

*REGISTRO DELLE
ATTIVITA' DI
TRATTAMENTO DEI DATI

E

ANALISI DEI RISCHI - DPIA*

ai sensi dell'art. 30 e art. 35 del GDPR 2016/679

25 novembre 2021

(pagina lasciata intenzionalmente bianca)

1 – TITOLARE DEL TRATTAMENTO

1.1 – DATI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO

DATI ANAGRAFICI	
RAGIONE SOCIALE:	Consiglio Nazionale Ordine Assistenti Sociali in persona del presidente legale rappresentante <i>pro</i> <i>tempore</i> dott. Gianmario Gazzi
SEDE LEGALE:	via del Viminale, 43, Roma
TELEFONO:	064827889
E-MAIL:	info@cnoas.it dpo@cnoas.it
PEC:	cnoas@pec.it
SITO WEB:	www.cnoas.it
CODICE FISCALE:	97131960581
TIPO DI ATTIVITA':	Ente pubblico non economico
ORGANIGRAMMA PRIVACY	
RESPONSABILE PROTEZIONE DATI:	avv. Andrea Gandino – in subordine avv. Edoardo Chiavirano
N. INCARICATI DEL TRATTAMENTO:	7
N. AMMINISTRATORI DI SISTEMA ESTERNI:	6
N. RESPONSABILI ESTERNI PRIVACY:	5
N. ADDETTI MANUTENZIONE IT:	1

2 – DATI PERSONALI TRATTATI

2.1 - ELENCO DELLE ATTIVITA' DI TRATTAMENTO ESERCITATE DAL TITOLARE

ELENCO DELLE ATTIVITA' DI TRATTAMENTO ESERCITATE DAL TITOLARE	
1)	Gestione Albo Unico Ordine Assistenti Sociali e Formazione Continua
2)	Gestione procedimenti disciplinari di II° grado tramite Consiglio Nazionale di Disciplina (CND)
3)	Gestione dei dipendenti: buste paghe, formazione sicurezza sul lavoro, formazione in genere
4)	Gestione fornitori: Fondazione Nazionale, consulenza fiscale, software house, manutentori, RSPP, assicurazioni, ecc.
5)	Comunicazione di dati degli iscritti ai tribunali (quando previsto da legge), agli enti di formazione esterni che collaborano con il CNOAS per Formazione Continua, a persone fisiche o giuridiche o autorità pubbliche, ecc. che ne facciano lecitamente richiesta (se la comunicazione è prevista da norma o regolamento)
6)	(Consiglio) Ricorsi elettorali / Ricorsi iscrizione e cancellazione iscritti

2.2 - ELENCO DEI DATI PERSONALI COMUNI TRATTATI

DATI PERSONALI COMUNI ISCRITTI
Dati anagrafici, indirizzo (residenza, domicilio) recapito telefonico, email, indirizzo PEC, domicilio lavorativo, numero di iscrizione, formazione pregressa, crediti formativi, pagamento quote
DATI PERSONALI COMUNI DIPENDENTI
Dati anagrafici, indirizzo, recapito telefonico, email, coordinate bancarie, malattie, certificati medici, buste paga, nucleo familiare (inquadramento fiscale, detrazioni, etc.)
DATI PERSONALI COMUNI FORNITORI
Dati aziendali, indirizzo aziendale, recapiti telefonici aziendali (anche personali se il fornitore è un libero professionista)
DATI PERSONALI COMUNI TERZI
Per il Consiglio Nazionale di Disciplina, è possibile trattare dati comuni di ogni tipo delle persone coinvolte in qualsiasi modo nel procedimento disciplinare di II° grado Comunicazione dati iscritti a assicurazione Reale Mutua nei casi previsti (tirocini formativi presso il Consiglio per Polizze infortuni ed RC)

2.3 - ELENCO DEI DATI PERSONALI PARTICOLARI TRATTATI

DATI PERSONALI PARTICOLARI ISCRITTI
Per il CND, è possibile trattare dati particolari di ogni tipo degli assistenti sociali coinvolti in un procedimento disciplinare di II° grado (trattamento eccezionale, ma non escludibile)
DATI PERSONALI PARTICOLARI DIPENDENTI
Buste paga: Dati finanziari, possibilità di altri tipi di dati particolari (pignoramenti, quote sindacali, finanziamenti, malattie – certificati medici, nucleo familiare e detrazioni, ecc.)
DATI PERSONALI PARTICOLARI FORNITORI
n.a.
DATI PERSONALI PARTICOLARI TERZI
Per il Consiglio Nazionale di Disciplina è possibile trattare dati particolari di ogni tipo delle persone coinvolte in qualsiasi modo nel procedimento disciplinare di II° grado

2.4 - ELENCO DEI DATI PERSONALI GIUDIZIARI TRATTATI

DATI PERSONALI GIUDIZIARI ISCRITTI
Per il Consiglio Nazionale di Disciplina è possibile trattare dati particolari giudiziari di ogni tipo degli assistenti sociali coinvolti in un procedimento disciplinare di II° grado (evento eccezionale, ma non escludibile)
DATI PERSONALI GIUDIZIARI DIPENDENTI
Casellario giudiziale e anagrafe delle sanzioni amministrative dipendenti da reato in fase di verifica requisiti in fase di assunzione
DATI PERSONALI GIUDIZIARI FORNITORI
Casellario giudiziale e anagrafe delle sanzioni amministrative dipendenti da reato in fase di verifica requisiti in gare d'appalto
DATI PERSONALI GIUDIZIARI TERZI
Per il Consiglio Nazionale di Disciplina è possibile trattare dati particolari giudiziari delle persone coinvolte in qualsiasi modo nel procedimento disciplinare di II° grado

3 – SISTEMA ARCHIVISTICO DEL TITOLARE

3.1 – SISTEMA DI ARCHIVIAZIONE CORRENTE

ARCHIVIO DI DEPOSITO				N.	1	
LOCALIZZAZIONE ARCHIVIO		Sala riunioni 2° piano / 3° piano				
TIPO DI ARCHIVIO						
	Locale Dedicato Chiuso a Chiave	X	Armadio Chiuso a Chiave			
	Schedario Chiuso a Chiave		Cassettiera Chiusa a Chiave			
ELENCO DOCUMENTI CARTACEI PRESENTI IN ARCHIVIO						
Contabilità; Buste paga; Fascicoli Consiglio Nazionale di Disciplina; Formazione continua: crediti formativi; controlli: sanzioni amministrative, casellario giudiziale, Certificazioni uniche, fascicoli del personale (in stanza del Direttore)						
CATEGORIE DI INTERESSATI	MODALITA' DI ARCHIVIAZIONE			DATI PERSONALI		
	Cartacea	Elettronica	Sostitutiva	Comuni	Particolari	Giudiziari
ASSISTENTI SOCIALI	X	X	X	X	X	X
FORNITORI	X	X	X	X		
DIPENDENTI	X	X	X	X	X	
TERZI	X	X	X	X	X	X

Nel breve periodo l'archiviazione cartacea sarà completamente sostituita da quella elettronica e sostitutiva.

4 – SISTEMA INFORMATICO DEL TITOLARE

4.1 – DESCRIZIONE DELL'ARCHITETTURA DI RETE

N.	TIPOLOGIA	DESCRIZIONE
1	SERVER	HP con Domain Controller abilitato
5	CLIENT	HP, nome utente e password su ogni PC
2	PERIFERICHE	Stampanti
4	SOFTWARE APPLICATIVI	Albo Unico (Area Riservata), Formazione Continua, Protocollo, Cogeswintop (contabilità), Procedis (Procedimenti disciplinari), Cisco Webex (videoconferenze)
2	APPARATI DI RETE	Modem e Wi-Fi
2	APPARATI DI SICUREZZA	Antivirus Seqrite - Firewall
1	APPARATI DI STORAGE	NAS con 4 dischi
	DATA BASE / BANCHE DATI	n.a.
	ALTRO	UPS

4.2 – DESCRIZIONE DEL SISTEMA INFORMATIVO DEL TITOLARE

SITI WEB	
DOMINIO:	cnoas.org
HOSTING PROVIDER:	Microsis srl
TIPO SITO WEB:	Descrittivo

POSTA ELETTRONICA	
DOMINI:	@cnoas.it
SERVICE PROVIDER:	Hochfeiler srl

SOFTWARE APPLICATIVI	
APPLICATIVO:	Albo Unico, Formazione Continua
PRODUTTORE:	Hochfeiler srl
TIPO APPLICATIVO:	Gestione Albo Unico, Formazione Continua

SOFTWARE APPLICATIVI	
APPLICATIVO:	Cogeswintop
PRODUTTORE:	Visura S.p.A – ISI Sviluppo Informatico srl
TIPO APPLICATIVO:	Gestione contabilità

SOFTWARE APPLICATIVI	
APPLICATIVO:	Procedis
PRODUTTORE:	Microsis srl
TIPO APPLICATIVO:	Gestione procedimenti disciplinari

SOFTWARE APPLICATIVI	
APPLICATIVO:	Cisco Webex
PRODUTTORE:	Cisco System Inc.
TIPO APPLICATIVO:	Gestione delle riunioni in videoconferenza

SOFTWARE APPLICATIVI	
APPLICATIVO:	El Time
PRODUTTORE:	Eltime Srl - Solari Udine - LaserLine
TIPO APPLICATIVO:	Gestione delle presenze

5 – SISTEMA ORGANIZZATIVO PRIVACY

5.1 – RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO-RDP)

DATI ANAGRAFICI		DPO Esterno	2
NOME E COGNOME:	avv. Andrea Gandino – in subordine avv. Edoardo Chiavirano		
LUOGO E DATA DI NASCITA:	Torino, 16/06/1978 Torino, 27/01/1986		
RESIDENZA:	Torino, Corso Galileo Ferraris 80 (10129); Torino, Corso Duca degli Abruzzi 80 (10129) Domicilio professionale (entrambi): Torino, Corso Duca degli Abruzzi 4 (10128)		
CODICE FISCALE:	GNDNDR78H16L219M CHVDRD86A27L219P		
COMPITI PRIVACY ASSEGNATI			
<p>Consulenza sul sistema di protezione dei dati e sui tipi di trattamenti dati effettuati dal titolare del trattamento, consulenza per i dipendenti che eseguono trattamenti, consulenza per la redazione del registro dei trattamenti e valutazione d'impatto, punto di contatto con il Garante della Privacy, valutazione del sistema informatico secondo il GDPR e la normativa nazionale.</p> <p>Adeguamento al Regolamento 679/2016 UE, assunzione dell'incarico di DPO, garantendo competenze specialistiche di carattere giuridico, amministrativo ed informatico, nonché relative ai trattamenti in concreto posti in essere dal titolare.</p> <p>Revisione ed implementazione delle misure di sicurezza per la protezione dei dati personali, con controlli attivi altresì in ottica preventiva; consulenza generale in materia di privacy</p>			

