PROCEDURA
DI RICOGNIZIONE E COMPLIANCE PRIVACY
marzo 2022

La presente relazione rappresenta quanto rilevato dal sottoscritto, affidatario della funzione di responsabile per la protezione dei dati personali (DPO) per conto del Consorzio dei Comuni B.I.M. SARCA MINCIO GARDA, nel contesto dell'attività condivisa con il Segretario Consorziale, Dott.ssa Luisa Ferrazza nell'incontro dello scorso 9 marzo 2022 e completata con l'analisi della "*Relazione sulle misure organizzative tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti"* redatta in data 30 dicembre 2021 dal sig. Maurizio Leonardi, affidatario della funzione di amministratore di sistema per l'anno 2021.

Questo intervento, oltre che finalizzato a fornire supporto per favorire il processo sopra richiamato, costituisce una delle funzioni proprie del DPO, che, ai sensi dell'art. 38 del GDPR, è tenuto ad informare e fornire consulenza al titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal vigente assetto normativo nonché a sorvegliarne l'osservanza.

L'attività descritta nella presente relazione ha riguardato un'analisi dei seguenti processi ed ambiti di trattamento:

1	STRUTTURA ORGANIZZATIVA E ATTRIBUZIONE DI RUOLI E FUNZIONI
2	ATTIVITÀ FORMATIVA RIVOLTA AL PERSONALE E AI COLLABORATORI
3	MISURE DI SICUREZZA RELATIVE AI TRATTAMENTI ELETTRONICI
4	MISURE DI SICUREZZA PER I TRATTAMENTI CARTACEI
5	RUOLO DEGLI AMMINISTRATORI DI SISTEMA
6	DEFINIZIONE DEI CRITERI DI CONSERVAZIONE DEI DATI TRATTATI
7	REGISTRO DEI TRATTAMENTI
8	GESTIONE DELL'ESERCIZIO DEI DIRITTI DA PARTE DEGLI INTERESSATI
9	GESTIONE DEGLI INCIDENTI DI SICUREZZA
10	INFORMATIVE E BASI GIURIDICHE DEI DIVERSI TRATTAMENTI
11	TRATTAMENTI A RISCHIO ELEVATO E VALUTAZIONI DI IMPATTO
12	TRATTAMENTI SVOLTI MEDIANTE I SITI WEB DEL TITOLARE

Per ciascuno dei punti sopra evidenziati si è predisposta una tabella di riepilogo in cui si da evidenza dei seguenti aspetti:

- ruolo/attività/misure da dover considerare in ragione del vigente assetto normativo;
- note relative allo "stato dell'arte";
- note del DPO con indicazioni operative per favorire l'attività di compliance e azioni da poter intraprendere.

Con l'occasione si segnala che, nel contesto delle attività che costituiscono le funzioni del DPO, è intenzione del sottoscritto completare nel primo semestre dell'anno in corso un'attività di controllo e supporto, coinvolgendo i referenti dell'attività di gestione degli strumenti informatici (preposti della società Altogarda Informatica Srl) e la nuova figura designata quale amministratore di sistema, dott.Giuseppe Carnessali, per eseguire congiuntamente un approfondimento sui seguenti argomenti:

- ricognizione delle misure tecnico-organizzative relativamente ai trattamenti elettronici svolti nei diversi ambiti operativi dell'Ente;
- identificazione di eventuali trattamenti aventi un "rischio elevato per i diritti e le libertà delle persone fisiche" e del relativo processo di valutazione di impatto (art. 35 GDPR).

Data breach

Si riferisce che l'Ente non ha comunicato al sottoscritto DPO alcun episodio di data breach occorso nei mesi precedenti all'accesso.

Si invita, laddove ciò possa avere luogo, ad osservare le indicazioni operative stabilite all'interno della omonima procedura adottata dall'Ente, coinvolgendo immediatamente il DPO per permettere le funzioni di cui competente.

