENOVA 14 – TRIESTE

tel: +39 040768720

fax: +39 0230133584

mail: architetti@trieste.awn.it

pec: archtrieste@pec.aruba.it

L'Ordine è un Ente Pubblico non economico ed è soggetto all'applicazione del Regolamento UE 679/2016 in quanto soggetto pubblico titolare di un trattamento di dati che coinvolge informazioni di natura personale, sensibile e giudiziaria.

Il Consiglio è l'organo collegiale con funzione di rappresentanza esterna dell'ordine. Il Consiglio dell'Ordine, oltre alle funzioni attribuitegli dal R.D. 23 ottobre 1925, n. 2537 "REGOLAMENTO PER LE PROFESSIONI DI ARCHITETTO E INGEGNERE" o da altre disposizioni legislative o regolamentari:

- 1) vigila alla tutela dell'esercizio professionale, e alla conservazione del decoro dell'Ordine, reprimendo gli abusi e le mancanze di cui gli Iscritti si rendessero colpevoli nell'esercizio della professione;
- 2) segnala al Consiglio di disciplina fatti o notizie suscettibili di valutazione disciplinare;
- 3) cura che siano repressi l'uso abusivo del titolo di ingegnere e di architetto e l'esercizio abusivo della professione, presentando, ove occorra, denuncia all'autorità giudiziaria;
- 4) determina il contributo annuale da corrispondersi da ogni iscritto per il funzionamento dell'Ordine, nonché le modalità del pagamento del contributo;
- 5) compila ogni triennio la tariffa professionale, la quale, in mancanza di speciali accordi, s'intende accettata dalle parti ed ha valore per tutte le prestazioni degli iscritti all'Ordine;
- 6) dà i pareri che fossero richiesti dalle pubbliche amministrazioni su argomenti attinenti alle professioni di ingegnere e di architetto.

Al Presidente eletto in seno al Consiglio è affidata la rappresentanza legale dell'Ordine ed altresì i poteri di convocazione e governo dell'Assemblea.

Al Consigliere Segretario spetta la sovrintendenza sull'organizzazione burocratica. Il Consigliere Segretario riceve le domande di iscrizione nell'albo, annotandole in apposito registro e rilasciando ricevuta ai richiedenti; stende le deliberazioni consiliari; tiene i registri prescritti dal Consiglio, cura la corrispondenza, autentica le copie delle deliberazioni dell'ordine; ha in consegna l'archivio e la biblioteca.

Al Consigliere Tesoriere-Economo è affidata la gestione delle finanze dell'Ordine. Il Consigliere Tesoriere-Economo è responsabile dei fondi e degli altri titoli di valore di proprietà dell'ordine; riscuote il contributo; paga i mandati firmati dal Presidente e controfirmati dal Segretario. Deve tenere i seguenti registri:

- a) registri a madre e figlia per le somme riscosse;
- b) registro contabile di entrata e di uscita;
- c) registro dei mandati di pagamento;
- d) inventario del patrimonio dell'Ordine.

La riforma delle professioni di cui al DPR n. 137/2012 ha stabilito la netta separazione tra le funzioni amministrative e quelle disciplinari svolte dagli organismi di autogoverno degli Ordini Professionali.

Mentre le prime rimangono in capo al Consiglio dell'Ordine, le seconde sono trasferite a un nuovo organismo, autonomo e indipendente, denominato "Consiglio di disciplina territoriale".

Il Consiglio di disciplina risiede presso l'Ordine degli Ingegneri della Provincia di Trieste, ha funzioni e poteri di valutazione preliminare, istruzione e decisione delle questioni disciplinari riguardanti gli iscritti all'Albo ai sensi dell'art. 5, punto 4 della legge istitutiva dell'Ordine (Legge n. 1395/1923) e degli artt. 43-50 del Regolamento attuativo (R.D. n. 2537/1925).

È previsto che il Consiglio di disciplina sia articolato in Collegi.

Normativa di riferimento per le attività dell'Ordine:

- **L. 24 giugno 1923, n. 1395** *"Tutela del titolo e dell'esercizio professionale degli ingegneri e degli architetti"*.
- **R.D. 23 ottobre 1925, n. 2537** *"Approvazione del Regolamento per le professioni di ingegnere e di architetto"*.
- **L. 25 aprile 1938, n. 897** *"Norme sull'obbligatorietà dell'iscrizione negli albi professionali e sulle funzioni relative alla custodia degli albi"*.
- **D.Lgs.Lgt. 23 novembre 1944, n. 382** *"Norme sui Consigli degli ordini e collegi e sulle Commissioni centrali professionali"*.
- **D.Lgs. C.P.S. 25 settembre 1947, n. 1063** *"Norme per l'esercizio delle libere professioni nel territorio della Repubblica da parte di coloro che acquistino la cittadinanza del territorio libero di Trieste"*.
- **Legge 03-08-1949, n. 536**
- **D.P.R. 3 luglio 1961, n. 1197** *"Regolamento di esecuzione della legge 8 dicembre 1956, n. 1378 concernente l'abilitazione definitiva all'esercizio professionale"*.
- **Direttiva 2003/98/CE**, (concernente il riutilizzo dei documenti del settore pubblico) e Ordinamento nazionale.
- **Art. 15 del D.Lgs. 157/95** modificato dal D.Lgs. 25 febbraio 2000, n. 65
- **D.P.R. 5 giugno 2001, n. 328** *"Modifiche ed integrazioni della disciplina dei requisiti per l'ammissione all'esame di Stato e delle relative prove per l'esercizio di talune professioni, nonché della disciplina dei relativi ordinamenti"*.
- **Decreto del Presidente della Repubblica 8 luglio 2005 n. 169** *"Regolamento per le elezioni del Consiglio"*.
- **D.L. 2 Febbraio 2006 n. 30** *"Riconoscizione dei principi fondamentali in materia di professioni, ai sensi dell'art. 1 della L. 5 Giugno 2003 n. 131"*.
- **D.Lgs. 30 giugno 2003, n. 196** *"Codice in materia di protezione dei dati personali"*.
- **Regolamento UE 679/2016** 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 (regolamento generale sulla protezione dei dati) – di seguito anche solo "Regolamento".