5.2 - ELENCO DEGLI INCARICATI INTERNI DEL TRATTAMENTO

DATI ANAGRAFICI		Incaricato Interno N.		1	
NOME E COGNOME:		Sabrina Russo			
LUOGO E DATA DI NASCITA:		Vibo Valentia, 28.09.1973			
CODICE FISCALE:		RSSSRN73P68F537H			
RUOLO AZIENDALE:		Direttore			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI	X	X	X		X
FORNITORI	X	X	X		X
DIPENDENTI	X	X	X	X	X
TERZI	X	X	X	X	
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione	X	Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione		
X	Selezione e Estrazione	X	Conservazione		
X	Diffusione				
MANSIONI ASSEGNATE					
Gestione Albo, Formazione continua, potere decisionale su trattamento dati, amministrazione trasparente, adempimenti privacy, anticorruzione, certificati del casellario giudiziale e/o carichi pendenti in caso di assunzione di nuovi dipendenti tramite concorso pubblico e verifica dei requisiti per i fornitori partecipanti a gare d'appalto, documentazione relativa al personale dipendente compresa quella relativa allo stato di salute					

DATI ANAGRAFICI		Incaricato Interno N.	2		
NOME E COGNOME:		Filomena Ardone			
LUOGO E DATA DI NASCITA:		Brindisi, 4.10.1982			
CODICE FISCALE:		RDNFMN82R44B180P			
RUOLO AZIENDALE:		Impiegata			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI	X	X	X		X
FORNITORI	X	X	X		
DIPENDENTI					
TERZI					
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione		
X	Selezione e Estrazione	X	Conservazione		
	Diffusione				
MANSIONI ASSEGNATE					
Gestione Albo, ricorsi non disciplinari, attività di segreteria, adempimenti CROAS, archivio, centralino, programma informatico di archivio documentazione, protocollo informatico, supporto amministrazione trasparente e adempimenti privacy					

DATI ANAGRAFICI		Incaricato Interno N.	3		
NOME E COGNOME:		Agnese Storti			
LUOGO E DATA DI NASCITA:		Urbino, 4.03.1980			
CODICE FISCALE:		STRGNS80C44L500P			
RUOLO AZIENDALE:		Funzionario			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI	X	X	X		
FORNITORI	X	X	X		
DIPENDENTI	X	X	X	X	X
TERZI					
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione		
X	Selezione e Estrazione	X	Conservazione		
	Diffusione				
MANSIONI ASSEGNATE					
Gestione Albo, contabilità, gestione finanziari, fiscale e del personale, segreteria CND (atti da archiviare), backup, monitoraggi adempimenti privacy, fornitori (adempimenti contrattualistici e di contabilità), amministrazione trasparente, adempimenti privacy. Controllo green pass (non rilevante dal punto di vista privacy, non essendoci raccolta e conservazione di alcun dato personale, bensì mero <i>check</i> della validità del documento)					

DATI ANAGRAFICI		Incaricato Interno N.	4		
NOME E COGNOME:		Isabella Pinna			
LUOGO E DATA DI NASCITA:		Furtei, 15.10.1972			
CODICE FISCALE:		PNNSLL72R55D827Z			
RUOLO AZIENDALE:		Impiegata			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI	X	X	X		X
FORNITORI	X	X	X		
DIPENDENTI					
TERZI					
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione		
X	Selezione e Estrazione	X	Conservazione		
	Diffusione				
MANSIONI ASSEGNATE					
Gestione Albo e formazione continua, archivio, economato, protocollo informatico, supporto tenuta e aggiornamento inventario					

DATI ANAGRAFICI		Incaricato Interno N.	5
NOME E COGNOME:		Maria Cristina Dell'Anna	
LUOGO E DATA DI NASCITA:		Soleto (LE), 24.09.1963	
CODICE FISCALE:		DLLMCR63P64I800Q	
RUOLO AZIENDALE:		Presidente Consiglio Nazionale di Disciplina	
AMBITO DEL TRATTAMENTO AUTORIZZATO			
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI
	Elettronico	Cartaceo	Comuni Particolari Giudiziari
ISCRITTI	X	X	X X X
FORNITORI			
DIPENDENTI			
TERZI	X	X	X X X
OPERAZIONI DI TRATTAMENTO CONSENTITE			
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione (in parte, per CND)
X	Selezione e Estrazione	X	Conservazione
	Diffusione		
MANSIONI ASSEGNATE			
Presidente del Consiglio Nazionale di Disciplina dal 14.05.2021: procedimenti disciplinari a carico degli iscritti. Trattamento dati ricorsi e giudiziari.			

DATI ANAGRAFICI		Incaricato Interno N.	6		
NOME E COGNOME:		Giuseppa Ferraro			
LUOGO E DATA DI NASCITA:		Misterbianco (CT), 31.07.1966			
CODICE FISCALE:		FRRGPP66L71F250G			
RUOLO AZIENDALE:		Vicepresidente Consiglio Nazionale di Disciplina			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI	X	X	X	X	X
FORNITORI					
DIPENDENTI					
TERZI	X	X	X	X	X
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione (in parte, per CND)		
X	Selezione e Estrazione	X	Conservazione		
	Diffusione				
MANSIONI ASSEGNATE					
Vicepresidente del Consiglio Nazionale di Disciplina dal 14.05.2021: procedimenti disciplinari a carico degli iscritti. Trattamento dati ricorsi e giudiziari.					

DATI ANAGRAFICI		Incaricato Interno N.	7		
NOME E COGNOME:		Gabriele Ronco			
LUOGO E DATA DI NASCITA:		Pinerolo (TO), 30.01.1981			
CODICE FISCALE:		RNCGR1.81A30G674J			
RUOLO AZIENDALE:		Segretario CND			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI	X	X	X	X	X
FORNITORI					
DIPENDENTI					
TERZI	X	X	X	X	X
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione (in parte, per CND)		
X	Selezione e Estrazione	X	Conservazione		
	Diffusione				
MANSIONI ASSEGNATE					
Segretario Consiglio Nazionale di Disciplina dal 14.05.2021: procedimenti disciplinari a carico degli iscritti. Trattamento dati ricorsi e giudiziari.					

5.3 - ELENCO DEGLI INCARICATI ESTERNI DEL TRATTAMENTO

n.a.

5.4 - ELENCO DEGLI AMMINISTRATORI INTERNI DEL SISTEMA

n.a.

5.5 - ELENCO DEGLI AMMINISTRATORI ESTERNI DEL SISTEMA (RESPONSABILI ESTERNI)

DATI ANAGRAFICI		A.d.S. Esterno N.	1
RAGIONE SOCIALE:		Hochfeiler srl	
SEDE:		Via Nerola, 20, Roma	
PARTITA IVA:		04092261009	
SISTEMI AMMINISTRATI			
SERVER:			
CLIENT:			
PERIFERICHE:			
SOFTWARE APPLICATIVI:		Albo Unico – Formazione Continua	
APPARATI DI RETE:			
APPARATI DI SICUREZZA:			
APPARATI STORAGE:		Archivio ottico / NAS	
DATA BASE / BANCHE DATI:			
ALTRO:		Posta elettronica / Protocollo	
AMBITO TRATTAMENTO CONSENTITO			
Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico conferito di amministratore di sistema. Backup dati software applicativi			

DATI ANAGRAFICI		A.d.S. Esterno N.	2
RAGIONE SOCIALE:	IT'S OK srls		
SEDE:	Via La Marmora, 8, Roma		
PARTITA IVA:	15141551000		
SISTEMI AMMINISTRATI			
SERVER:	X		
CLIENT:	X		
PERIFERICHE:	X		
SOFTWARE APPLICATIVI:			
APPARATI DI RETE:	X		
APPARATI DI SICUREZZA:	X		
APPARATI STORAGE:	X		
DATA BASE / BANCHE DATI:			
ALTRO:			
AMBITO TRATTAMENTO CONSENTITO			
Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico conferito di amministratore di sistema, in particolare su posta elettronica e posta elettronica certificata			

DATI ANAGRAFICI		A.d.S. Esterno N.	3
RAGIONE SOCIALE:		Point Two Points srls	
SEDE:		Via di Novella, 10, Roma	
PARTITA IVA:		13265201007	
SISTEMI AMMINISTRATI			
SERVER:			
CLIENT:		X	
PERIFERICHE:			
SOFTWARE APPLICATIVI:			
APPARATI DI RETE:			
APPARATI DI SICUREZZA:			
APPARATI STORAGE:			
DATA BASE / BANCHE DATI:			
ALTRO:		Posta elettronica	
AMBITO TRATTAMENTO CONSENTITO			
Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico relativo a posta elettronica			

DATI ANAGRAFICI		A.d.S. Esterno N.	4
RAGIONE SOCIALE:	Ardesia srl		
SEDE:	Via A. Giuriato, 48, Vicenza		
PARTITA IVA:	02634040246		
SISTEMI AMMINISTRATI			
SERVER:			
CLIENT:			
PERIFERICHE:			
SOFTWARE APPLICATIVI:			
APPARATI DI RETE:			
APPARATI DI SICUREZZA:			
APPARATI STORAGE:			
DATA BASE / BANCHE DATI:			
ALTRO:	Posta elettronica certificata / conservazione digitale pec		
AMBITO TRATTAMENTO CONSENTITO			
Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico relativo a posta elettronica certificata			

DATI ANAGRAFICI		A.d.S. Esterno N.	5
RAGIONE SOCIALE:	Microsis srl		
SEDE:	Via degli Olmetti, 8/A, Formello (Roma)		
PARTITA IVA:	06701631001		
SISTEMI AMMINISTRATI			
SERVER:			
CLIENT:			
PERIFERICHE:			
SOFTWARE APPLICATIVI:	Procedis (CND)		
APPARATI DI RETE:			
APPARATI DI SICUREZZA:			
APPARATI STORAGE:			
DATA BASE / BANCHE DATI:			
ALTRO:	Sito web		
AMBITO TRATTAMENTO CONSENTITO			
Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico conferito di amministratore di sistema. Backup dati Procedis (software procedimenti disciplinari)			