Formazione personale e collaboratori

Si ricorda l'importanza della formazione quale elemento fondamentale del "modello organizzativo privacy" implementato dall'Ente. Nel corso dell'incontro si è colta la sensibilità e l'attenzione sul tema e si è condivisa l'importanza della formazione quale presupposto per favorire la corretta adozione di adeguate misure tecnico-organizzative finalizzate a garantire che i trattamenti eseguiti siano adeguati ai rischi che a varia natura possano aver luogo nel contesto dell'Ente.

Nell'incontro si è stabilito di programmare anche nel corrente anno 2022 attività formativa rivolta al personale per favorire la corretta esecuzione delle funzioni assegnate.

Per quanto riguarda i trattamenti realizzati attraverso strumenti elettronici, si è convenuto sull'opportunità di richiamare l'attenzione di tutti i collaboratori sulle misure di sicurezza riferite alla gestione delle password e all'utilizzo della posta elettronica anche condividendo il vademecum dell'Autorità Garante "Suggerimenti per creare e gestire password a prova di privacy" (accessibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4248578) e le infografiche relative al rischio "spamming e fishing" sempre predisposte dall'Autorità Garante.

Si ringrazia per l'attenzione e si porgono distinti saluti.

Riva del Garda, 1 aprile 2022

avv. Matteo Grazioli
responsabile protezione dei dati personali

1) STRUTTURA ORGANIZZATIVA E ATTRIBUZIONE DI RUOLI E FUNZIONI

ruolo	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
individuazione del Titolare del trattamento	Consorzio dei Comuni B.I.M. SARCA MINCIO GARDA Viale Dante, 46 – 38079 TIONE DI TRENTO Tel. e Fax 0465/321210	il titolare del trattamento è la persona fisica o giuridica che singolarmente o assieme ad altri determina le finalità e i mezzi del trattamento di dati personali	nessuna
sono presenti trattamenti eseguiti in contitolarità?	alla data della ricognizione non si rilevano trattamenti eseguiti in contitolarità con terzi.	l'eventuale contitolarità deve essere accompagnata da un accordo interno tra i contitolari (art. 26 GDPR).	nessuna
il titolare è stato nominato quale "responsabile del trattamento" da parte di terzi per trattamenti svolti per conto di quest'ultimo?	alla data della ricognizione non si rilevano trattamenti eseguiti da parte dell'Ente in veste di responsabile del trattamento.	verificare la presenza del documento di nomina ed in caso specificare nel Registro dei trattamenti, se ancora non dettagliato, quanto segue: 1) il nome e i dati di contatto del/dei titolari per conto del quale si agisce come responsabile; 2) le categorie dei trattamenti effettuati per conto di ogni titolare; 3) l'eventuale trasferimento dei dati extra UE; 4) una descrizione delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati trattati.	nessuna
sono stati designati quali "responsabili del trattamento" i soggetti che debbano effettuare trattamenti per conto del vostro Ente (art. 28 GDPR)?	il Registro dei trattamenti riporta l'elenco dei soggetti individuati quali responsabili del trattamento.	prevedere la conservazione dell'atto di nomina nella documentazione che può essere esibita agli interessati, al DPO e all'Autorità Garante; dettagliare la loro elencazione nel Registro dei trattamenti; svolgere periodicamente nei confronti di ciascun Responsabile un controllo circa la conformità de trattamento svolto da quest'ultimo al dettato normativo, sollecitando una copia del Registro dei trattamenti elaborato testo conto dell'art. 30, punto 2 GDPR.	Si suggerisce di verificare quali siano i soggetti (persone fisiche e giuridiche esterne alla società) che abbiano modo di eseguire trattamenti per conto del titolare, prendendo in considerazione l'elenco riportato nel Registro e, se necessario, formalizzare la nomina di "responsabile del trattamento" nei confronti dei soggetti che non siano stati già individuati come tali. Nei confronti dei soggetti che sono stati designati quali responsabili del trattamento è opportuno compiere una attività di compliance anche tramite il documento messo a disposizione dal DPO.
all'interno dell'Ente sono stati individuati soggetti aventi un ruolo apicale e di coordinamento quali "designati del trattamento" (primo comma art. 2-quaterdecies d.lgs 196/03)?	L'assetto organizzativo del titolare non rende necessario individuare tale funzione.		nessuna

