

Allegato 5 - Registro dei Rischi

(redatto sulla base del Registro delle attività di trattamento ex art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Dati identificativi soggetto a cui appartiene il registro	
Denominazione	Comune di Corneliano d'Alba
Forma giuridica	Ente pubblico non economico regionale o locale
Indirizzo/Sede legale	Piazza Cottolengo, n. 49 - 12040 Corneliano d'Alba (CN)
P.IVA/C.F.	P.Iva: 00324510049
N. telefono / FAX	Telefono: 0173/619964 - Fax 0173/619954
Email	corneliano.dalba@ruparpiemonte.it
Domicilio digitale (PEC o altro)	corneliano.dalba@cerrt.ruparpiemonte.it
Referente Ufficio Privacy	Marta Nervo
Componenti Ufficio Privacy	Marta Nervo

Responsabile della Protezione dei Dati (DPO)	
Denominazione	AVVOCATO MARCO GALVAGNO
Indirizzo	Piazza Medici 16 - 14100 Asti
P.IVA/C.F.	GLVMRC74A16A479D
N. telefono	0141/593025
Email	avv.galvagno@gmail.com
Domicilio digitale (PEC o altro)	rdp.privacy@pec.it
Certificazione	Professionista certificato UNI 11697 Registro KHC DPO2455 scad. 2023

Data di creazione:	04/05/2018
Data di aggiornamento:	12/12/2021
Responsabile della tenuta del registro	Marta Nervo

ID	CONTESTO	Fonte di rischio	VALUTAZIONE DEL LIVELLO DI SIGNIFICATIVITA' DELLE FONTI DI RISCHIO SULLA PROTEZIONE DEI DATI PERSONALI	LIVELLO	
CE.1	esterno	socioeconomico	Poiché i dati personali degli utenti sono trattati mediante sistemi IT, esiste rischio di attacchi informatici esterni è significativo	5	5
CE.2	esterno	socioeconomico	Poiché i dati personali su supporta cartaceo sono custoditi presso i locali dell'Ente, esiste un rischio di accesso fisico non autorizzato ai locali	1	1
CE.3	esterno	ambientale	Poiché tutte le sedi dell'Ente sono localizzate in zona non soggetta a eventi atmosferici estremi, non esistono rischi associati a fattori ambientali esterni	n.a.	n.a.
CE.5	esterno	settoriale	Poiché tratta dati personali che potrebbero avere interesse per competitors, esiste il rischio di tentativi di sottrazione	2	2
CE.6	esterno	settoriale	Poiché i dati personali di cui l'Ente ha la titolarità sono trattati anche da fornitori esterni, esiste il rischio di incidenti o trattamenti illeciti	3	3
CE.7	esterno	tecnologico	Poiché i dati personali sono trattati in modalità informatica, esiste il rischio di incidenti derivanti da vulnerabilità dei sistemi IT può essere significativo	4	4
CI.1	interno	Perimetro IT	Poiché i dati personali di utenti, fornitori, dipendenti sono trattati da personale in modalità informatica, esiste il rischio di attacchi informatici interni	3	3
CI.2	interno	Perimetro IT	Poiché i dati personali sono trattati in modalità informatica, esiste il rischio di incidenti derivanti da guasti dei sistemi IT	4	4
CI.3	interno	Perimetro organizzativo	Poiché i dati personali sono trattati da personale interno, esiste il rischio di illeciti nel trattamento di tali dati	2	2
CI.4	interno	Perimetro organizzativo	Poiché i dati personali sono trattati da personale interno, esiste il rischio di errori nel trattamento di tali dati	3	3
CI.5	interno	perimetro fisico	Poiché i dati personali sono trattati presso i locali dell'Ente, esiste il rischio di incidenti che distruggano i supporti dei dati (incendio, allagamento)	2	2
CI.6	interno	perimetro fisico	Poiché i dati personali sono trattati presso i locali dell'Ente, esiste il rischio di incidenti che interrompono i trattamenti dei dati	2	2