DATI ANAGRAFICI		A.d.S. Esterno N.	6
RAGIONE SOCIALE:	Eltime S.r.l.		
SEDE:	Via della Tenuta di Torrenova, 72 – 00133 Roma		
PARTITA IVA:	03717821007		
SISTEMI AMMINISTRATI			
SERVER:			
CLIENT:			
PERIFERICHE:			
SOFTWARE APPLICATIVI:	ElTime (presenze)		
APPARATI DI RETE:			
APPARATI DI SICUREZZA:			
APPARATI STORAGE:			
DATA BASE / BANCHE DATI:			
ALTRO:	software gestione presenze		
AMBITO TRATTAMENTO CONSENTITO			
<p>Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico conferito di amministratore di sistema, con specifico riferimento alla rilevazione della presenza dei dipendenti a fini retributivi e contributivi</p>			

5.6 - ELENCO DEGLI ADDETTI ALLA MANUTENZIONE DEL SISTEMA IT

DATI ANAGRAFICI		Addetto IT N.	1
RAGIONE SOCIALE:	Visura Spa		
SEDE LEGALE:	Lungotevere dei Mellini, 44, Roma		
CODICE FISCALE:			
PARTITA IVA:	05338771008		
INCARICO ASSEGNATO:	Manutenzione Cogeswintop		
SISTEMI MANUTENZIONATI			
SERVER:			
CLIENT:			
PERIFERICHE:			
SOFTWARE APPLICATIVI:	Contabilità Cogeswintop		
APPARATI DI RETE:			
APPARATI DI SICUREZZA:			
APPARATI STORAGE:			
DATA BASE / BANCHE DATI:			
ALTRO:			
AMBITO TRATTAMENTO CONSENTITO			
Svolgimento di operazioni tecniche e eventuale trattamento di dati personali strettamente necessario all'adempimento dell'incarico conferito di amministratore di sistema, in particolare in ambito di contabilità			

5.7 - ELENCO DEGLI ADDETTI AL BACK UP

DATI ANAGRAFICI		Addetto Back Up N.	1
NOME E COGNOME:	Agnese Storti		
LUOGO E DATA DI NASCITA:	Urbino, 4.03.1980		
CODICE FISCALE:	STRGNS80C44L500P		
INQUADRAMENTO CONTRATTUALE:	Funzionario		
PROCEDURA DI BACK UP ASSEGNATA			
SERVER DATI:	X		
CLIENT:	n.a.		
PERIFERICHE:	n.a.		
SOFTWARE APPLICATIVI:	n.a. (aggiornamenti costanti forniti dai produttori)		
APPARATI DI RETE:	n.a.		
APPARATI DI SICUREZZA:	n.a. (aggiornamenti costanti forniti dai produttori e nel corso della consulenza)		
APPARATI STORAGE:	n.a. (revisione continuativa del corretto funzionamento)		
DATA BASE / BANCHE DATI:	X		
ALTRO:	n.a.		
Back up automatici vengono effettuati giornalmente al fine di ridurre notevolmente il rischio di perdita dei dati personali conservati			

5.8 - ELENCO DEI RESPONSABILI ESTERNI DEL TRATTAMENTO

DATI ANAGRAFICI			Responsabile Esterno N.		1
RAGIONE SOCIALE:		Ferrari & Associati, Studio Legale e Commerciale			
SEDE LEGALE:		Viale Umberto Tupini, 103, Roma			
PARTITA IVA:		06380741006			
INCARICO ASSEGNATO:		Consulenza fiscale e del lavoro			
DURATA CONTRATTUALE:		Annuale			
AMBITO DEL TRATTAMENTO AUTORIZZATO					
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI		
	Elettronico	Cartaceo	Comuni	Particolari	Giudiziari
ISCRITTI					
FORNITORI	X	X	X		
DIPENDENTI	X	X	X	X	X
TERZI					
OPERAZIONI DI TRATTAMENTO CONSENTITE					
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione		
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione		
X	Selezione e Estrazione	X	Conservazione		
	Diffusione				
ATTIVITA' ESTERNALIZZATE					
Consulenza fiscale e buste paga dipendenti. Dati personali bancari e di assunzione, procedimenti giudiziari in essere (pignoramenti, cessioni del quinto, etc.), agevolazioni, detrazioni, nucleo familiare.					

DATI ANAGRAFICI		Responsabile Esterno N.	2
RAGIONE SOCIALE:	Napolitano Flavio		
SEDE LEGALE:	Via Torre di Spizzichino, 98, Roma		
CODICE FISCALE:	NPLFLV78E22H501A		
INCARICO ASSEGNATO:	RSPP		
DURATA CONTRATTUALE:	Annuale		
AMBITO DEL TRATTAMENTO AUTORIZZATO			
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI
	Elettronico	Cartaceo	Comuni Particolari Giudiziari
ISCRITTI			
FORNITORI			
DIPENDENTI	X	X	X X*
TERZI			
OPERAZIONI DI TRATTAMENTO CONSENTITE			
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione
X	Selezione e Estrazione	X	Conservazione
	Diffusione		
ATTIVITA' ESTERNALIZZATE			
Responsabile del Servizio di Prevenzione e Protezione – designato dal datore di lavoro. (*) Potrebbe altresì trattare dati personali particolari dei dipendenti (si pensi, in via esemplificativa, al dipendente facente parte delle categorie protette)			

DATI ANAGRAFICI		Responsabile Esterno N.	3
RAGIONE SOCIALE:	Criscuolo Fabio Piergiorgio		
SEDE LEGALE:	Via Cosseria, 2, Roma		
CODICE FISCALE:	CRSFPR70R16I754J		
INCARICO ASSEGNATO:	Consulenza legale e assistenza in giudizio		
DURATA CONTRATTUALE:	Annuale		
AMBITO DEL TRATTAMENTO AUTORIZZATO			
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI
	Elettronico	Cartaceo	Comuni Particolari Giudiziari
ISCRITTI	X	X	X X*
FORNITORI	X	X	X X* X*
DIPENDENTI	X	X	X X* X*
TERZI			
OPERAZIONI DI TRATTAMENTO CONSENTITE			
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione
X	Selezione e Estrazione	X	Conservazione
	Diffusione		
AMBITO DI TRATTAMENTO			
Consulenza legale ed assistenza in giudizio. (*) Trattamento dei dati solo in caso di avvio di procedimento legale			

DATI ANAGRAFICI		Responsabile Esterno N.	4
RAGIONE SOCIALE:	Fondazione Nazionale Assistenti Sociali		
SEDE LEGALE:	Via del Viminale, 43, Roma		
CODICE FISCALE:	13545141007		
INCARICO ASSEGNATO:	Contabilità e buste paghe		
DURATA CONTRATTUALE:	Annuale		
AMBITO DEL TRATTAMENTO AUTORIZZATO			
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI
	Elettronico	Cartaceo	Comuni Particolari Giudiziari
ISCRITTI			
FORNITORI	X	X	X
DIPENDENTI	X	X	X X X
TERZI			
OPERAZIONI DI TRATTAMENTO CONSENTITE			
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione
X	Selezione e Estrazione	X	Conservazione
	Diffusione		
ATTIVITA' ESTERNALIZZATE			
Contabilità gestita in collaborazione con lo Studio Ferrari & Associati, già Responsabile Esterno del Trattamento			

DATI ANAGRAFICI		Responsabile Esterno N.	5
RAGIONE SOCIALE:	Andrea Gandino		
SEDE LEGALE:	Corso Duca degli Abruzzi, 4, Torino (10128)		
CODICE FISCALE:	GNDNDR78H16L219M		
INCARICO ASSEGNATO:	Assistenza e consulenza per problematiche giuridiche afferenti la materia ordinistica e le disposizioni giuridiche rilevanti per la categoria		
DURATA CONTRATTUALE:	Annuale		
AMBITO DEL TRATTAMENTO AUTORIZZATO			
CATEGORIA DI INTERESSATI	MODALITA' DI TRATTAMENTO		DATI PERSONALI
	Elettronico	Cartaceo	Comuni Particolari Giudiziari
ISCRITTI			
FORNITORI	X	X	X
DIPENDENTI	X	X	X X X
TERZI			
OPERAZIONI DI TRATTAMENTO CONSENTITE			
X	Visualizzazione e Consultazione		Cancellazione, Blocco e Distruzione
X	Utilizzo e Comunicazione	X	Registrazione e Elaborazione
X	Selezione e Estrazione	X	Conservazione
	Diffusione		
ATTIVITA' ESTERNALIZZATE			
Assistenza e consulenza per problematiche giuridiche afferenti la materia ordinistica e le disposizioni giuridiche rilevanti per la categoria			

6 – ANALISI DEI RISCHI

6.1 – LEGENDA VALUTAZIONE RISCHI

6.1.1 – LEGENDA DEFINIZIONE EVENTI

ELENCO EVENTI	
CALAMITA' NATURALI	Perdita di Dati conseguente ad Allagamento
	Perdita di Dati conseguente ad Incendio
MINACCE INTENZIONALI	Accessi non consentiti e/o Furti
	Accessi non autorizzati e/o Trattamenti non Consentiti
	Furto e/o Manomissione di Dati su Supporti Cartacei
	Furto e/o Manomissione di Dati su Supporti Informatici
	Furto di Strumenti Elettronici
	Perdita di Dati dovuta a Virus o a Intrusione Informatica
MINACCE INVOLONTARIE	Blackout elettrico
	Anomalie e Guasti dell'Alimentazione e/o del Sistema Elettrico
	Anomalie e Guasti del Sistema di Condizionamento e Raffreddamento
	Malfunzionamenti Software
	Malfunzionamenti Hardware