sono stati individuati ed autorizzati al trattamento tutti i soggetti coinvolti (secondo comma art. 2-quaterdecies d.lgs 196/03)?	le nomine sono agli atti.	verificare la presenza delle "lettere di incarico" attribuite a tutti i soggetti che debbano essere autorizzati; controllare che con tutti i soggetti autorizzati siano stati condivisi i seguenti documenti: a) materiale formativo ed istruzioni operative; b) regolamento interno riferito all'utilizzo degli strumenti elettronici aziendali; c) procedura di gestione del "data breach"; d) circolari interne o note di servizio in relazione a particolari trattamenti.	Verificare che l'attribuzione dell'incarico/autorizzazione al trattamento nei confronti di ciascun soggetto operante sotto l'autorità del titolare sia coerente con le necessità derivanti dal ruolo e dalle necessità organizzative dell'Ente. Verificare che i profili di accesso assegnati a ciascun soggetto autorizzato tengano conto di tale requisito, escludendo l'accesso ad informazioni non indispensabili o ridondanti rispetto alle necessità derivanti dalla mansione svolta.
è stato/sono stati individuati soggetti con il ruolo di amministratori di sistema?	dott. Giuseppe Carnessali, referente della società Altogarda Informatica Srl.	sollecitare all'amministratore di sistema il rilascio di una relazione periodica (si suggerisce una cadenza annua) sul suo operato, sugli interventi svolti e programmati, sullo stato di adozione delle misure di sicurezza relativamente all'infrastruttura elettronica dell'Ente; informare l'amministratore di sistema di poter coinvolgere il DPO laddove abbia necessità; condividere con l'amministratore di sistema la procedura di gestione del "data breach".	Dare attuazione alle indicazioni ripotate nella colonna precedente.
i dati di contatto del DPO sono stati comunicati all'Autorità garante e sono facilmente accessibili agli interessati?	avv. Matteo Grazioli	verificare l'avvenuta comunicazione dei dati di contatto del DPO ai dipendenti, agli interessati (anche tramite una verifica delle informative in uso e dei dati di contatto diffusi mediante il sito web dell'Ente)	nessuna

2) ATTIVITÀ FORMATIVA E ISTRUZIONI FORNITE AI SOGGETTI AUTORIZZATI AL TRATTAMENTO

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
i soggetti incaricati/autorizzati sono stati istruiti sulle politiche di sicurezza volte a garantire il rispetto della normativa vigente in materia di protezione dati personali?	Sì, anche attraverso una sessione formativa tenuta dal DPO.	Il titolare del trattamento e il responsabile del trattamento è tenuto a far sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso. Si invita il titolare ad istruire tutti i soggetti autorizzati sule condotte da osservare, sulle misure di sicurezza cui attenersi, sulle procedure di gestione degli incidenti di sicurezza, sulle procedure aziendali riferite a particolari trattamenti. Si prescrive di condividere e rendere facilmente accessibili agli incaricati i seguenti documenti: - istruzioni operative; - materiale formativo; - disciplinare riferito all'utilizzo degli strumenti informatici; - procedura di gestitone del "data breach"; - istruzioni o note elaborate dall'amministratore di sistema (se presente).	Ricordarsi di consegnare in sede di assunzione il materiale formativo predisposto in materia di protezione dati personali. Anche nell'anno in corso è in programma una sessione formativa con il coinvolgimento del DPO.