- **D.P.R. 7 Agosto 2012, n. 137** *Regolamento recante riforma degli ordinamenti professionali, a norma dell'articolo 3, comma 5, del decreto-legge 13 agosto 2011, n. 138, convertito, con modificazioni, dalla legge 14 settembre 2011, n. 148. 12G0159).*
- **Circolare Agid 18 Aprile 2017 n. 2** *“Misure Minime Di Sicurezza ICT Per Le Pubbliche Amministrazioni)*

FINALITÀ DEL TRATTAMENTO

Le finalità del trattamento sono quelle finalità relative:

- all'espletamento delle attività istituzionali e statutarie previste dalla normativa su indicata (tenuta dell'albo, fissazione del contributo dovuto dagli iscritti, richieste di pareri sulle controversie professionali e sulla liquidazione di onorari e spese, vigilanza e tutela dell'esercizio professionale; comunicazioni agli iscritti; gestione della formazione);
- alle attività amministrative della gestione dei rapporti di lavoro dei dipendenti e collaboratori;
- all'attività contrattualistica e contabile dei rapporti con i fornitori di beni e servizi;
- alla gestione dei procedimenti disciplinari attraverso il Consiglio di Disciplina di cui al D.P.R. 137/2012;
- all'adempimento degli obblighi di trasparenza (D.Lgs. 33/2013 e provvedimenti ANAC);
- all'adempimento agli obblighi di legge e attività amministrative correlati alle su elencate finalità.

Modalità di trattamento

Il trattamento dei dati personali avviene con e senza l'ausilio di strumenti elettronici, con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza e l'integrità dei dati stessi e sempre nel rispetto dei principi di cui all'art. 5 del Regolamento.

Per lo svolgimento di alcune delle attività relative al trattamento dei dati personali, l'Ordine comunica determinati dati a soggetti esterni di fiducia con compiti e responsabilità specificate di cui si dirà in seguito.

Il trattamento non comporta processi decisionali automatizzati, compresa la profilazione, che producano effetti giuridici o incidano in modo analogamente significativo sugli interessati ai sensi dell'art. 22 del Regolamento.

DATI DI CONTATTO DEL TITOLARE E DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Titolare del trattamento è l'Ordine degli Architetti, Pianificatori, Paesaggisti e Conservatori della Provincia di Trieste, in persona del Presidente pro tempore, con sede in Via Genova n. 14 a Trieste, Tel. 040768720, E-mail architetti@trieste.awn.it.

L'Ordine ha designato quale Responsabile della protezione dei dati (art. 37 del Regolamento UE 679/2016) l'Avv. Stefano Corsini, raggiungibile agli stessi dati di contatto del Titolare o all'indirizzo E-mail dpo@avvocatocorsini.it.

1. ELENCO DEI TRATTAMENTI DI DATI

I dati trattati sono riconducibili alle seguenti categorie:

- Elementi d'identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato e di lavoro, numero di telefono, di fax, indirizzi di posta elettronica e P.E.C., partita IVA, codice fiscale, natura del titolo di abilitazione);
- Stato di salute;
- Adesione a sindacati od organizzazioni a carattere sindacale.

Altre categorie di dati

- Dati relativi a provvedimenti o procedimenti giudiziari.
- Dati relativi a giudizi disciplinari (limitatamente alla ricezione di esposti e all'applicazione dei provvedimenti stabiliti dal Consiglio di Disciplina).
- Dati relativi a controversie professionali e sulla liquidazione di onorari e spese, ai sensi dell'art. 5 L. 1395/1923 e s.m..
- Dati relativi al grado di istruzione e di cultura.

Soggetti cui si riferiscono i dati

Le categorie di soggetti fisici e giuridici interessati a cui si riferiscono i dati, in dettaglio, sono le seguenti:

- Iscritti; sono da considerare iscritti anche i membri del Consiglio dell'Ordine.
- Personale dipendente;
- Fornitori di beni e/o servizi;

I dati personali sono trattati con e senza l'ausilio di strumenti elettronici.

1 Dati degli iscritti

ISCRITTI	
Descrizione sintetica	Indirizzo, Codice Fiscale, P.IVA, telefono, indirizzo e-mail, certificato di nascita; certificato di cittadinanza italiana o il certificato dello Stato avente trattamento di reciprocità con l'Italia; certificato di residenza; certificato generale del casellario giudiziale; certificato di aver conseguita l'approvazione nell'esame di Stato. Parcelle e incarichi. Provvedimenti disciplinari. Data e natura del titolo abilitativo. Nei procedimenti di valutazione delle parcelle e degli incarichi possono venire in rilievo dati personali di terzi eventualmente coinvolti nei menzionati procedimenti. Finalità e base giuridica: finalità di interesse pubblico necessarie allo svolgimento delle funzioni istituzionali (ai sensi di quanto previsto da: L. 1395/1923 – R.D. 2537/1925 – L. 897/1938 – D.Lgs.Lgt. 382/1944 – D.P.R. 328/2001 – D.P.R. 137/2012 – D.Lgs. 33/2013 - L. 183/2011 - D.M. 8/2/2013 n. 34 e s.m.i.), e più precisamente: 1) per perfezionare l'iscrizione all'Albo professionale della Provincia di Trieste unitamente alle operazioni necessarie di aggiornamento dello stesso, ivi incluse le operazioni di trasferimento o cancellazione; 2) per il rilascio di pareri sulle controversie professionali e sulla liquidazione di onorari e spese (ai sensi di quanto previsto dall'art. 5 L. 1395/1923) e adempiere agli obblighi correlati; 3) rappresentanza istituzionale e di categoria; 4) tutela della professione di architetto; 5) organizzazione e gestione delle attività per la formazione obbligatoria; 6) per assolvere agli obblighi di pubblicità legale; per trasmettere agli iscritti le comunicazioni relative all'attività istituzionale dell'Ente (invio di pubblicazioni informative, organizzazione di convegni, informazioni su concorsi di progettazione, ecc.), anche attraverso l'invio di posta elettronica, anche mediante la piattaforma Htemail (scheda 5), in esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare, ai sensi dell'art. 6, comma 1, lett. e, e comma 3, del Regolamento e dell'art. 2-ter del D.Lgs. 196/2003.
Natura dei dati	I dati trattati sono di natura comune, sensibile e giudiziaria.
Struttura di riferimento	A questi dati personali accedono i dipendenti incaricati, il Consiglio dell'Ordine, il Consigliere Segretario, il Consigliere Tesoriere-Economo e le Commissioni istituite per legge secondo il principio di competenza. I dati relativi ai procedimenti disciplinari sono di pertinenza esclusiva dell'organo di disciplina – Responsabile del trattamento. L'Ordine riceve gli esposti e