6.1.2 – LEGENDA PARAMETRI DI VALUTAZIONE DEL RISCHIO

TERMINE	DESCRIZIONE	
EVENTO	Fatto o avvenimento preso in considerazione nell'analisi dei rischi	
PROBABILITA'	Probabilità che l'evento accada	
	1	Poco Probabile
	2	Probabile
	3	Molto Probabile
	4	Altamente Probabile
GRAVITA'	Livello di criticità dell'evento e/o non conformità di un comportamento ad una normativa aziendale	
	1	Molto Bassa
	2	Bassa
	3	Alta
	4	Molto Alta
RILEVANZA	Entità del potenziale danno in termini di perdita di immagine, irrogazione di sanzioni amministrative e penali	
	1	Molto Bassa
	2	Bassa
	3	Media
	4	Alta
CONSEGUENZE	Possibili Conseguenze per l'Interessato a seguito del Verificarsi dell'Evento	
	1	Nessuna Conseguenza Rilevante per i Dati Personali e per i diritti e libertà dell'Interessato
	2	Distruzione o Perdita, anche Accidentale, di Dati Personali in genere
	3	Diffusione, modifica, accesso non autorizzato a Dati Personali comuni
	4	Diffusione, modifica, accesso non autorizzato a Dati Particolari o Giudiziari
CONTROMISURE	Contromisure Adottate per Diminuire il Rischio del Verificarsi dell'Evento	
	4	Adozione di Ottimali Misure di Sicurezza
	3	Adozione di Adeguate Misure di Sicurezza
	2	Adozione di Minime Misure di sicurezza
	1	Non sono state Adottate di Misure di Sicurezza idonee

6.1.3 – LEGENDA RISULTATI DI VALUTAZIONE DEL RISCHIO

TABELLA DI VALUTAZIONE DEL RISCHIO			
Rischi per i diritti e le libertà delle persone fisiche = (Probabilità x Gravità x Rilevanza x Conseguenze)/Contromisure			
RISCHIO	0 - 16	Molto Basso	Sono state correttamente definite ed implementate idonee misure di sicurezza ed il rischio residuo è stato definito accettabile dal Titolare del trattamento
	17 – 23	Basso	Sono state correttamente definite ed implementate preventive misure di sicurezza per ridurre il rischio, ma si potrebbe aumentare il livello di sicurezza per portare il rischio a livello Molto Basso. Il rischio residuo è stato comunque definito accettabile dal Titolare.
	24 – 63	Medio	Sono state correttamente definite e implementate alcune preventive misure di sicurezza per ridurre il rischio, ma il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza adottate non configurano un livello di protezione ancora del tutto ottimale. Il trattamento è consentito, ma è necessario implementare tutte le idonee misure di sicurezza nel breve tempo per portare il rischio a un livello almeno Basso.
	64 – 127	Alto	Sono state definite le misure minime di sicurezza, ma parte di esse sono ancora in fase di implementazione o non sono state correttamente implementate ed il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza adottate non configurano un livello accettabile di protezione. È necessario implementare tutte le idonee misure di sicurezza prima di procedere al trattamento.
	128 - 256	Molto Alto	Il titolare del Trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile, quindi i rischi residui restano elevati. È necessario consultare l'autorità di controllo prima di procedere all'attività di trattamento.

6.2 – ANALISI DEI RISCHI

6.2.1 – ELENCO ATTIVITA' ANALIZZATE

- Gestione Albo Unico e Formazione Continua attraverso piattaforma (6.2.2)
- Gestione procedimenti disciplinari attraverso piattaforma Procedis (6.2.3)
- Gestione dei dipendenti e dei fornitori (6.2.4)

6.2.2 – GESTIONE ALBO UNICO E FORMAZIONE CONTINUA

DESCRIZIONE	
PERSONALE AUTORIZZATO	Impiegati e funzionari del Consiglio Nazionale Ordine Assistenti Sociali, Direttore del Consiglio Nazionale Ordine Assistenti Sociali
RESPONSABILI ESTERNI COINVOLTI	Ditta Hochfeiler srl in qualità di amministratore di sistema
DESCRIZIONE DEL TRATTAMENTO	Utilizzo del software per inserimento iscritti in Albo Unico nazionale dell'Ordine degli assistenti sociali e della formazione effettuata dagli iscritti. Il software viene co-utilizzato anche dai componenti dei Consigli Regionali (<i>Autonomi Titolari del Trattamento</i>) per ottemperare all'obbligo di comunicazione dei dati degli iscritti di ciascun Ordine e della formazione continua. Il CNOAS si occupa della pubblicazione dei soli dati pertinenti nel sito istituzionale, nel pieno rispetto del principio di minimizzazione (ottemperanza alla formazione)
FINALITA' DEL TRATTAMENTO	Il trattamento viene effettuato per la tenuta dell'Albo e della formazione continua di ciascun iscritto
BASE GIURIDICA PER IL TRATTAMENTO DATI	Legge 84/1993 – Decreto 615/1994 – DPR 169/2005 – Codice deontologico Ordine Assistenti Sociali (obbligo legale, art. 6, lett. c, GDPR)
TIPI DI DATI TRATTATI	Dati comuni anagrafici e di contatto: nome, cognome, codice fiscale, data e luogo di nascita, consiglio di appartenenza, sezione e numero iscrizione (Dati pubblicati su sito istituzionale) Numero di telefono, indirizzo, posta elettronica, PEC, dati del luogo di lavoro in genere, curriculum, crediti formativi, formazione effettuata (Dati inseriti nella piattaforma ma non pubblicati) Pagamento quote, procedimenti disciplinari
CATEGORIE DI INTERESSATI	Isritti all'Albo Unico dell'Ordine degli Assistenti sociali
CATEGORIE DI DESTINATARI	I dati pubblicati sono accessibili a chiunque. I dati non pubblicati possono essere comunicati solo a soggetti pubblici e privati che ne facciano motivata e giustificata richiesta, previa idonea valutazione
INFORMATIVA	Viene resa un'informativa agli iscritti in fase di iscrizione direttamente dell'Ordine regionale di appartenenza (trattasi di trattamento congiunto CNOAS / CROAS)
PROFILAZIONE	No (ogni eventuale studio <i>statistico</i> non è riconducibile al singolo iscritto)

CONSENSO	No
MINORI	No
FREQUENZA TRATTAMENTO	In fase di revisione dei dati (ogni 2 anni), oppure quando necessario per lo svolgimento dell'attività dell'Ordine (quotidiana revisione ed aggiornamento da parte del CNOAS e CROAS, nonché dai singoli iscritti mediante le proprie credenziali personali)
TERMINI DI CANCELLAZIONE	10 anni dalla richiesta di cancellazione dall'albo (i dati pubblicati nel sito vengono immediatamente cancellati dalla consultazione pubblica in caso di cancellazione dell'iscritto dall'Albo)
TRASFERIMENTO DATI PAESI TERZI	No
MODALITA' DI ELABORAZIONE DATI	Cartacea / Elettronica
SOFTWARE UTILIZZATI	Albo Unico – Formazione Continua
TIPOLOGIA E FREQUENZA DI BACKUP	L'amministratore di sistema garantisce il salvataggio dei dati 6 volte al giorno su server gemello di backup
MISURE DI SICUREZZA TECNICHE ADOTTATE	<p>Relativi a amministratore di sistema:</p> <p>Server dedicati nella web farm di Aruba spa nella sede di Arezzo, in armadio dedicato ad uso esclusivo</p> <p>Server protetti da router CISCO con prevenzione attacchi DDOS</p> <p>Firewall</p> <p>Crittografia campi con algoritmo proprietario di Hochfeiler</p> <p>Relativi ai sistemi informatici CNOAS:</p> <p>Antivirus Seqrite, Server con Domain Controller</p>
MISURE DI SICUREZZA ORGANIZZATIVE ADOTTATE	<p>Credenziali e password associata ad ogni utente Iscritto, con cambio password semestrale.</p> <p>Nomine scritte Autorizzati ed Incaricati al trattamento, oltre a puntuale formazione del personale</p> <p>Nomina scritta Amministratore di sistema</p>

RISPETTO DEI PRINCIPI FONDAMENTALI DEL GDPR	
LICEITA'	Il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento
FINALITA'	Il trattamento viene effettuato per la tenuta dell'Albo e della formazione continua di ciascun iscritto, Legge 84/1993 – Decreto 615/1994 – DPR 169/2005 – Codice deontologico Ordine Assistenti Sociali
PROPORZIONALITA'	I dati vengono trattati solo per il raggiungimento della finalità prefissata
NECESSITA' E PERTINENZA	I dati trattati sono adeguati, pertinenti e limitati a quelli necessari al raggiungimento della finalità per cui sono stati raccolti, nel pieno rispetto della minimizzazione dei dati
TRASPARENZA	Gli Interessati sono informati sulle modalità di trattamento al momento della raccolta dei dati, mediante informativa aggiornata al GDPR. L'informativa viene pubblicata anche sul sito internet istituzionale, oltre ad essere consegnata da CNOAS o CROAS (trattamento congiunto)
ESATTEZZA	Si garantisce l'esattezza dei dati (possibilità di inserimento degli stessi direttamente da parte dell'Interessato) e si garantisce il diritto alla rettifica tempestiva o cancellazione dei dati che non dovessero risultare esatti
CONSERVAZIONE	Come da informativa, i dati verranno conservati negli archivi cartacei ed elettronici per 10 anni dalla richiesta di cancellazione dall'Albo, mentre verranno immediatamente cancellati i dati pubblicati sulla piattaforma del sito istituzionale
INTEGRITA' E RISERVATEZZA	Si garantisce integrità e riservatezza dei dati mediante formazione e nomina del personale Autorizzato, con riferimenti agli obblighi di segreto professionale e ai compiti per cui sono o non sono autorizzati, utilizzo di tecniche crittografiche del programma gestionale, protezione dei sistemi informatici dell'Ordine
CORRETTEZZA	Gli Interessati sono preventivamente informati sulle modalità di trattamento ed eventuali trattamenti diversi rispetto alle finalità dichiarate verranno comunicati tempestivamente all'Interessato. Dove previsto verrà chiesto il consenso al Trattamento (ad esempio pubblicità dell'Ordine per via telematica)
RESPONSABILITA'	Il titolare del trattamento mette in atto le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR, tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento e dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli Interessati (<i>accountability</i>)