sono state elaborate e condivise istruzioni operative, policy interne, procedure di gestione (es. data breach, riscontro ai diritti degli interessati, gestione esercizio diritto di accesso?)	la documentazione è agli atti	Si ricorda la necessità che ogni soggetto autorizzato al trattamento presti attenzione ai seguenti accorgimenti minimi: *Autenticazione degli incaricati*: assegnare credenziali dedicate a ciascun incaricato. Adottare una politica per l'aggiornamento delle password degli utenti. Obbligare l'incaricato ad aggiornare la password al primo accesso. Limitare il numero di tentativi d'accesso ad un account. Disabilitare l'account al cessare del rapporto con l'autorizzato. *Gestione delle abilitazioni*: definire profili di abilitazione differenziati in ragione delle funzioni assegnate a ciascun soggetto autorizzato. Disabilitare i profili autorizzati obsoleti. Procedere a una revisione semestrale delle autorizzazioni. Adottare tutti gli accorgimenti possibili per escludere la condivisione delle credenziali di accesso tra i soggetti autorizzati. *Tracciare gli accessi e gestire gli incidenti:* prevedere un sistema di tracciatura degli accessi. Informare gli incaricati dell'esistenza del sistema di tracciatura. Proteggere i sistemi di logging e le informazioni registrate. Prevedere procedure per la segnalazione di violazioni di dati personali. *Sicurezza sul posto di lavoro*: prevedere una procedura di disconnessione automatica della sessione. Utilizzare antivirus aggiornati regolarmente. Installare un firewall. Prevedere che gli strumenti removibili in dotazione degli incaricati siano protetti da cifratura. Non autorizzare l'utilizzo di dispositivi removibili (chiavette usb, notebook personali, ecc. *Proteggere la rete informatica interna*: limitare il trattamento ed il flusso di dati allo stretto necessario e solo con soggetti che, nell'esercizio delle proprie competenze, abbiano stretta necessità di accedervi. Verificare che l'accesso via VPN avvenga solo da dispositivi fidati sotto il controllo dell'Ente e adeguatamente protetti. *Gestione archivi*: proteggere tutti gli archivi (elettronici e cartacei) escludendo ogni possibile accesso da parte di terzi non autorizzati. Prevedere che l'accesso agli archivi (elettronici e cartacei) sia consentito solo a personale autorizzato. Conformare tutti i profili di accesso alle diverse banche dati escludendo la possibilità che soggetti non autorizzati possano consultare dati personali estranei a quanto di propria competenza nel rispetto dei principi di necessità, temporalità e limitatezza. Provvedere alla cancellazione/distruzione dei dati personali nel rispetto delle disposizioni vigenti e dei criteri temporali che il titolare deve osservare. *Condivisione di dati con terzi*: adottare sistemi protetti per la condivisione in elettronico di dati personali con i terzi legittimati (es. reti cifrate, supporti criptati, ecc.); assicurarsi che il destinatario sia l'effettivo titolare dell'account di posta; evitare la condivisione di dati personali ed indirizzi di posta elettronica in CCN; trasmettere eventuali password di accesso ai documenti con strumenti diversi e separati.	Si suggerisce di raccomandare nuovamente a tutti i dipendenti e ai collaboratori l'invito alla massima attenzione circa l'utilizzo degli strumenti informatici dell'Ente Tale raccomandazione potrebbe essere integrata con le infografiche elaborate dal Garante relativamente alla corretta gestione delle password, al rischio derivante dall'attività di spamming e fishing.
si effettua un controllo sull'operato degli addetti alla manutenzione e gestione dell'infrastruttura informatica aziendale e dei software di gestione dei dati personali?	il controllo è cadenzato annualmente, agli atti risulta la relazione dell'ads riferita all'anno 2021.	si invita voler sottoporre con cadenza periodica (annualmente) agli amministratori di sistema un documento in cui venga fornita una relazione sull'attività svolta e descritte le misure di sicurezza presenti	il DPO ha contattato il dott. Carnessali, chiedendo di essere tenuto aggiornato sulle misure tecnico organizzative adottate per mitigare ogni rischio informatico.