	provvede agli adempimenti di legge una volta ricevute le decisioni dell'organo disciplinare.	
Strumenti utilizzati	Archivi Cartacei	Strumenti elettronici
	I documenti quali parcelle, contabilità, circolari, comunicazioni varie, archivio iscritti vengono conservati in armadi chiusi a chiave in zona non accessibile a terzi non autorizzati. Ai documenti contenenti dati giudiziari accedono solo soggetti autorizzati in qualità di incaricati e Responsabili del trattamento, nell'espletamento delle rispettive mansioni lavorative o istituzionali. L'archivio storico con i documenti più vecchi è situato in una stanza chiusa a chiave. L'accesso è controllato dal personale incaricato, il quale presidia altresì i locali ove sono ubicati gli archivi cartacei ed informatici.	Computer ad uso degli incaricati, accessibili con credenziali d'autenticazione personali, sui quali è installata la suite di programmi elencati nella relazione tecnica allegata. Software di videoscrittura, browser, Outlook per la posta elettronica, fax, P.E.C. per le comunicazioni istituzionali. Piattaforma Htemail per l'invio delle comunicazioni istituzionali agli iscritti (scheda 5).
Destinatari e categorie di destinatari	I dati personali diversi da quelli sensibili o giudiziari che devono essere inseriti nell'albo professionale in conformità alla legge potranno essere comunicati a soggetti pubblici e privati, ad enti previdenziali e pubbliche amministrazioni competenti o diffusi, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che a qualsiasi titolo incidono sull'esercizio della professione. Nell'espletamento delle sue funzioni istituzionali (Legge 24 Giugno 1923 n. 1395 e s.m.; R.D.L. 24 gennaio 1924, n. 103 e s.m.; R.D. 23.10.1925 N. 2537 e s.m.; D.L.L. 23.11.1944 N. 382 e s.m.; Legge 03-08-1949, n. 536, art. 2, e s.m.; Legge 25.04.1938 N. 897 e s.m.) l'Ordine potrà, se necessario, comunicare dati sensibili e/o giudiziari a pubbliche amministrazioni, organi e Autorità competenti. I dati potranno essere altresì comunicati al Consiglio di Disciplina qualora necessario per l'esercizio della potestà disciplinare riservata al predetto Organo che opera in qualità di Responsabile del trattamento ai sensi dell'art. 28 del GDPR. E' coinvolto nel trattamento dei dati degli iscritti, per l'aspetto disciplinare in supporto al C.d.D. e in caso di controversie con gli iscritti, un professionista Avvocato nominato responsabile del trattamento. Cognome, nome e indirizzo e-mail degli iscritti sono trattati, per conto del titolare, da Gruppo Semplitech srl, responsabile del trattamento ai sensi	

	dell'art. 28 del Regolamento, per l'invio delle comunicazioni istituzionali mediante la piattaforma Htemail (scheda 5).
Durata della conservazione	I dati sono conservati per il tempo previsto dalla legge. L'Ordine è un Ente pubblico e sottopone i suoi documenti ad archiviazione per tutta la durata dell'iscrizione all'ordine ed anche successivamente per ragioni di archiviazione storica.

2 Dati dei fornitori

ANAGRAFICA FORNITORI		
Descrizione sintetica	In questo archivio sono conservati i dati personali dei fornitori di beni e servizi dell'Ordine, in particolare: ▪ Dati anagrafici dei fornitori. ▪ Corrispondenza con i fornitori. ▪ Dati da pubblicare in Amministrazione trasparente. ▪ Documenti necessari ai fini della fatturazione e della tenuta della contabilità. Finalità e base giuridica: esecuzione degli obblighi contrattuali e l'adempimento degli obblighi di legge conseguenti e correlati al rapporto di fornitura.	
Natura dei dati	Dati personali comuni.	
Struttura di riferimento	A questi dati personali accedono i dipendenti incaricati, il Consigliere Tesoriere-Economo e il Consiglio dell'Ordine.	
Strumenti utilizzati	Archivi Cartacei	Strumenti elettronici
	I documenti quali parcelle, fatture, contabilità dei fornitori di beni e servizi sono conservati in fascicoli presso l'ufficio segreteria ed in ulteriori locali in zona non accessibile a terzi non autorizzati.	Computer ad uso degli incaricati, accessibili con credenziali d'autenticazione personali, sui quali è installata la suite di programmi elencati nella relazione tecnica allegata. Software di videoscrittura, browser, Outlook per la posta elettronica, fax, P.E.C. per le comunicazioni istituzionali. Sito web "Amministrazione trasparente".

Destinatari e categorie di destinatari	I dati strettamente necessari alle operazioni contabili e fiscali saranno comunicati ad un professionista di fiducia. Per le suesposte finalità, inoltre, i Suoi dati potranno essere comunicati a Banche ed Istituti di Credito, nonché a Studi Legali (per la tutela giudiziale e stragiudiziale), al Consiglio Nazionale degli Architetti, all'ANAC. L'ambito di comunicazione è nazionale e, salvo obblighi di legge (ad es. trasparenza ai sensi del D.Lgs. 33/2013), tali dati non saranno diffusi.
Durata della conservazione	I dati sono conservati per il tempo previsto dalla legge, ad es. 10 anni per le fatture. Dai 3 ai 5 anni per i dati in Amministrazione trasparente.

3 Dati dei dipendenti e collaboratori

ANAGRAFICA COLLABORATORI E DIPENDENTI		
Descrizione sintetica	Dati personali del personale dipendente e/o dei collaboratori, necessari alla gestione del rapporto di lavoro: ▪ Dati anagrafici. ▪ Corrispondenza e/o comunicazioni. ▪ Documenti necessari per la gestione anche fiscale, assistenziale e previdenziale del rapporto di lavoro. Finalità e base giuridica: finalità connesse alla gestione amministrativa, giuslavoristica, fiscale, assistenziale e retributiva della posizione lavorativa, ivi compreso la gestione del contenzioso e dei procedimenti disciplinari. Si precisa che il trattamento dei dati avviene per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, ed inoltre che il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.	
Natura dei dati	Dati personali comuni e sensibili.	
Struttura di riferimento	A questi dati personali accedono i dipendenti e collaboratori incaricati, il Consiglio dell'Ordine, il Consigliere Segretario e il Consigliere Tesoriere-Economo.	
Strumenti utilizzati	Archivi Cartacei	Strumenti elettronici
	I documenti (contratti, anagrafica, comunicazioni, certificati medici) sono conservati in archivi ad accesso selezionato presso l'ufficio segreteria cui accedono solo soggetti autorizzati.	Computer ad uso dei dipendenti incaricati, accessibili con credenziali d'autenticazione personali, sui quali è installata la suite di programmi elencati nella relazione tecnica allegata. Software di videoscrittura, browser, Outlook per la posta elettronica, fax, P.E.C. per le comunicazioni istituzionali.
Destinatari e categorie di destinatari	I dati strettamente necessari per il perfezionamento delle operazioni di elaborazione della busta paga e della relativa gestione fiscale e assistenziale potranno inoltre essere comunicati a professionisti di fiducia (Commercialista e Consulente del Lavoro). I dati potranno inoltre essere comunicati a: Pubbliche Amministrazioni, Banche, Assicurazioni private (per la gestione di pratiche relative a rischi assicurati), enti di formazione, consulenti per la sicurezza ex D.Lgs. 81/2008. L'ambito di comunicazione è nazionale	