RISPETTO DEI DIRITTI DELL'INTERESSATO	
TRASPARENZA	All'Interessato viene fornita l'informativa sulle modalità di trattamento dei dati, preventivamente, in forma concisa, trasparente, intelligibile, utilizzando un linguaggio semplice e chiaro (al momento dell'iscrizione presso il CROAS, comunque disponibile su sito istituzionale)
RISCONTRO	Il diritto di riscontro viene garantito all'Interessato, il quale può richiedere le informazioni alla segreteria dell'Ordine
INFORMATIVA	Viene consegnata l'Informativa dagli Ordini regionali in fase di raccolta dati ed è disponibile l'informativa anche sul sito istituzionale
ACCESSO	Il diritto di riscontro viene garantito all'Interessato, il quale può richiedere le informazioni alla segreteria dell'Ordine
RETTIFICA	L'Interessato può rettificare i dati che lo riguardano autonomamente dal sito inserendo le proprie credenziali di accesso oppure proponendo istanza alla segreteria dell'Ordine
CANCELLAZIONE	Il diritto alla cancellazione è limitato. L'Ordine ha necessità di conservare i dati per 10 anni dopo l'iscrizione per poter assolvere ad eventuali richieste di procedimento disciplinare per i 10 anni successivi alla data di disiscrizione dall'Albo. Vengono immediatamente eliminati i dati oggetto di pubblicazione all'Albo pubblico qualora l'interessato provveda alla disiscrizione
LIMITAZIONE DEL TRATTAMENTO	Verrà rispettato il diritto alla limitazione del trattamento quando l'interessato contesta l'esattezza dei propri dati (fino ad accertamento), in caso di presunto trattamento illecito, in caso di opposizione al trattamento per motivi legittimi (in attesa della verifica dei motivi legittimi)
PORTABILITA'	n.a.
COMUNICAZIONE	Il titolare comunicherà a tutti i destinatari ai quali sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate, salvo che ciò si rilevi impossibile o implichi uno sforzo sproporzionato
OPPOSIZIONE	Non applicabile, se l'Interessato si oppone al trattamento non può iscriversi all'Albo Unico

– RISCHIO RELATIVO AL COMPORTAMENTO DEGLI OPERATORI

EVENTI RELATIVI AL COMPORTAMENTO DEGLI OPERATORI						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Sottrazione di Credenziali di Autenticazione	1	4	3	3	4	9
Cessione Volontaria di Credenziali di Autenticazione	1	4	3	3	4	9
Accessi non Autorizzati e/o Trattamenti non Consentiti	1	3	3	3	4	<u>6,75</u>
Carenza di Consapevolezza, Disattenzione o Incuria	1	3	3	3	4	<u>6,75</u>
Comportamenti Sleali o Fraudolenti	1	3	3	3	4	<u>6,75</u>
Errore Materiale	1	3	3	3	4	<u>6,75</u>
Sottrazione di Documentazione Aziendale	1	2	3	3	4	<u>4,50</u>
Incuria nella Custodia dei Documenti Cartacei e/o Supporti Removibili	1	2	3	3	4	<u>4,50</u>

– RISCHIO RELATIVO AL SISTEMA INFORMATICO

EVENTI RELATIVI AL SISTEMA INFORMATICO						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Virus Informatici e/o Programmi Malevoli	1	2	2	3	4	<u>3</u>
Spamming o Tecniche di Sabotaggio	1	2	2	3	4	<u>3</u>
Accesso Abusivo al Sistema Informatico	1	2	2	3	4	<u>3</u>
Impedimento o Interruzione del Sistema Informatico	1	1	1	1	4	<u>≤1</u>
Intercettazione di Informazioni in Rete	1	2	2	2	4 (Dati solo su piattaforma)	<u>2</u>
Malfunzionamento, indisponibilità Software	1	2	2	2	4	<u>2</u>
Malfunzionamento, indisponibilità Hardware	1	1	1	1	4 (Server appena rinnovato)	<u>≤1</u>
Malfunzionamento, indisponibilità dei Sistemi di Backup	1	3	3	3	4	<u>6,75</u>
Malfunzionamento, indisponibilità Connettività Internet	1	1	1	1	4	<u>≤1</u>
Sovraccarico del Sistema Elaborativo e/o Trasmissivo	1	1	1	1	4	<u>≤1</u>

– RISCHIO RELATIVO AL CONTESTO AZIENDALE

EVENTI RELATIVI AL CONTESTO AZIENDALE						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Ingressi non autorizzati a locali/reparti ad accesso ristretto	1	1	1	1	4 (Dati su piattaforma online)	≤ 1
Sottrazione di Documenti cartacei e Strumenti contenenti Dati	1	1	1	1	4 (Dati su piattaforma online)	≤ 1
Eventi Distruttivi, Naturali o Artificiali (Terremoti...)	1	1	1	1	4 (Dati su piattaforma online)	≤ 1
Eventi Distruttivi Dolosi, Accidentali o Dovuti ad Incuria	1	1	1	1	4 (Dati su piattaforma online)	≤ 1
Guasto ai Sistemi Complementari (Impianto Elettrico, Climatizzazione, ecc.)	1	1	1	1	4 (Dati su piattaforma online)	≤ 1
Inagibilità dei Locali	1	1	1	1	4 (Dati su piattaforma online)	≤ 1
Errori Umani nella Gestione della Sicurezza Fisica	1	1	1	1	4 (Dati su piattaforma online)	≤ 1

– CONCLUSIONI (TITOLARE DEL TRATTAMENTO)

Dall'analisi dei rischi si evince che i principi del GDPR e i diritti degli Interessati sono rispettati e il livello di rischio è Molto Basso.

– CONCLUSIONI (DPO)

Si ritiene che la valutazione di impatto sia nel complesso positiva. Rimane infatti necessario implementare minimi aspetti di sicurezza nella tenuta degli archivi cartacei, seppur la maggior parte degli stessi siano posti in armadi chiusi con serratura, posizionati in stanze (a loro volta) chiuse con serratura. Si riscontra inoltre la mancanza di alcuni contratti tra il Titolare del Trattamento ed i Responsabili (esterni del trattamento), nonostante – ad ogni buon conto – dai contratti di servizio visionati è possibile evincere le mansioni delle parti, anche in termini di trattamento dei dati. Si consiglia di adempiere a tali due *gap* a stretto di giro.

6.2.3 – GESTIONE PROCEDIMENTI DISCIPLINARI

DESCRIZIONE	
PERSONALE AUTORIZZATO	Componenti Consiglio Nazionale di Disciplina
RESPONSABILI ESTERNI COINVOLTI	Ditta Microsis srl in qualità di amministratore di sistema (Procedis)
DESCRIZIONE DEL TRATTAMENTO	Utilizzo del software per inserimento degli atti e generalità degli assistenti sociali coinvolti nel procedimento disciplinare di II° grado. Il software viene utilizzato anche dai componenti dei Consigli Regionali (Autonomi Titolari del Trattamento) per l'inserimento di atti e generalità degli assistenti sociali coinvolti nel procedimento disciplinare di I° grado. Il software, seppur medesimo, ha funzionamenti separati per i procedimenti di diversi gradi
FINALITA' DEL TRATTAMENTO	Il trattamento viene effettuato per l'avvio e lo svolgimento dei procedimenti disciplinari
BASE GIURIDICA PER IL TRATTAMENTO DATI	DPR 7 agosto 2012, n. 137 – Regolamento istitutivo del Consiglio nazionale di disciplina – Regolamento per l'esercizio della funzione disciplinare nazionale
TIPI DI DATI TRATTATI	Vengono trattati i dati comuni anagrafici e di contatto dell'assistente sociale coinvolto nel procedimento disciplinare. I procedimenti disciplinari possono avviarsi anche da segnalazioni o istanze ad opera di qualsiasi persona fisica o giuridica che ne ravvisi la necessità. Queste segnalazioni potrebbero contenere qualsiasi tipo di informazioni, dati (anche sensibili – categorie particolari), descrizione di avvenimenti o fatti e potrebbero coinvolgere altre persone fisiche, con conseguente trattamento di dati comuni e particolari di Interessati anche vulnerabili e aventi carattere estremamente personale.
CATEGORIE DI INTERESSATI	Generalmente le persone fisiche coinvolte nel procedimento disciplinare, sia gli Iscritti sottoposti al procedimento, che i soggetti a cui si potrebbero riferire fatti e avvenimenti
CATEGORIE DI DESTINATARI	I dati trattati possono essere comunicati solo al tribunale competente (Tribunale Amministrativo), come da Regolamento. I dati relativi all'esito finale del procedimento (tutte le sanzioni previste dal Regolamento) vengono pubblicati nell'Albo Unico
INFORMATIVA	Viene resa un'informativa agli iscritti all'Albo in fase di iscrizione direttamente dell'Ordine regionale di appartenenza. Informativa generale pubblicata sul sito istituzionale per chi chiede l'avvio del procedimento disciplinare e per i soggetti coinvolti in altro modo
PROFILAZIONE	No
CONSENSO	No
MINORI	Sì (potrebbero essere coinvolti nel procedimento disciplinare)
FREQUENZA TRATTAMENTO	Per tutto il tempo necessario ad espletare la procedura del procedimento disciplinare

TERMINI DI CANCELLAZIONE	I dati degli atti verranno conservati per 10 anni dalla conclusione del procedimento
TRASFERIMENTO DATI PAESI TERZI	No
MODALITA' DI ELABORAZIONE DATI / CONSERVAZIONE	Cartacea / Elettronica
SOFTWARE UTILIZZATI	Procedis
TIPOLOGIA E FREQUENZA DI BACKUP	L'amministratore di sistema garantisce il salvataggio dei dati più volte al giorno su server e dispositivi archiviati in cassaforte
MISURE DI SICUREZZA TECNICHE ADOTTATE	<p>Relativi a amministratore di sistema: server di proprietà dedicati, protetti da firewall e router CISCO per la prevenzione di attacchi DDOS; applicativi anti Sql-injection; Server criptato</p> <p>Relativi ai sistemi informatici CNOAS: Antivirus Seqrite, Server con Domain Controller</p>
MISURE DI SICUREZZA ORGANIZZATIVE ADOTTATE	Credenziali e password associata ad ogni operatore, con cambio password trimestrale. Nomine scritte Autorizzati e Formazione del personale Nomina scritta Amministratore di sistema