3) MISURE DI SICUREZZA TRATTAMENTI ELETTRONICI

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere

esiste ed è disponibile in caso di richiesta del DPO e dell'Autorità Garante una ricognizione aggiornata dell'infrastruttura informatica utilizzata dal titolare?	Reazione di conformità infrastrutturale redatto dal sig. Maurizio Leonardi di data 30 dicembre 2021.	elaborare e mantenere costantemente aggiornata una ricognizione dell'infrastruttura e delle relative misure di sicurezza;	Valutare (e portare a compimento) le azioni di mitigazione dei rischi suggerite dall'ads. Mantenere aggiornata l'analisi dei rischi tenuto conto degli interventi di mitigazione eseguiti da parte della società Altogarda Informatica Srl.
esiste ed è disponibile un inventario dei software autorizzati?	vedi sopra	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop. Utilizzare macchine virtuali o altri sistemi adeguati per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	vedi sopra
Si effettuano regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzati?	vedi sopra	Utilizzare configurazioni sicure per la protezione dei sistemi operativi; eseguire tutte le operazioni di amministrazione remota per mezzo di connessioni protette (protocolli intrinsecamente sicuri e su canali sicuri).	vedi sopra
E' garantita la protezione dei dati personali oggetto di trattamento?	vedi sopra	Verificare se l'amministratore di sistema ha individuato elementi di vulnerabilità e porvi rimedio senza ritardo. Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati. Eseguire periodicamente la ricerca delle vulnerabilità con frequenza commisurata alla complessità dell'infrastruttura utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione. Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni. Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti.	Si suggerisce di elevare al massimo livello le misure di protezione!
sono presenti eventuali ipotesi di vulnerabilità? Come sono gestite?	vedi sopra	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio. Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). Verificare che le vulnerabilità siano state risolte implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Si suggerisce di elevare al massimo livello le misure di protezione
i privilegi di amministratore sono gestiti correttamente?	vedi sopra	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa. Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Si suggerisce di elevare al massimo livello le misure di protezione

i profili di accesso sono gestiti correttamente?	vedi sopra	Mantenere l'inventario di tutte le utenze garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito. Utilizzare sistemi di autenticazione differenziati per tutti gli accessi. Assicurare che le credenziali delle utenze vengano sostituite con frequenza semestrale. Impedire che credenziali già utilizzate possano essere riutilizzate o entrare in possesso di terzi. Conservare e far conservare agli assegnatari le credenziali in modo da garantirne disponibilità e riservatezza.	Si suggerisce di elevare al massimo livello le misure di protezione
sono presenti difese contro eventuali malware?	vedi sopra	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti devono essere mantenuti aggiornati in modo automatico. Installare su tutti i dispositivi firewall adeguati. Limitare l'uso di dispositivi removibili non protetti da cifratura. Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi. Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che un codice malevolo raggiunga l'infrastruttura informatica. Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione. Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. Disattivare l'apertura automatica dei messaggi di posta elettronica. Disattivare l'anteprima automatica dei contenuti dei file. Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione. Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam. Filtrare il contenuto del traffico web. Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non sia strettamente necessaria per l'organizzazione. Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni. Implementare strumenti per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie. Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Si suggerisce di elevare al massimo livello le misure di protezione

esiste una adeguata procedura di back up?	vedi sopra	Effettuare giornalmente una copia di sicurezza delle informazioni. Eseguire backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore. Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova. Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Si suggerisce di elevare al massimo livello le misure di protezione