Durata della conservazione	I dati dei dipendenti sono conservati per tutta la durata del rapporto e fino ai dieci anni successivi all'interruzione.
-----------------------------------	--

4 SEGNALAZIONE DI ILLECITI

WHISTLEBLOWING		
Descrizione sintetica	Dati personali dei soggetti che segnalano illeciti e dati personali dei soggetti segnalati. Finalità e base giuridica: gestione del canale interno di segnalazione in adempimento degli obblighi di legge.	
Natura dei dati	Dati personali. La natura dei dati può variare a seconda delle informazioni fornite dal segnalante. Ad oggi nessuna segnalazione è pervenuta.	
Struttura di riferimento	A questi dati personali accedono i dipendenti incaricati a supporto del RPCT ed eventualmente del suo sostituto.	
Strumenti utilizzati	Archivi Cartacei	Strumenti elettronici
	Nessun archivio cartaceo esistente.	Piattaforma whistleblowing. Mail del RPCT (non per lo scambio corrispondenza con segnalanti).
Destinatari e categorie di destinatari	I dati possono essere comunicati alle Autorità competenti per obbligo di legge, all'ANAC se necessario.	
Durata della conservazione	I dati sono conservati per 5 anni decorrenti dalla comunicazione del termine del procedimento.	
DPIA	Il trattamento è stato sottoposto a valutazione d'impatto ex art. 13 D.lgs. 24/2023 il cui esito è stato favorevole.	

5 COMUNICAZIONI ISTITUZIONALI AGLI ISCRITTI

NEWSLETTER	
Descrizione sintetica	Gestione della rubrica dei destinatari, predisposizione, programmazione e invio delle newsletter, circolari, avvisi e comunicazioni istituzionali dell'Ordine mediante la piattaforma Htemail; gestione delle cancellazioni; consultazione delle statistiche di invio, consegna ed errore di consegna. Non sono attivate la rilevazione dell'apertura dei messaggi e dei click sui collegamenti. Interessati: iscritti all'Albo ed eventuali ulteriori destinatari individuati dal titolare; utenti della piattaforma autorizzati dal titolare.

	Finalità e base giuridica: invio delle comunicazioni istituzionali agli iscritti, in esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare, ai sensi dell'art. 6, comma 1, lett. e, e comma 3, del Regolamento e dell'art. 2-ter del D.Lgs. 196/2003 (L. 1395/1923 - R.D. 2537/1925 - D.Lgs.Lgt. 382/1944 - D.P.R. 137/2012).	
Natura dei dati	Dati personali comuni: a) cognome, nome e indirizzo e-mail dei destinatari; b) dati generati dall'utilizzo del servizio (data e ora degli invii, esiti di consegna e di mancata consegna, richieste di cancellazione); c) dati degli utenti della piattaforma (credenziali, indirizzo e-mail per l'autenticazione a due fattori, registrazioni degli accessi e delle operazioni). È vietato l'inserimento di dati di cui agli artt. 9 e 10 del Regolamento e di dati relativi a procedimenti disciplinari.	
Struttura di riferimento	Accedono alla piattaforma la Responsabile Amministrativa della Segreteria e il Consigliere Segretario, come da atti di autorizzazione.	
Strumenti utilizzati	Archivi Cartacei	Strumenti elettronici
	Nessun archivio cartaceo.	Piattaforma Htemail in modalità cloud, accessibile via HTTPS con credenziali individuali e autenticazione a due fattori.
Destinatari e categorie di destinatari	I dati sono trattati, per conto del titolare, da Gruppo Semplitech srl (Udine), responsabile del trattamento ai sensi dell'art. 28 del Regolamento, che si avvale del sub-responsabile OVH per l'hosting e i backup. Dati e backup sono localizzati in Francia e Germania; non sono previsti trasferimenti verso Paesi terzi. Non sono previste comunicazioni a terzi né diffusione.	
Durata della conservazione	Cognome, nome e indirizzo e-mail: per la durata dell'iscrizione all'Albo o fino alla richiesta di cancellazione dalle comunicazioni. Dati generati dall'utilizzo del servizio e registrazioni degli accessi: dodici mesi dalla generazione. Alla cessazione del servizio si applica quanto previsto dall'accordo ex art. 28 del Regolamento.	
DPIA	Il trattamento è stato sottoposto a valutazione preliminare, con esito negativo circa la necessità della valutazione d'impatto ex art. 35 del Regolamento.	

2. RUOLI, COMPITI E RESPONSABILITÀ

L'Ordine degli Architetti della Provincia di Trieste (di seguito Ordine) ha nominato i propri dipendenti e collaboratori quali incaricati del trattamento con il preciso scopo di fornire loro le dovute istruzioni per garantire il trattamento dei dati personali in conformità alla legge.

Ciascun soggetto è stato istruito al fine del corretto svolgimento delle proprie mansioni, ed attraverso periodici interventi formativi o di aggiornamento viene edotto circa i propri compiti e responsabilità all'interno dell'Ordine.

2.1 Gli incaricati del trattamento

- **Dipendenti e collaboratori**, come da atti di nomina che si allegano al presente Documento.

Elenco trattamenti autorizzati: archivi informatici *iscritti, fornitori, dipendenti-collaboratori*; archivi cartacei *dipendenti-collaboratori (per consultazione ed organizzazione), fornitori, iscritti*.