ID RSK	FONTE DI RISCHIO	INDIVIDUAZIONE SCENARIO DI RISCHIO (VULNERABILITA' E MINACCIA)	ARCHIVIO DATI	INTERESSATI	DPIA	TITOLARE DEL RISCHIO	OB.CO NF.	OB.IN TEG.	OB.DI SP.	L.VER. RSK	L.IMP. RSK	L RSK	LIV.TOT. RSK	PONDERAZIONE LIV.TOT. RSK	OPZIONE TRATTAMENTO	TRATTAMENTO RSK	LRR.RSK	PONDERAZIONE LRR
RSK.01	esterna	Poiché non sono state adottate le misure tecniche organizzative inerenti la gestione dei sistemi IT, soggetti esterni non autorizzati hanno compromesso la sicurezza dei dati personali di utenti, fornitori, dipendenti	Informatico	Clienti; Fornitori; Dipendenti	no	responsabile interno Servizio IT nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	4	5	20	20	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	5	accettabile
RSK.02	interna	Poiché non sono state adottate le misure tecniche organizzative inerenti la gestione dei sistemi IT, soggetti esterni non autorizzati hanno compromesso la sicurezza dei dati personali cittadini, utenti, fornitori, dipendenti	Informatico	Utenti; Fornitori; Dipendenti	no	responsabile interno Servizio IT nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	4	5	20	20	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	5	accettabile
RSK.03	esterna	Poiché non sono state adottate le misure tecniche organizzative inerenti la gestione degli accessi alla sede fisica, soggetti esterni non autorizzati sono entrati nei locali e hanno compromesso la sicurezza dei dati personali di utenti, fornitori, dipendenti	cartaceo; informatico	Utenti; Fornitori; Dipendenti	si	responsabile interno del Personale nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	3	4	12	12	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	2	accettabile
RSK.04	interna	Poiché non sono state adottate misure tecnico organizzative per assicurare i backup e il disaster recovery dei Sistemi IT, un incidente ha compromesso la sicurezza dei dati personali di utenti, fornitori, dipendenti	Informatico	Utenti; Fornitori; Dipendenti	no	responsabile interno Servizio IT nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	4	5	20	20	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	4	accettabile
RSK.04	interna	Poiché non sono state adottate misure tecnico organizzative per assicurare i backup e il disaster recovery dei Sistemi IT, un incidente ha compromesso la sicurezza dei dati personali di utenti, fornitori e dipendenti	Informatico	Utenti; Fornitori; Dipendenti	si	responsabile interno Servizio IT nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	4	5	20	20	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	4	accettabile
RSK.05	interna	Poiché non sono state adottate misure tecnico organizzative per formare e sensibilizzare il personale in merito alle lecite modalità di trattamento dei dati personali, questi hanno effettuato trattamenti illeciti	Informatico; Cartaceo	Tutti gli interessati	si	responsabile interno del Personale nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	3	3	9	9	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	3	accettabile
RSK.06	interna	Poiché non sono state adottate misure tecnico organizzative per formare e sensibilizzare il personale in merito alle sicure modalità di trattamento dei dati personali, questi hanno effettuato trattamenti illeciti	Informatico; Cartaceo	Tutti gli interessati	si	responsabile interno nominato ex art. 2-quaterdecies del d.lgs 196/2003	x	x	x	4	3	12	12	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	4	accettabile
RSK.07	esterna	Poiche i fornitori esterni che trattano dati personali sotto la titolarità dell'Ente non hanno adottato misure tecnico organizzative di protezione, la sicurezza dei dati personali è stata compromessa.	Informatico; Cartaceo	Tutti gli interessati	si	Responsabili esterno del trattamento	x	x	x	3	4	12	12	non accettabile	Adottare misure tecnico organizzative	Vedi dichiarazione di applicabilità misure tecnico organizzative	4	accettabile