4) MISURE DI SICUREZZA TRATTAMENTI CARTACEI

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
la sede del titolare è protetta contro accessi esterni non autorizzati?	Gli archivi cartecei sono protetti in stanze soggette al controllo del personale incaricato.	si ritiene utile suggerire di rafforzare possibili misure di protezione contro accessi fisici non autorizzati.	Dare compimento alle note del DPO indicate nella colonna precedente. Nel corso dell'anno 2022 l'ente intende adottare un sistema di allarme a presidio della propria sede.
Gli archivi sono dislocati in più contesti? Ogni luogo di conservazione è protetto?	Sì	verificare la sicurezza degli archivi contro possibili intromissioni, allagamenti, incendi.	Si ritiene utile suggerire di rafforzare possibili misure di protezione contro accessi fisici non autorizzati per escludere rischi connessi al furto, perdita, danneggiamento, accessi abusivi ai dati personali.
i documenti contenti dati personali sono protetti in modo tale da escludere l'accesso da parte di terzi?	Sì	si caldeggia la massima attenzione sulla conservazione della documentazione cartacea. Massima cautela nella gestione di documentazione cartacea all'interno della quale vi siano categorie particolari di dati personali. Si suggerisce di prestare attenzione alle procedure di gestione di stampanti, fotocopiatrici, scanner (riduzione del rischio di perdita o condivisione non necessitata di documenti)	Si suggerisce di dedicare la massima attenzione per ovviare alla perdita, alla diffusione o all'accesso di terzi non autorizzati ai documenti contenenti dati personali rafforzando il sistema di controllo per scongiurare tali ipotesi.
Sono presenti indicazioni riferite alle procedure di distruzione dei documenti decorso il periodo di conservazione?	Sì, tramite la lettera di incarico assegnata a ciascun collaboratore.	è necessario rispettare i tempi di conservazione definiti dalle normative vigenti. E' necessario definire criteri di conservazione che tengano conto dei differenti dati trattati.	Dare compimento alle note del DPO indicate nella colonna precedente.

5) RUOLO DEGLI AMMINISTRATORI DI SISTEMA

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere

sono presenti amministratori di sistema?	dott. Giuseppe Carnessali, referente della società Altogarda Informatica Srl.	L'attribuzione della qualifica di amministratore di sistema deve avvenire previa valutazione delle caratteristiche personali di esperienza, capacità e affidabilità del soggetto designato. Tale soggetto deve fornire idonee garanzie di rispetto delle vigenti disposizioni in materia di trattamento dei dati, con particolare riferimento alla sicurezza. La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante. Laddove siano presenti più amministratori di sistema potrebbe essere necessario suddividere tali figure in apposite categorie, ciascuna distinta in funzione delle mansioni agli stessi attribuite.	nessuna
l'eventuale affidamento terzi di attività di assistenza, manutenzione e gestione dei sistemi informatici è supportata dalla nomina di tali soggetti quali responsabili del trattamento con richiamo alle indicazioni previste dal Provvedimento Generale del garante in materia di amministratore di sistema	Sì	I soggetti terzi dovrebbero fornire una relazione nella quale attestano di aver effettuato le verifiche sui relativi ADS.	nessuna
si svolge un attività di controllo sull'amministratore di sistema	si, controllo annuale	L'operato degli amministratori di sistema deve essere oggetto di un'attività di verifica, con cadenza almeno annuale, da parte dei titolari del trattamento o dei responsabili, al fine di controllare la sua corrispondenza con le misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.	Dare compimento alle note del DPO indicate nella colonna precedente.
è attivo un sistema di registrazione e conservazione dei log?	da verificare	Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.	Comunicare l'esito al DPO

6) DEFINIZIONE DEI CRITERI DI CONSERVAZIONE DEI DATI TRATTATI

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
sono definiti e rispettati differenti tempi di conservazione dei dati trattati?	termini di legge e criteri adottati dal titolare.	ogni attività di trattamento deve rispettare specifici periodi di conservazione dei dati raccolti (temporalità del trattamento).	Si caldeggia una verifica circa l'esatta definizione dei tempi di conservazione dei dati personali trattati nel contesto delle diverse attività svolte ed in ragione delle specifiche finalità della loro raccolta. E' necessario osservare il rispetto dei tempi di conservazione.