Compiti: la raccolta, la registrazione, l'organizzazione, 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 (con espressa esclusione di dati sensibili e giudiziari salvo esprese deroghe di legge), il raffronto, la limitazione, la cancellazione e la distruzione dei dati trattati in relazione:

- all'attività di gestione dei rapporti di lavoro all'interno dell'ente;
- all'espletamento delle attività istituzionali (tenuta dell'albo, fissazione del contributo dovuto dagli iscritti, richieste di pareri sulle controversie professionali e sulla liquidazione di onorari e spese, vigilanza e tutela dell'esercizio professionale, gestione della formazione);
- alle attività di supporto all'organismo di disciplina;
- attività contrattualistica e contabile dei rapporti con i fornitori di beni e servizi;
- alla gestione dei curriculum pervenuti all'Ordine;

- all'adempimento degli obblighi di legge e attività amministrative correlati alle suelencate finalità.

L'unità organizzativa "**Consiglio dell'Ordine**" è stata autorizzata al trattamento dei dati per lo svolgimento delle proprie funzioni istituzionali come per legge. Si rimanda all'atto di nomina per i dettagli della designazione.

L'unità organizzativa "**Commissione Parcelle**" è stata autorizzata al trattamento dei dati di rispettiva competenza.

2.2 Responsabile del trattamento

L'Ordine ha individuato quali responsabili del trattamento ai sensi dell'art. 28 del Regolamento UE 679/2016 i seguenti soggetti:

- 1) Consiglio di disciplina territoriale.
- 2) Società Visura SpA (ex ISI Sviluppo Informatico Srl) per l'assistenza sul software gestionale.
- 3) Dott. Mario Costa consulente del lavoro.
- 4) Studio Russo Vuch commercialisti.
- 5) Ergon S.T.P. per il servizio di RSPP.
- 6) Avv. Marco Antonucci per il servizio di consulenza giuridica al Consiglio di Disciplina.
- 7) Avv. Romea Bon per il servizio di consulenza giuridica continuativa.
- 8) Gruppo Semplitech srl per l'attivazione, la configurazione, l'assistenza e la gestione tecnica del servizio di comunicazione Htemail (sub-responsabile: OVH, per hosting e backup).

Per i trattamenti esternalizzati di breve durata, l'Ordine comunque procede con designazione ai sensi dell'art. 28 GDPR.

2.3 Responsabile della protezione dei dati

L'Ordine, sulla scorta dell'art. 37 che impone la nomina obbligatoria del Responsabile della protezione dei dati per gli enti pubblici (cd. RPD), ha inteso individuare per ricoprire tale ruolo il professionista esterno Avv. Stefano Corsini del Foro di Pordenone,

contattabile all'indirizzo eMail *dpo@avvocatocorsini.it*. Il RPD è stato scelto sulla base della sua formazione professionale e della sua comprovata esperienza in tema di protezione dei dati personali a favore di enti pubblici – anche ordinistici – e privati.

3. ANALISI DEI RISCHI E MISURE DI SICUREZZA

3.1 Comportamenti degli operatori

Ad ogni soggetto, responsabile e incaricato del trattamento, viene consegnata una copia del "Regolamento privacy e sicurezza" (o anche "Mansionario"), in cui vengono descritte dettagliatamente le corrette modalità operative; in particolare il Regolamento serve a:

1. rendere edotto l'utente circa la corretta gestione delle credenziali di autenticazione, per evitare che possano essere carpite ed utilizzate da soggetti non autorizzati, siano essi esterni all'Ordine, o interni allo stesso.
2. spiegare minuziosamente le corrette procedure da applicare, e il motivo per cui è necessario operare in tal modo: questo è opportuno per minimizzare gli errori materiali e gli errori causati da scarsa consapevolezza, disattenzione, incuria.
3. illustrare le modalità di utilizzo degli strumenti elettronici messi a disposizione dall'Ordine e della posta elettronica.

Quanto al rischio che l'incaricato o i responsabili, tramite comportamenti sleali o fraudolenti, diffonda o comunichi senza autorizzazione informazioni e/o duplicati estratti dagli archivi cartacei o informatici, il titolare si è tutelato facendo firmare ad ognuno di loro l'atto di nomina, con cui si sono impegnati a non divulgare informazioni che riguardano le attività ed i dati personali dell'Ordine.

3.2 Eventi relativi agli strumenti

a) Rischio di distruzione, perdita, alterazione dei dati:

- accesso abusivo al sistema informatico dall'esterno *ex art. 615 ter c.p.* volto al danneggiamento, distruzione o alterazione dei dati.

misura: sono presenti sui computer un software antivirus ed un firewall. I sistemi operativi e i software gestionali vengono aggiornati al momento del rilascio di una patch di sicurezza ad opera delle rispettive software house.

- installazione di un programma diretto a danneggiare un sistema informatico *ex art. 615 quinquies c.p.* dall'esterno o dall'interno.

misura: è vietato installare software non autorizzati dal titolare del trattamento all'interno del sistema informatico dell'ufficio (come da regole di comportamento contenute nel Manuale). È attivo un software antivirus, aggiornato automaticamente ad ogni *update* disponibile. Si provvede all'aggiornamento dei software utilizzati e dei sistemi operativi appena una patch risulta disponibile.

Il Regolamento Privacy e Sicurezza spiega il comportamento da tenere per evitare infezioni indesiderate o per scongiurare il rischio di vulnerabilità della rete e degli strumenti.

- furto o sottrazione di elaboratori su cui sono custoditi i dati, furto o sottrazione di archivi cartacei:

misura: l'Ordine si trova al primo piano di un edificio privato ed ha una sola entrata. Durante l'orario in cui l'Ordine è aperto gli accessi sono controllati dal personale dell'Ordine. I computer e l'archivio cartaceo sono posti nell'area dell'ufficio segreteria di pertinenza dell'Ordine Ingegneri.

I locali di segreteria consistono in un *open space* diviso a metà fra l'Ordine degli Architetti e l'Ordine degli Ingegneri; i rispettivi archivi cartacei, come gli archivi e la rete informatica, sono separati ed altresì protetti da serratura con chiave e posti sotto il controllo costante e diretto degli incaricati del trattamento. Ogni accesso abusivo e non autorizzato di soggetti terzi o estranei può ritenersi scongiurato.

- danneggiamenti ad archivi o distruzione di apparecchiature hardware dovute a: sabotaggio, atti vandalici, problemi all'alimentazione di rete dovuti ad eventi eccezionali, incendi, calamità naturali:

misura: vista l'ubicazione dell'ufficio e la natura delle attività svolte, non si ritiene che tali rischi possano essere evitati del tutto poiché rientrano nelle tipologie della forza maggiore e/o del caso fortuito.