RISPETTO DEI PRINCIPI FONDAMENTALI DEL GDPR	
LICEITA'	Il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento
FINALITA'	Il trattamento viene effettuato per l'avvio e lo svolgimento dei procedimenti disciplinari – DPR 7 agosto 2012, n. 137 – Regolamento istitutivo del Consiglio nazionale di disciplina – Regolamento per l'esercizio della funzione disciplinare nazionale
PROPORZIONALITA'	I dati vengono trattati solo per il raggiungimento della finalità prefissata
NECESSITA' E PERTINENZA	I dati trattati sono adeguati, pertinenti e limitati a quelli necessari al raggiungimento della finalità per cui sono stati raccolti. Dati relativi a terze persone coinvolte potrebbero essere trattati volontariamente (per necessità di equo procedimento disciplinare) o involontariamente (dati ricevuti da segnalazioni) trattati. Il trattamento dati è limitato ai soli operatori Autorizzati coinvolti nel procedimento disciplinare, che sono tenuti al segreto professionale. Rispetto del principio di minimizzazione.
TRASPARENZA	Gli Interessati sono informati sulle modalità di trattamento al momento della raccolta dei dati, mediante informativa aggiornata al GDPR. L'informativa viene pubblicata anche sul sito internet istituzionale
ESATTEZZA	Si garantisce l'esattezza dei dati (possibilità di inserimento degli stessi direttamente da parte dell'Interessato) e si garantisce il diritto alla rettifica tempestiva o cancellazione dei dati che non dovessero risultare esatti
CONSERVAZIONE	Come da informativa, i dati verranno conservati negli archivi cartacei ed elettronici per 10 anni dalla richiesta di cancellazione dall'Albo, mentre verranno immediatamente cancellati i dati diffusi mediante sito istituzionale (pubblicazione su Albo online)
INTEGRITA' E RISERVATEZZA	Si garantisce integrità e riservatezza dei dati mediante formazione e nomina del personale Autorizzato, con riferimenti agli obblighi di segreto professionale e ai compiti per cui sono o non sono autorizzati, utilizzo di tecniche di autenticazione del programma gestionale, protezione dei sistemi informatici dell'Ordine. I dati vengono da ultimo scambiati tra CNOAS e CROAS, entrambi soggetti già in possesso dei medesimi dati personali
CORRETTEZZA	Gli Interessati sono preventivamente informati sulle modalità di trattamento ed eventuali trattamenti diversi rispetto alle finalità dichiarate verranno comunicati tempestivamente all'Interessato
RESPONSABILITA'	Il titolare del trattamento mette in atto le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR, tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento e dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli Interessati

RISPETTO DEI DIRITTI DELL'INTERESSATO	
TRASPARENZA	All'Interessato viene fornita l'informativa sulle modalità di trattamento dei dati, preventivamente, in forma concisa, trasparente, intelligibile, utilizzando un linguaggio semplice e chiaro
RISCONTRO	Il diritto di riscontro viene garantito all'Interessato, il quale può richiedere le informazioni alla segreteria dell'Ordine (se dati relativi allo stato d'iscrizione) o al Presidente del CND (dati relativi al procedimento)
INFORMATIVA	Viene consegnata l'Informativa dagli Ordini regionali in fase di raccolta dati ed è disponibile l'informativa anche sul sito istituzionale
ACCESSO	Il diritto di riscontro viene garantito all'Interessato, il quale può richiedere le informazioni alla segreteria dell'Ordine (se dati relativi allo stato d'iscrizione) o al Presidente del CND / Segreteria (dati relativi al procedimento)
RETTIFICA	L'Interessato può rettificare i dati che lo riguardano autonomamente dal sito inserendo le proprie credenziali di accesso o facendo richiesta alla segreteria dell'Ordine (se dati relativi allo stato d'iscrizione) o al Presidente del CND (dati relativi al procedimento)
CANCELLAZIONE	Il diritto alla cancellazione è limitato. L'Ordine ha necessità di conservare i dati per 10 anni dopo l'iscrizione
LIMITAZIONE DEL TRATTAMENTO	Verrà rispettato il diritto alla limitazione del trattamento quando l'interessato contesta l'esattezza dei propri dati (fino ad accertamento), in caso di presunto trattamento illecito, in caso di opposizione al trattamento per motivi legittimi (in attesa della verifica dei motivi legittimi)
PORTABILITA'	n.a.
COMUNICAZIONE	Il titolare comunicherà a tutti i destinatari ai quali sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato
OPPOSIZIONE	Non applicabile, se l'Interessato si oppone al trattamento non può iscriversi all'Albo Unico

– RISCHIO RELATIVO AL COMPORTAMENTO DEGLI OPERATORI

EVENTI RELATIVI AL COMPORTAMENTO DEGLI OPERATORI						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Sottrazione di Credenziali di Autenticazione	1	4	4	4	4	<u>16</u>
Cessione Volontaria di Credenziali di Autenticazione	1	4	4	4	4	<u>16</u>
Accessi non Autorizzati e/o Trattamenti non Consentiti	1	4	4	4	4	<u>16</u>
Carenza di Consapevolezza, Disattenzione o Incuria	1	4	4	4	4	<u>16</u>
Comportamenti Sleali o Fraudolenti	1	4	4	4	4	<u>16</u>
Errore Materiale	1	4	4	4	4	<u>16</u>
Sottrazione di Documentazione Aziendale	1	4	4	4	4	<u>16</u>
Incuria nella Custodia dei Documenti Cartacei e/o Supporti Removibili	1	4	4	4	4	<u>16</u>

– RISCHIO RELATIVO AL SISTEMA INFORMATICO

EVENTI RELATIVI AL SISTEMA INFORMATICO						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Virus Informatici e/o Programmi Malevoli	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Spamming o Tecniche di Sabotaggio	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Accesso Abusivo al Sistema Informatico	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Impedimento o Interruzione del Sistema Informatico	1	1	1	1	4	<u>≤1</u>
Intercettazione di Informazioni in Rete	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Malfunzionamento, indisponibilità Software	1	2	2	2	4	<u>2</u>
Malfunzionamento, indisponibilità Hardware	1	1	1	1	4 (Server sostituito e rinnovato da ultimo)	<u>≤1</u>
Malfunzionamento, indisponibilità dei Sistemi di Backup	1	4	2	2	4	<u>4</u>
Malfunzionamento, indisponibilità Connettività Internet	1	1	1	1	4	<u>≤1</u>
Sovraccarico del Sistema Elaborativo e/o Trasmissivo	1	1	1	1	4	<u>≤1</u>

– RISCHIO RELATIVO AL CONTESTO AZIENDALE

EVENTI RELATIVI AL CONTESTO AZIENDALE						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Ingressi non autorizzati a locali/reparti ad accesso ristretto	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>
Sottrazione di Documenti cartacei e Strumenti contenenti Dati	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>
Eventi Distruttivi, Naturali o Artificiali (Terremoti...)	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>
Eventi Distruttivi Dolosi, Accidentali o Dovuti ad Incuria	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>
Guasto ai Sistemi Complementari (Impianto Elettrico, Climatizzazione, ecc.)	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>
Inagibilità dei Locali	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>
Errori Umani nella Gestione della Sicurezza Fisica	1	1	1	1	4 (Dati su piattaforma online)	<u>≤1</u>

– CONCLUSIONI (TITOLARE)

Dall'analisi dei rischi si evince che i principi del GDPR e i diritti degli Interessati sono rispettati e il livello di rischio è Basso.

- CONCLUSIONI (DPO)

Si ritiene che la valutazione di impatto sia nel complesso positiva. Rimane infatti necessario implementare minimi aspetti di sicurezza nella tenuta degli archivi cartacei, seppur la maggior parte degli stessi siano posti in armadi chiusi con serratura, posizionati in stanze (a loro volta) chiuse con serratura

6.2.4 – GESTIONE DIPENDENTI / FORNITORI

DESCRIZIONE	
PERSONALE AUTORIZZATO	Impiegati e funzionari + Direttore del Consiglio Nazionale Ordine Assistenti Sociali
RESPONSABILI ESTERNI COINVOLTI	Studio Ferrari & Associati, Avvocato Gandino, Visura Srl, Eltime Srl
DESCRIZIONE DEL TRATTAMENTO	Raccolta e trattamento dati personali per elaborazione buste paga (dati comuni, bancari, residenza e domicilio, nucleo familiare, detrazioni, pignoramenti e cessioni del quinto, etc)
FINALITA' TRATTAM.	Ex lege / contrattuale per elaborazione buste paga
BASE GIURIDICA PER IL TRATTAMENTO DATI	d.lgs. 165/01 / contratto individuale / CCNL applicabili
TIPI DI DATI TRATTATI	Nome, cognome, residenza e domicilio, composizione del nucleo familiare, posta elettronica e pec (se presente), dati bancari (IBAN), detrazioni, pignoramenti, cessione del quinto
CATEGORIE DI INTERESSATI	Dipendenti e fornitori
CATEGORIE DI DESTINATARI	Su richiesta degli interessati. Dati comuni pubblicati – se necessario – in Amministrazione trasparente su sito istituzionale
INFORMATIVA	Viene resa un'informativa in fase di sottoscrizione contrattuale con dipendenti e fornitori
PROFILAZIONE	No
CONSENSO	No – non necessario
MINORI	No
FREQUENZA TRATTAMENTO	Mensile / a richiesta

TERMINI DI CANCELLAZIONE	I dati degli atti verranno conservati per 10 anni dalla conclusione del contratto
TRASFERIMENTO DATI PAESI TERZI	No
MODALITA' DI ELABORAZIONE DATI	Cartacea / Elettronica
SOFTWARE UTILIZZATI	ElTime / Cogeswintop di Visura
TIPOLOGIA E FREQUENZA DI BACKUP	L'amministratore di sistema garantisce il salvataggio dei dati più volte al giorno su server e dispositivi archiviati in cassaforte
MISURE DI SICUREZZA TECNICHE ADOTTATE	<p>Relativi a amministratore di sistema: server di proprietà dedicati, protetti da firewall e router CISCO per la prevenzione attacchi DDOS; applicativi anti Sql-injection; Server criptato</p> <p>Relativi ai sistemi informatici CNOAS: Antivirus Seqrite, Server con Domain Controller</p>
MISURE DI SICUREZZA ORGANIZZATIVE ADOTTATE	<p>Credenziali e password associata ad ogni operatore, con cambio password trimestrale</p> <p>Nomine scritte Autorizzati e Formazione del personale</p> <p>Nomina scritta Amministratore di sistema</p>