periodo conservazione dati personale e collaboratori	termini di legge e criteri adottati dal titolare.	verificare che gli stessi siano riportati nelle informative in uso	E' necessario osservare il rispetto dei tempi di conservazione.
periodo conservazione dati utenti	termini di legge e criteri adottati dal titolare.	verificare che gli stessi siano riportati nelle informative in uso	E' necessario osservare il rispetto dei tempi di conservazione.
periodo conservazione dati amministratori	termini di legge e criteri adottati dal titolare.	verificare che gli stessi siano riportati nelle informative in uso	E' necessario osservare il rispetto dei tempi di conservazione.
periodo conservazione dati fornitori	termini di legge e criteri adottati dal titolare.	verificare che gli stessi siano riportati nelle informative in uso	E' necessario osservare il rispetto dei tempi di conservazione.
periodo conservazione curricula	2 anni dalla loro raccolta.	verificare che gli stessi siano riportati nelle informative in uso	E' necessario osservare il rispetto dei tempi di conservazione.

7) GESTIONE DEL REGISTRO DEI TRATTAMENTI

attività	**note del titolare del trattamento**	**note del DPO**	**azioni da dover intraprendere**
E' presente il Registro dei trattamenti ed è disponibile in caso di richiesta del DPO e dell'Autorità Garante	Sì	Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Il Registro dei trattamenti deve essere sempre accessibile al DPO.	portare a compimento la revisione del Registro.
sono presenti il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati?	Sì	se necessario integrare il Registro con le informazioni mancanti	
sono indicate le finalità di tutti i trattamenti svolti?	Sì	integrare il Registro con i trattamenti conseguenti alla gestione dell'epidemia COVID-19.	
E' presente una descrizione delle categorie di interessati e delle categorie di dati personali?	Sì	se necessario integrare il Registro con le informazioni mancanti	
sono descritte le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali?	Sì	se necessario integrare il Registro con le informazioni mancanti	
sono indicati eventuali trasferimenti di dati personali extra UE?	I dati non sono trasferiti all'esterno del territorio UE		
sono riportati i termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati?	Sì	vedere tabella 6 della presente ricognizione	
Riporta una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dal titolare?	Sì, con rinvio alla relazione dell'ads.	si suggerisce di allegare al Registro un inventario aggiornato delle misure di sicurezza relativamente ai trattamenti cartacei ed elettronici.	

8) GESTIONE DELL'ESERCIZIO DEI DIRITTI DA PARTE DEGLI INTERESSATI

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
E' stata elaborata una procedura per gestire l'eventuale esercizio da parte degli interessati degli artt. da 15 e segg. del GDPR?	da aggiornare	si suggerisce l'adozione di una procedura di gestione e l'individuazione di un soggetto/funzione responsabile di tale attività	da adottare lo schema proposto dal DPO
E' stato individuato un referente per tale attività?	Segretario	si suggerisce l'individuazione di un referente per la gestione di tale attività	la procedura individua il Segretari quale referente per tale attività.
E' presente un modello per favorire all'interessato una domanda avente ad oggetto la proposizione di tali diritti?	agli atti	si suggerisce l'adozione di una modello con cui acquisire l'eventuale richiesta di esercizio dei predetti diritti da parte dell'interessato.	