E' attivo un UPS per evitare danneggiamenti o perdite di dati a causa di una interruzione improvvisa della corrente o di sbalzi di tensione.

L'impianto elettrico è da ritenersi a norma di legge.

b) Rischio di accessi esterni non autorizzati:

- accesso non autorizzato ai dati contenuti nel sistema informatico:

misura: Su tutti i PC è stata attivata la password di accesso al Sistema Operativo. La password è composta da almeno 8 caratteri alfanumerici (o pari al massimo consentito), non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. Per accedere ai software della suite ISI esiste una password personale per i dipendenti e collaboratori di segreteria. Gli elaboratori sono comunque ad esclusivo utilizzo degli incaricati del trattamento. Quanto al rischio che soggetti esterni riescano a penetrarvi fraudolentemente, l'Ordine ha approntato le seguenti misure:

- software antivirus aggiornato automaticamente, per impedire che l'utente, anche in maniera inconsapevole, esegua programmi che consentano a malintenzionati di accedere ai dati senza autorizzazione;
- firewall hardware per evitare accessi abusivi al sistema informatico dell'Ordine;
- aggiornamento automatico del Sistema Operativo e dell'antivirus.
- Verifica periodica delle vulnerabilità tecnologiche tramite il Responsabile esterno su base contrattuale.

- accesso non autorizzato ai documenti cartacei:

misura: tutte le attività dell'Ordine sono regolate secondo le norme indicate in premessa, secondo il codice deontologico di categoria e secondo i principi dettati negli atti di nomina ad incaricato e responsabile del trattamento e nel relativo Regolamento (allegato 1).

I documenti cartacei sono conservati in maniera tale da prevenire che soggetti non autorizzati possano venirne a contatto: il Regolamento contiene l'indicazione delle procedure che l'incaricato deve rispettare per non pregiudicare la sicurezza dei documenti cartacei.

c) Malfunzionamento, indisponibilità o degrado degli strumenti informatici

- **misura:** l'Ordine provvede affinché gli strumenti informatici utilizzati siano in buono stato di conservazione e perfettamente funzionanti; se del caso, provvede a far effettuare gli interventi di manutenzione necessari.

Per evitare che il comportamento disattento del dipendente o la sua scarsa conoscenza del funzionamento degli apparati che compongono il sistema

informatico possa causare un malfunzionamento allo stesso, l'Ordine provvederà a rendere edotto il dipendente circa i comportamenti corretti e quelli da evitare.

E' attivo un gruppo di continuità (cd. UPS) per evitare danneggiamenti alle apparecchiature informatiche dovute a interruzioni improvvise della corrente elettrica o sbalzi di tensione.

L'Ordine provvede volta per volta a farsi rilasciare dagli installatori e manutentori del sistema informatico un rapporto che descrive gli interventi effettuati e le operazioni eseguite.

Il backup frequente dei dati trattati con strumenti elettronici consente di garantire la disponibilità dei dati.

3.3 Eventi relativi al contesto

a) Accesso non autorizzato ai locali

Misura: I locali dove sono situati gli archivi cartacei e le apparecchiature hardware sono sorvegliate dagli incaricati al trattamento ed altresì chiusi a chiave, i quali si preoccupano che i locali in oggetto non vengano lasciati incustoditi o comunque a disposizione di soggetti estranei all'Ordine o che non siano autorizzati ad entrare in contatto con i dati ivi custoditi.

La sede dell'Ordine si trova al primo piano di un edificio, cui si accede da una unica porta munita di serratura. Il rischio che qualche malintenzionato possa introdursi fraudolentemente forzando le serrature non può essere scongiurato del tutto.

b) Asportazione e furto di strumenti contenenti dati

Misura: la sede dell'Ordine è dotata delle misure logistiche per minimizzare il rischio di furti e asportazioni degli strumenti elettronici:

- 1) Accesso chiuso a chiave nelle ore notturne;
- 2) Stanze sorvegliate dal personale;
- 3) Archivi chiusi a chiave e sorvegliati dal personale.

L'accesso ai locali che contengono gli elaboratori con i dati personali può avvenire solo sotto il controllo del personale preposto.

c) Eventi distruttivi naturali, artificiali, dolosi, accidentali

Misura: danneggiamenti o distruzione di apparecchiature hardware o di archivi cartacei dovute a: sabotaggio, atti vandalici, problemi all'alimentazione di rete dovuti ad eventi eccezionali, incendi, calamità naturali; vista l'ubicazione dell'ufficio e la natura delle attività svolte, non si ritiene che tali rischi possano essere evitati del tutto in quanto rientrano nelle tipologie della forza maggiore e/o del caso fortuito. L'impianto di alimentazione delle macchine è adeguato alle più recenti normative di legge.

Sulle macchine e sugli impianti vengono svolti i necessari interventi di manutenzione. I locali sono dotati di estintori a polvere, regolarmente controllati, secondo le disposizioni di legge.

d) Errori umani nella gestione della sicurezza fisica

Misura: pur non potendo scongiurare in maniera assoluta il rischio di una falla nella sicurezza causata da un errore umano, il titolare, per minimizzarlo entro limiti accettabili, si affida al Manuale, che descrive in maniera chiara e precisa tutte le procedure da seguire, e agli interventi formativi, di cui si dirà al Capitolo 6, in cui gli incaricati potranno chiedere ulteriori spiegazioni ai docenti, in modo tale da sciogliere gli eventuali dubbi rimasti dopo lo studio del Manuale stesso.

Nella tabella riassuntiva sono indicati e descritti i rischi che incombono sui dati e sono riportate le relative misure d'azione per ridurre al minimo la possibilità che essi si verifichino

Tabella riassuntiva. Analisi dei rischi e misure tecniche ed organizzative.

Il Titolare ha proceduto ad una ricognizione dei rischi che potrebbero comportare una distruzione, sottrazione, perdita - anche accidentali -, trattamento illecito dei dati, accessi non autorizzati di origine dolosa, colposa o meramente fortuita, in grado di recare pregiudizio ai diritti degli interessati.

Le fonti di rischio sono state accorpate in:

- 1) Comportamenti degli operatori;
- 2) Eventi relativi agli strumenti;
- 3) Eventi relativi al contesto fisico-ambientale.

La gravità stimata di verifica del rischio va da ALTA (la possibilità che accada l'evento è notevole e le misure sono insufficienti e richiedono un intervento migliorativo urgente), MEDIA (la possibilità è minore e le misure adottate sono sufficienti a contrastare il rischio), a BASSA (il rischio è minimo e le misure possono ritenersi idonee), passando per livelli intermedi (MEDIO-ALTA e MEDIO-BASSA).