RISPETTO DEI PRINCIPI FONDAMENTALI DEL GDPR	
LICEITA'	Il Trattamento è necessario per adempiere un obbligo contrattuale al quale è soggetto il Titolare del Trattamento
FINALITA'	Contrattuali (d.lgs. 50/2016 – d.lgs. 165/01 / contratti individuali / CCNL applicabili
PROPORZIONALITA'	I dati vengono trattati solo per il raggiungimento della finalità prefissata
NECESSITA' E PERTINENZA	(Minimizzazione) I dati trattati sono pertinenti e limitati a quelli necessari al raggiungimento delle finalità
TRASPARENZA	Gli Interessati sono informati sulle modalità di trattamento al momento della raccolta dei dati, mediante informativa aggiornata al GDPR. L'informativa viene pubblicata anche sul sito internet istituzionale, nonché consegnata al momento della sottoscrizione contrattuale ovvero, in sede di concorso pubblico finalizzato all'assunzione, in uno con il bando di concorso
ESATTEZZA	Si garantisce il diritto alla rettifica tempestiva o cancellazione dei dati che non dovessero risultare esatti
CONSERVAZIONE	Come da informativa, i dati verranno conservati negli archivi cartacei ed elettronici per 10 anni dalla conclusione contrattuale
INTEGRITA' E RISERVATEZZA	Si garantisce integrità e riservatezza dei dati mediante formazione e nomina del personale Autorizzato, con riferimenti agli obblighi di segreto professionale e ai compiti per cui sono o non sono autorizzati, utilizzo di tecniche crittografiche del programma gestionale, protezione dei sistemi informatici dell'Ordine
CORRETTEZZA	Gli Interessati sono preventivamente informati sulle modalità di trattamento ed eventuali trattamenti diversi rispetto alle finalità dichiarate verranno comunicati tempestivamente all'Interessato
RESPONSABILITA'	Il titolare del trattamento mette in atto le misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR, tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento e dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli Interessati (<i>accountability</i>)

RISPETTO DEI DIRITTI DELL'INTERESSATO	
TRASPARENZA	All'Interessato viene fornita l'informativa sulle modalità di trattamento dei dati, preventivamente, in forma concisa, trasparente, intelligibile, utilizzando un linguaggio semplice e chiaro
RISCONTRO	Il diritto di riscontro viene garantito all'Interessato, il quale può richiedere le informazioni alla segreteria dell'Ordine ovvero agli uffici Amministrazione del personale / fornitori
INFORMATIVA	Viene consegnata l'Informativa dal Consiglio in fase di raccolta dati ed è disponibile l'informativa anche sul sito istituzionale
ACCESSO	Il diritto di riscontro viene garantito all'Interessato, il quale può richiedere le informazioni alla segreteria dell'Ordine ovvero agli uffici Amministrazione del personale / fornitori
RETTIFICA	L'Interessato può rettificare i dati che lo riguardano mediante istanza e/o comunicazione da inviarsi alla Segreteria ovvero all'Ufficio Amministrazione personale / fornitori
CANCELLAZIONE	Il diritto alla cancellazione è limitato. L'Ordine ha necessità di conservare i dati per 10 anni dopo la conclusione del contratto
LIMITAZIONE DEL TRATTAMENTO	Verrà rispettato il diritto alla limitazione del trattamento quando l'interessato contesta l'esattezza dei propri dati (fino ad accertamento), in caso di presunto trattamento illecito, in caso di opposizione al trattamento per motivi legittimi (in attesa della verifica dei motivi legittimi)
PORTABILITA'	n.a.
COMUNICAZIONE	Il titolare comunicherà a tutti i destinatari ai quali sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato
OPPOSIZIONE	Non applicabile, se l'Interessato si oppone al trattamento non può avere rapporti con il Consiglio Nazionale

– RISCHIO RELATIVO AL COMPORTAMENTO DEGLI OPERATORI

EVENTI RELATIVI AL COMPORTAMENTO DEGLI OPERATORI						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Sottrazione di Credenziali di Autenticazione	1	4	4	4	4	<u>16</u>
Cessione Volontaria di Credenziali di Autenticazione	1	4	4	4	4	<u>16</u>
Accessi non Autorizzati e/o Trattamenti non Consentiti	1	4	4	4	4	<u>16</u>
Carenza di Consapevolezza, Disattenzione o Incuria	1	4	4	4	4	<u>16</u>
Comportamenti Sleali o Fraudolenti	1	4	4	4	4	<u>16</u>
Errore Materiale	1	4	4	4	4	<u>16</u>
Sottrazione di Documentazione Aziendale	1	4	4	4	4	<u>16</u>
Incuria nella Custodia dei Documenti Cartacei e/o Supporti Removibili	1	4	4	4	4	<u>16</u>

– RISCHIO RELATIVO AL SISTEMA INFORMATICO

EVENTI RELATIVI AL SISTEMA INFORMATICO						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Virus Informatici e/o Programmi Malevoli	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Spamming o Tecniche di Sabotaggio	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Accesso Abusivo al Sistema Informatico	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Impedimento o Interruzione del Sistema Informatico	1	1	1	1	4	<u>≤1</u>
Intercettazione di Informazioni in Rete	1	4	4	4 (Manca criptazione totale dei dati)	3	<u>21</u>
Malfunzionamento, indisponibilità Software	1	2	2	2	4	<u>2</u>
Malfunzionamento, indisponibilità Hardware	1	1	1	1	4 (Server da ultimo rinnovato)	<u>≤1</u>
Malfunzionamento, indisponibilità dei Sistemi di Backup	1	4	2	2	4	<u>4</u>
Malfunzionamento, indisponibilità Connettività Internet	1	1	1	1	4	<u>≤1</u>
Sovraccarico del Sistema Elaborativo e/o Trasmissivo	1	1	1	1	4	<u>≤1</u>

– RISCHIO RELATIVO AL CONTESTO AZIENDALE

EVENTI RELATIVI AL CONTESTO AZIENDALE						
EVENTO	IMPATTO SULLA SICUREZZA					
	Probabilità	Gravità	Rilevanza	Conseguenze	Contromisure	Rischio
Ingressi non autorizzati a locali/reparti ad accesso ristretto	1	1	1	1	4	<u>≤1</u>
Sottrazione di Documenti cartacei e Strumenti contenenti Dati	1	1	1	1	4	<u>≤1</u>
Eventi Distruttivi, Naturali o Artificiali (Terremoti...)	1	1	1	1	4	<u>≤1</u>
Eventi Distruttivi Dolosi, Accidentali o Dovuti ad Incuria	1	1	1	1	4	<u>≤1</u>
Guasto ai Sistemi Complementari (Impianto Elettrico, Climatizzazione, ecc.)	1	1	1	1	4	<u>≤1</u>
Inagibilità dei Locali	1	1	1	1	4	<u>≤1</u>
Errori Umani nella Gestione della Sicurezza Fisica	1	1	1	1	4	<u>≤1</u>

– CONCLUSIONI (TITOLARE)

Dall'analisi dei rischi si evince che i principi del GDPR e i diritti degli Interessati sono rispettati e il livello di rischio è Basso.

- CONCLUSIONI (DPO)

7 – MISURE DI SICUREZZA ADOTTATE

7.1 – DESCRIZIONE DEL SISTEMA DI SICUREZZA FISICA

7.1.1 – MISURE DI SICUREZZA CONTRO I RISCHI DI INCENDIO

CONTROMISURE - RISCHI DI INCENDIO	
Estintori	

7.1.2 – MISURE DI SICUREZZA CONTRO ACCESSI NON AUTORIZZATI

CONTROMISURE - RISCHI DI ACCESSO NON AUTORIZZATO			
X	Portineria	X	Portone Blindato
	Sistema d'Allarme	X	Controllo Accessi
	Videosorveglianza		Vigilanza
	Biometria		

MODALITA' DI ACCESSO AGLI ARCHIVI
Archivi chiusi a chiave in armadi in sala riunioni, locale presidiato durante l'attività lavorativa

7.1.3 – MISURE DI SICUREZZA CONTRO GUASTI E ANOMALIE TECNICI

CONTROMISURE - RISCHI DI GUASTI E ANOMALIE IMPIANTO ELETTRICO
Gruppo di continuità, controlli periodici messa a terra e impianto elettrico

CONTROMISURE - RISCHI DI GUASTI E ANOMALIE HARDWARE
Sostituzione preventivata del server, contratto di assistenza continua con amministratore di sistema IT'S OK srls, contattabile in caso di malfunzionamenti

7.2 – DESCRIZIONE DEL SISTEMA DI SICUREZZA LOGICA

ANTIVIRUS / ANTISPAM	
MARCA:	Seqrte con crittazione dati e antimalware
AMMINISTRATORE:	IT'S OK srls
MODALITA' DI AGGIORNAMENTO:	Automatico
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Semestrale

7.2 – DESCRIZIONE DEL SISTEMA DI AUTENTICAZIONE

SERVER	
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Ogni 3 mesi

CLIENT	
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Ogni 3 mesi

SOFTWARE APPLICATIVI	
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Ogni 3 mesi

APPARATI DI RETE	
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Ogni 6 mesi

POSTA ELETTRONICA	
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Ogni 3 mesi

STORAGE	
MODALITA' DI AUTENTICAZIONE:	Password
MODALITA' CAMBIO PASSWORD:	Ogni 3 mesi

7.3 – DESCRIZIONE DEL SISTEMA DI BACK UP

SISTEMA DI BACK UP UFFICIO CNOAS				Scheda N.	1
DESCRIZIONE BACK UP					
AUTOMATICO GIORNALIERO UFFICIO CNOAS					
X	Data Base	X	Applicativo (Cogeswintop)	X	Cartella/File
MODALITA' DI BACK UP					
	Tape		HD Esterno		CD/DVD
X	Nas RAID5 4 dischi		Cloud		
INCARICATO CONTROLLO AVVENUTO BACK UP			Agnese Storti		

7.4 – DESCRIZIONE DEL SISTEMA DI RIPRISTINO DEI DATI

SISTEMA DI RIPRISTINO DEI DATI E DISASTER RECOVERY
<p>Per ogni programma gestionale, ripristino totale dei dati contattando l'amministratore di sistema di riferimento del programma. Per i dati contenuti nel PC aziendali, ripristino dei dati da server (contattare amministratore di sistema hardware)</p>