ID	TRATTAMENTO	INTERESSATI	FINALITA' TRATTAMENTO	VALUTAZIONE NECESSITA' TRATTAMENTO	VALUTAZIONE IMPATTO DIRITTI E LIBERTA' FONDAMENTALI INTERESSATO	LIVELLO IMPATTO		TRATTAMENTO		
DPIA.01	ciclo passivo	fornitori	adempimenti contrattuali e contabili	opzionale	Poiché sono stati compromessi dati personali di alcuni fornitori, il ciclo passivo e attivo è stato a sua volta compromesso e ha avuto impatto sul corretto adempimento degli obblighi contrattuali	3	3	Vedi dichiarazione di applicabilità misure tecnico organizzative	1	1
DPIA.02	gestione cedolini	dipendenti	adempimenti contrattuali e contabili	opzionale	Poiché sono stati compromesse dati personali di dipendenti, il processo di predisposizione dei cedolini è stato a sua volta compromesso e ha avuto impatto sulla regolarità di corresponsione delle retribuzioni	4	4	Vedi dichiarazione di applicabilità misure tecnico organizzative	2	2

DICHIARAZIONE DI APPLICABILITA' DELLE MISURE TECNICO ORGANIZZATIVE (CONTROLLI OPERATIVI) PER IL TRATTAMENTO DEI RISCHI

ID RSK	SCENARIO DI RISCHIO (MINACCIA E VULNERABILITA')	Politiche e Istruzioni	Organizzazione per la Sicurezza	Sicurezza delle Risorse Umane	Gestione degli Assett	Controllo Accessi ai Sistemi IT	Crittografia	Sicurezza Fisica e Ambientale	Sicurezza Operatività IT	Sicurezza Comunicazioni e Networking	Acquisizione, Sviluppo, Manutenzione e Sistemi IT	Relazioni con i fornitori	Gestione degli Incidenti	Continuità Operativa e Resilienza	Conformità
RSK.01	Poiché non sono state adottate le misure tecniche organizzative inerenti la gestione dei sistemi IT, soggetti esterni non autorizzati hanno compromesso la sicurezza dei dati personali di utenti, fornitori, dipendenti				X	X	X		X	X	X		X		X
RSK.02	Poiché non sono state adottate le misure tecniche organizzative inerenti la gestione dei sistemi IT, soggetti esterni non autorizzati hanno compromesso la sicurezza dei dati personali cittadini, utenti, fornitori, dipendenti				X	X	X		X	X	X		X		X
RSK.03	Poiché non sono state adottate le misure tecniche organizzative inerenti la gestione degli accessi alla sede fisica, soggetti esterni non autorizzati sono entrati nei locali e hanno compromesso la sicurezza dei dati personali di utenti, fornitori, dipendenti		X		X			X					X		
RSK.04	Poiché non sono state adottate misure tecnico organizzative per assicurare i backup e il disaster recovery dei Sistemi IT, un incidente ha compromesso la sicurezza dei dati personali di utenti, fornitori, dipendenti				X				X				X	X	
RSK.04	Poiché non sono state adottate misure tecnico organizzative per assicurare i backup e il disaster recovery dei Sistemi IT, un incidente ha compromesso la sicurezza dei dati personali di utenti, fornitori e dipendenti				X				X				X	X	
RSK.05	Poiché non sono state adottate misure tecnico organizzative per formare e sensibilizzare il personale in merito alle lecite modalità di trattamento dei dati personali, questi hanno effettuato trattamenti illeciti	X	X	X	X								X		
RSK.06	Poiché non sono state adottate misure tecnico organizzative per formare e sensibilizzare il personale in merito alle sicure modalità di trattamento dei dati personali, questi hanno effettuato trattamenti illeciti	X	X	X	X										
RSK.07	Poiche i fornitori esterni che trattano dati personali sotto la titolarità dell'Ente non hanno adottato misure tecnico organizzative di protezione, la sicurezza dei dati personali è stata compromessa.	X									X	X	X		X