Evento	Impatto sulla sicurezza e sui diritti degli interessati		Rif. misure d'azione	Misure da adottare
	Descrizione	Gravità stimata		
Comportamento degli operatori	furto di credenziali di autenticazione	Sottrazione di password o nome utente	Media	Regolamento Privacy e Sicurezza; Nomina ad incaricato. Procedura data breach.
	carenza di consapevolezza, disattenzione, incuria	Superficialità degli incaricati; insufficiente formazione del personale autorizzato al trattamento, manchevole rispetto delle disposizioni di sicurezza stabilite dal titolare del trattamento e portate alla conoscenza di tutti gli autorizzati, manchevole custodia delle credenziali/chivi di accesso da parte del singolo operatore autorizzato	Media	Regolamento Privacy e Sicurezza; Nomina ad incaricato. Procedura data breach.
	comportamenti sleali o fraudolenti dei colleghi di lavoro o collaboratori	comunicazione e/o diffusione senza autorizzazione di dati dei quali l'operatore autorizzato è venuto a conoscenza in virtù dell'incarico assegnatogli, duplicazione e sottrazione di archivi cartacei e/o informatici, sottrazione di credenziali di	Bassa	Regolamento Privacy e Sicurezza; Nomina ad incaricato. Procedura data breach.

Eventi relativi agli strumenti	Comportamento inadeguato dei Responsabili del trattamento nominati dal Titolare	autenticazione o chiavi di accesso ad archivi cartacei	Media	Adeguate atto di nomina a responsabile	
	Accessi non autorizzati agli archivi elettronici per azione di virus informatici o di programmi suscettibili di recare danno (es. <i>Ransomware</i>)	Azione pregiudizievole per la sicurezza informatica	Bassa	Aggiornamenti dei software e del S.O. + Antivirus + Firewall del S.O. + Regolamento Privacy e Sicurezza; Backup. Procedura data breach. Accesso al server da remoto disabilitato.	
	Accessi non autorizzati agli archivi elettronici da parte di persone <i>in loco</i>	mancaanza di procedure di accesso mediante credenziali e di corretta custodia delle stesse	Bassa	aggiornamenti dei software e del S.O. + Antivirus + Firewall del S.O. + Regolamento Privacy e Sicurezza; Backup. Procedura data breach.	
	Spamming o altre tecniche di sabotaggio	Utilizzo non consentito dei dati che causa invio di e-mail indesiderate	Bassa	Antivirus + Firewall del S.O. + aggiornamenti dei software e del S.O.; Regolamento Privacy e Sicurezza; Nomina ad incaricato. Procedura data breach.	
	Malfunzionamento, indisponibilità o degrado degli strumenti	Indisponibilità dei dati	Bassa	controllo periodico sullo stato di funzionalità delle apparecchiature; backup; impianti a norma; Regolamento Privacy e Sicurezza; Procedura data breach.	
	Accessi esterni non autorizzati	Intrusione non autorizzata dall'esterno verso il sistema informatico	Bassa	Antivirus + aggiornamenti dei software e del S.O.; Regolamento Privacy e Sicurezza; Procedura data breach. Accesso al server da remoto disabilitato.	Controllo di account dormienti riferiti a utenti obsoleti e mai disattivati.
	Intercettazione di informazioni in rete	intercettazione di informazioni in rete dovute a scarsa attenzione verso la segretezza e integrità dei dati immessi in rete	Bassa	Antivirus + Firewall + aggiornamenti dei software e del S.O.; Regolamento Privacy e Sicurezza;	
	accessi non autorizzati a locali ad accesso ristretto	accessi non autorizzati a locali da parte di persone estranee	Bassa	Regolamento Privacy e Sicurezza + Bancone front-office.	

	Accessi non autorizzati agli archivi cartacei	manca di procedure di custodia e/o sorveglianza degli archivi, inadeguate misure di archiviazione dei dati	Bassa	Regolamento Privacy e Sicurezza; Chiusura locali; Procedura data breach.	
	asportazione e furto di strumenti contenenti dati	asportazione e furto di strumenti contenenti dati	Bassa	Locali presidiati; Chiusura locali; Regolamento Privacy e Sicurezza; BackUp dei dati; Procedura data breach.	
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Pericolo concreto per la integrità e segretezza dei dati; danneggiamento di archivi cartacei e/o di apparecchiature elettroniche	Medio-bassa	Impianti a norma; regolare manutenzione sugli stessi; Regolamento Privacy e Sicurezza; Procedura data breach.	
	errori umani nella gestione della sicurezza fisica	Comportamento distratto nella gestione dei documenti e degli strumenti di lavoro	Media	Nomina ad incaricato + Regolamento Privacy e Sicurezza; Procedura data breach.	
	guasto ai sistemi complementari (impianto elettrico, idraulico, ecc)	Inadeguatezza dell'impianto elettrico (corto circuito o carico di voltaggio eccessivo, ecc.), climatizzazione inadeguata, allagamenti da perdita delle tubature della farmacia.	Medio-bassa	Impianti a norma; manutenzione ordinaria; Procedura data breach.	

4. MISURE ADOTTATE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

4.1 Misure per i trattamenti informatici

- **L'individuazione per iscritto degli incaricati e dei responsabili del trattamento**
è contenuta nel "Fascicolo Privacy" dell'Ordine.
- **Credenziali di autenticazione**
Esiste una password utente di accesso a windows e quindi alla rete aziendale diversa per ogni utente.
Esempio: l'utente dell'ufficio A può accedere soltanto ai documenti che riguardano l'ufficio A.
E' vietato inserire una password uguale alla precedente o simile (6 caratteri su 8).
La password contiene caratteri di tre delle categorie seguenti:
 - Lettere maiuscole delle lingue europee (dalla A alla Z, con segni diacritici, caratteri greci e cirillici)
 - Lettere minuscole delle lingue europee (dalla a alla z, eszett, con segni diacritici, caratteri greci e cirillici)
 - Cifre in base 10 (da 0 a 9)
 - Caratteri non alfanumerici (caratteri speciali), ad esempio,!, \$, #, %
 - Qualsiasi carattere Unicode classificato come un carattere alfabetico ma che non è maiuscolo o minuscolo.Sono inclusi i caratteri Unicode delle lingue asiatiche.
Periodicità di sostituzione della/e password: 6 MESI.
- **Sistemi di autorizzazione**
Attualmente non è previsto alcun criterio specifico di autorizzazione, in quanto vi è un unico dipendente con pieno accesso ai dati personali trattati con strumenti elettronici.
- **Altre misure di sicurezza**

a) Software antivirus, aggiornamento del software, firewall

L'Ordine ha adottato le seguenti misure:

- Software antivirus, aggiornato automaticamente ad ogni accesso ad internet;
- Aggiornamento del sistema operativo, aggiornato automaticamente ad ogni accesso ad internet secondo le *patch* rese disponibili dal produttore;
- Aggiornamento del software gestionale;
- Verifica annuale delle vulnerabilità tecnologiche.