7.5 – PROCEDURA DATA BREACH

PROCEDURA DATA BREACH
<ol style="list-style-type: none">1) Chiunque all'interno della struttura, nonché i fornitori in outsourcing (Responsabili) abbia notizia di una violazione dei dati personali, è tenuto a segnalarlo senza indugio al Titolare affinché prenda le necessarie misure2) Il Titolare o il suo delegato devono informare dell'avvenuta violazione il Responsabile della Protezione dei dati (DPO)3) Il titolare o il suo delegato devono valutare senza indugio la categoria di Interessati e il loro numero (anche approssimativo), la tipologia di dato violato, la tipologia di violazione, le misure di sicurezza applicate. Sulla base di tali informazioni, il Titolare deve compiere una valutazione circa i rischi per i diritti e le libertà degli Interessati.4) Nel caso in cui la valutazione rilevi un rischio per i diritti e le libertà delle persone fisiche, il Titolare o il suo delegato devono attuare tutte le misure opportune al fine di limitare gli effetti della violazione ed evitare conseguenze più gravi. A tal fine il Titolare o il suo delegato devono contattare i soggetti interni o esterni in grado di predisporre adeguate misure tecniche ed organizzative, a seconda della tipologia di violazione5) Nel caso in cui la valutazione rilevi un rischio per i diritti e le libertà delle persone fisiche, è necessario procedere alla notifica al Garante privacy, ai sensi dell'art. 33 del GDPR. La notifica deve essere trasmessa entro 72 ore dalla scoperta dell'evento. In caso di superamento del termine è necessario motivare il ritardo. La notifica e gli eventuali allegati devono essere trasmessi via pec all'indirizzo protocollo@pec.gpdp.it. Ogni notifica deve essere registrata con un numero di protocollo interno da riportare nell'apposito Registro delle violazioni6) Nel caso in cui la valutazione rilevi un pericolo elevato, la comunicazione agli Interessati è effettuata per iscritto (via posta ordinaria o via email) e deve contenere la descrizione dell'evento, il nome e i dati di contatto del DPO o di un altro punto di contatto presso cui ottenere più informazioni, le probabili conseguenze della violazione di dati personali, le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se possibile, per attenuare i possibili effetti negativi. Nel caso in cui la comunicazione venga inviata via email a più destinatari è necessario utilizzare le impostazioni che consentano di nascondere l'elenco completo dei destinatari al soggetto ricevente7) Ogni violazione di cui si abbia notizia, indipendentemente dalla gravità e dall'avvenuta notifica all'Autorità Garante, deve essere annotata nell'apposito "Registro delle violazioni" da parte del titolare o da un suo delegato.8) Dopo la violazione, devono essere approntati modelli organizzativi, procedure o misure di sicurezza in modo da evitare il successivo verificarsi della stessa violazione <p>Ad esempio, in caso di accesso illecito ai dati in formato elettronico, si consiglia di cambiare le password esistenti e di installare/aggiornare il firewall.</p> <p>In caso di accesso illecito ai dati in formato cartaceo, si consiglia di sostituire le serrature dei locali e/o degli armadi. È opportuno tenere traccia degli aggiornamenti e delle modifiche delle misure di sicurezza.</p>

8 – REGISTRO DEI TRATTAMENTI

REGISTRO DEI TRATTAMENTI						
Tipologia di trattamento	Finalità e basi legali del trattamento	Categorie di interessati	Categorie di dati personali	Categorie di destinatari	Termini ultimi di cancellazione previsti	Misure di sicurezza tecniche ed organizzative
Gestione Albo Unico e formazione continua	Il trattamento viene effettuato per la tenuta dell'Albo e della formazione continua di ciascun iscritto Legge 84/1993 – Decreto 615/1994 – DPR 169/2005 – Codice deontologico Ordine Assistenti Sociali	Iscritti all'Albo Unico	Dati comuni anagrafici e di contatto: nome, cognome, codice fiscale, data e luogo di nascita, Consiglio di appartenenza, sezione e numero iscrizione (Dati pubblicati su sito istituzionale) numero di telefono, indirizzo, domicilio, posta elettronica, PEC, dati del luogo di lavoro in genere, curriculum, crediti formativi, formazione effettuata (Dati inseriti nella piattaforma ma non pubblicati)	I dati pubblicati sono accessibili a chiunque. I dati non pubblicati possono essere comunicati solo a soggetti pubblici e privati che ne facciano motivata e giustificata richiesta, previa valutazione del Consiglio in termini di ostensibilità	10 anni dalla richiesta di cancellazione dall'albo (i dati pubblicati nel sito vengono immediatamente cancellati in caso di cancellazione dell'iscrizione dall'Albo)	Per CNOAS: Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati Dispositivi antincendio Gestione delle password degli utenti: sono modificate ogni 3 mesi, sono modificate al primo utilizzo, sono composte da almeno 8 caratteri alfanumerici, esistono diversi livelli di autorizzazione Le credenziali sono disattivate se inutilizzate per sei mesi È presente un gruppo di continuità e l'impianto elettrico è certificato e a norma Gli archivi dei dati cartacei sono chiusi a chiave Sono applicate procedure di <i>disaster recovery</i> che garantiscono il ripristino dell'accesso ai dati in tempi ridotti Sono gestiti i backup Sono stabiliti programmi di formazione del personale autorizzato

Gestione procedimenti disciplinari di II° grado tramite Consiglio Nazionale di Disciplina (CND)	Il trattamento viene effettuato per l'avvio e lo svolgimento dei procedimenti disciplinari DPR 7 agosto 2012, n. 137 – Regolamenti Consiglio di disciplina	Generalmente le persone fisiche coinvolte nel procedimento disciplinare sia gli "imputati" che i soggetti a cui si potrebbero riferire fatti e avvenimenti	Vengono trattati i dati comuni anagrafici e di contatto dell'assistente sociale coinvolto nel procedimento disciplinare. I procedimenti disciplinari possono avviarsi anche da segnalazioni o istanze ad opera di qualsiasi persona fisica o giuridica che ne ravvisi la necessità. Queste segnalazioni potrebbero contenere qualsiasi tipo di informazioni, dati (anche sensibili), descrizione di avvenimenti o fatti e potrebbero coinvolgere altre persone fisiche, con conseguente trattamento di dati comuni e particolari di Interessati anche vulnerabili e aventi carattere estremamente personale.	I dati trattati possono essere comunicati solo al tribunale competente, come da Regolamento. I dati relativi all'esito finale del procedimento (solo la sospensione) viene pubblicata nell'Albo Unico	I dati degli atti verranno conservati per 10 anni dalla conclusione del procedimento	Per CNOAS: come sopra
Gestione dei dipendenti: rapporto di lavoro, buste paghe, formazione	Gestione del rapporto di lavoro di dipendenti e collaboratori: legittimo interesse (Art. 2 – sexies del D.Lgs. 196/2003 e 101/2018)	-Dipendenti - Collaboratori	- Dati comuni anagrafici e di contatto - Dati finanziari - Dati assenze/permessi per malattia	- Studi commerciali - Consulente del lavoro - Enti previdenziali	10 anni dall'ultima registrazione (art. 2220c.c.)	Per CNOAS: come sopra
Gestione dei dipendenti: formazione sicurezza sul lavoro	Adempimenti di legge sicurezza sul lavoro (attestati di formazione) (D.Lgs. 81/08)	- Dipendenti	- Dati anagrafici	- RSPP - Enti formazione	10 anni	Per CNOAS: come sopra
Gestione fornitori	Gestione degli ordini	- Fornitori	- Dati comuni anagrafici e di contatto	- Studio commercialistico	10 anni	Per CNOAS: come sopra
Verifica dei requisiti per forniture dei servizi	Controllo della dichiarazione sostitutiva ai sensi dell'art. 71 n.445/2000	- Fornitori	- Casellario giudiziale e anagrafe delle sanzioni amministrative dipendenti da reato	- Nessuno	10 anni	Per CNOAS: come sopra

Verifica dei requisiti per vincitori concorsi per dipendenti	Controllo della dichiarazione sostitutiva ai sensi dell'art. 71 n. 445/2000	- Partecipanti ai concorsi pubblici	- Casellario giudiziale e anagrafe delle sanzioni amministrative dipendenti da reato	- Nessuno	10 anni	Per CNOAS: come sopra
Misurazione temperatura corporea	Gestione emergenza sanitaria	- Fornitori - Dipendenti, collaboratori - Utenti	- Dati Sanitari (non conservati né trattati)	- Nessuno	I dati non vengono registrati, ma solo comunicati a voce all'Interessato	-

Nessuno dei trattamenti prevede il trasferimento di dati in Paesi Terzi

9.1 – INTERVENTI DI FORMAZIONE SVOLTI

INTERVENTI DI FORMAZIONE PRIVACY SVOLTI				
Luogo e Data		Roma, dicembre 2018 – gennaio 2019		
Docente:		dott. Colonnello Francesco		
Modalità Didattica:		X	Corso in Aula	X E-learning
Partecipanti:		Tutti gli autorizzati interni del CNOAS		
INTERVENTI DI FORMAZIONE PRIVACY SVOLTI				
Luogo e Data		Roma, 22 settembre 2021		
Docente:		avv. Edoardo Chiavirano		
Modalità Didattica:		X	Colloqui/approfondimenti individuali	
Partecipanti:		Tutti gli autorizzati interni del CNOAS		
Oggetto:		Colloqui individuali posti in essere al fine della verifica degli adempimenti privacy, nonché al fine di chiarire aspetti applicativi della normativa, anche in tempo di Covid 19 (rilevamento temperatura corporea, utilizzo green pass e possibilità di presa visione, impossibilità di archiviazione, registrazione e profilazione dei dati). Evasione quesiti brevi, applicativa della disciplina specifica posta in essere dal CNOAS. Verifica e discussione delle informative privacy.		

10 – DICHIARAZIONE DI IMPEGNO E FIRMA

Il presente documento, revisionato il 25 novembre 2021, viene firmato in calce per accettazione e formale ufficializzazione dal Presidente del CNOAS, dott. Gianmario Gazzì.

L'originale del presente documento viene custodito presso la sede legale, per essere esibito in caso di controlli, verifiche e/o ispezioni.

Luogo: Roma

Data: 25 novembre 2021

Il Presidente CNOAS: Dott. Gianmario Gazzì

Il DPO/RDP (presa visione): avv. Andrea Gandino / avv. Edoardo Chiavirano