- **Gestione dei supporti rimovibili**

L'Ordine impartisce all'incaricato le istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati personali al fine di evitare accessi non autorizzati e trattamenti non consentiti.

Tali supporti, se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati solo se i dati in essi contenuti non sono intellegibili e tecnicamente in alcun modo ricostruibili.

- **Procedure di ripristino dei dati**

Per il salvataggio dei dati e il ripristino dell'accesso agli stessi in caso di danneggiamento degli strumenti elettronici o altra causa, si veda oltre.

4.2 Misure per i trattamenti senza l'ausilio di strumenti elettronici

I documenti vengono conservati in fascicoli e raccoglitori custoditi in armadi e cassettiere muniti di serratura di sicurezza e ubicati in locali ad accesso sorvegliato. Le stanze contenenti gli archivi cartacei, come per quelli informatici, sono costantemente sorvegliate dal personale di segreteria.

I documenti stessi vengono riposti in archivio al termine del trattamento. Nessun incaricato ha accesso all'archivio dopo l'orario di chiusura.

Con cadenza almeno annuale il titolare provvede a verificare ed eventualmente aggiornare l'ambito di trattamento consentito ai soggetti nominati incaricati del trattamento. Nel "Regolamento Privacy e Sicurezza" adottato dall'Ordine sono individuate,

altresi, le procedure per una corretta ed idonea custodia e conservazione dei documenti durante il tempo della loro consultazione.

5. RIPRISTINO DISPONIBILITÀ DEI DATI

Il back up avviene con modalità automatizzate a cadenza periodica giornaliera, mediante salvataggio su Unità NAS con più copie incrementali.

Le misure adottate sono idonee a garantire l'integrità dei dati e il loro ripristino in tempi certi a tutela dei diritti degli interessati.

La descrizione completa del backup è contenuta nella relazione tecnica allegata al presente documento.

VALUTAZIONE DEL RISCHIO

Principale obiettivo di un sistema di sicurezza è la salvaguardia dei dati trattati mediante un'adeguata formazione del personale e l'adozione di procedure di lavoro adeguate alla natura dei dati trattati.

In riferimento alla sicurezza dei dati personali gestiti in azienda, il Titolare del trattamento applica i seguenti principi:

- **LICEITÀ, CORRETTEZZA e TRASPARENZA:** i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **LIMITAZIONE DELLA FINALITÀ:** i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- **MINIMIZZAZIONE DEI DATI:** i dati raccolti sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **ESATTEZZA:** i dati sono esatti e, se necessario, aggiornati;
- **LIMITAZIONE DELLA CONSERVAZIONE:** 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;
- **INTEGRITÀ e RISERVATEZZA:** 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.

Tutte le tipologie di trattamento effettuate sono state descritte nella sezione “Trattamenti informatici” e “Trattamenti senza l’ausilio di strumenti informatici”.

Sulla base di esse, il Titolare del trattamento ha provveduto ad identificare i rischi che incombono sui dati nonché le procedure di lavoro adottate al fine di contenere i suddetti rischi.

Tenuto conto dei rischi che incombono sui dati personali, della natura dei dati personali trattati, delle modalità di trattamento e delle misure tecniche ed organizzative adottate, il rischio di violazione dei dati che include la possibile distruzione, perdita, modifica, divulgazione o accesso non autorizzati, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati si ritiene BASSO.

6. ELENCO DEGLI AGGIORNAMENTI

L'Ente dispone di strumenti hardware e software che garantiscono il rispetto degli obblighi di sicurezza del Regolamento UE 679/2016, e a tal fine si fa rilasciare dall'installatore esterno una relazione descrittiva dell'intervento effettuato.

Attraverso una politica di formazione e aggiornamento l'Ordine fa in modo che tutti gli incaricati sappiano utilizzare correttamente gli strumenti a loro disposizione mediante un comportamento attento e responsabile.

Alla data di emissione del presente Documento, il titolare ha riscontrato quanto segue:

- è stata effettuata l'analisi dei rischi che incombono sui dati, le misure tecniche ed organizzative adottate, presi in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione degli interessati, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici, sono da ritenersi adeguate alla loro prevenzione;
- è stato mappato il trattamento relativo alla segnalazione di illeciti ex D.Lgs. 24/2023;
- successivamente alla verifica dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione e manutenzione degli strumenti elettronici (sia per quanto riguarda i trattamenti con l'ausilio di strumenti elettronici sia per quelli cartacei), non si è reso necessario alcun aggiornamento;
- annotata l'attività di assistenza del Responsabile Avv. Bon nell'esercizio della sua attività consulenziale prestata in via continuativa e dell'Avv. Antonucci nell'esercizio della sua attività consulenziale prestata in via continuativa al Consiglio di Disciplina;
- è stata verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento rispetto a quanto indicato negli atti di nomina, non rendendosi necessario alcun aggiornamento;
- è stato aggiornato l'elenco dei Responsabili del trattamento-;
- è stato mappato il trattamento relativo alle comunicazioni istituzionali agli iscritti mediante la piattaforma Htemail (scheda 5), con designazione di Gruppo Semplitech srl quale responsabile del trattamento;

- è stata corretta la base giuridica della finalità di invio delle comunicazioni istituzionali nella scheda relativa ai dati degli iscritti, riconducendola all'art. 6, comma 1, lett. e, del Regolamento;
- sono stati adottati gli atti di autorizzazione per l'utilizzo della piattaforma Htemail;
- il trattamento è stato sottoposto a valutazione preliminare sulla necessità della valutazione d'impatto, con esito negativo.

Per quanto concerne invece la strumentazione informatica, sia hardware che software, salvi i dovuti e necessari aggiornamenti dei programmi, il titolare non ha riscontrato l'opportunità di sostituire le apparecchiature, garantendone tuttavia il corretto funzionamento attraverso una periodica manutenzione.