9) GESTIONE DEGLI INCIDENTI DI SICUREZZA

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
E' stata elaborata una procedura per gestire eventuali incidenti di sicurezza (data breach)?	Sì	si suggerisce l'adozione di una procedura di gestione del data breach	Si rinnova l'invito a voler osservare le modalità di gestione del data breach definite nell'omonima procedura interna. Si rinnova l'invito a voler immediatamente coinvolgere il DPO in caso di data breach.
E' stato individuato un referente per tale attività e/o un gruppo di gestione del "data breach"?	Segretario	si suggerisce l'individuazione di una responsabile referente per la gestione di tale attività	la procedura individua il Segretari quale referente per tale attività.
E' disponibile un modello per la notifica del data breach all'Autorità Garante?	Sì	si suggerisce l'adozione di un modello con cui notificare al Garante l'eventuale "data breach" che debba essere comunicato all'Autorità di controllo.	la notifica potrà essere effettuata mediante la procedura telematica elaborata dall'Autorità Garante e accessibile sul sito web di quest'ultima.

10) INFORMATIVE E CONSENSI

attività	note del titolare del trattamento	note del DPO	azioni da dover intraprendere
Sono presenti informative relative ai trattamenti svolti?	Sì	In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento deve fornire all'interessato, nel momento in cui i dati personali sono ottenuti, un'informativa competa delle informazioni di seguito elencate. Si suggerisce una verifica sull'adeguatezza dei documenti in uso. Si invita a diffondere tutte le informative in uso attraverso il sito web del titolare	Si suggerisce una verifica sull'adeguatezza dei documenti in uso, coinvolgendo se necessario il DPO per ricevere supporto nel merito della loro eventuale revisione.

ciascuna informativa contiene le seguenti informazioni? **a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante?** **b) i dati di contatto del responsabile della protezione dei dati?** **c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento?** **d) la base giuridica del trattamento?** **e) l'esistenza di un processo decisionale automatizzato?** **f) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali?** **g) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale?** **h) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo?** **i) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati?** **l) il diritto di porre reclamo e le coordinate di contatto dell'Autorità Garante?**	da verificare	Si suggerisce una verifica sull'adeguatezza dei documenti in uso.	vedi sopra
Alcuni trattamenti eseguiti dal titolare hanno come base giuridica il consenso dell'interessato?	Sì	Si caldeggia la massima attenzione nella raccolta del consenso (laddove necessario) e nella conservazione dei relativi supporti che attestino tale operazione e la volontà dell'interessato.	Si suggerisce una verifica sull'adeguatezza dei documenti in uso e nell'individuazione delle basi giuridiche che legittimano i diversi trattamenti svolti.

11) VALUTAZIONE DI IMPATTO (DPIA)

misure adottate	note titolare	note DPO	azioni da dover intraprendere
il titolare compie: trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti)?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR.	nessuna
il titolare compie: trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*)?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*)?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti automatizzati finalizzati ad assumere decisioni che producono "*effetti giuridici*" oppure che incidono "*in modo analogo significativamente*"sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.?	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna

il titolare compie: **trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti)?**	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: **trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento?**	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna
il titolare compie: **trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento?**	no	E' necessario per tale trattamento eseguire una valutazione di impatto (DPIA) conforme all'art. 35 del GDPR	nessuna

12) TRATTAMENTI SVOLTI MEDIANTE IL SITO WEB DEL TITOLARE

misure adottate	note titolare	note DPO	azioni da dover intraprendere
privacy policy	presente in home page	in home page deve essere accessibile un'informativa riferita ai trattamenti svolti dal titolare mediante il proprio sito web. L'informativa deve essere esaustiva e trasparente.	nessuna
informative ad hoc	presenti sul sito	l'eventuale raccolta di dati personali mediante il sito o apposite aree dello stesso deve essere accompagnata da una specifica informativa.	nessuna
designazione responsabili	sì	l'eventuale affidamento a terzi di un servizio di manutenzione/assistenza e/o di hosting del sito deve essere accompagnato con la designazione a responsabile	nessuna
stato di adozione delle Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021	adeguato	**a) se il sito prevede l'utilizzo di soli cookie tecnici (per i quali non serve il consenso ma vanno indicati nella cookie policy) la cookie policy dovrà esplicitare quali sono i cookies attivi ed i trattamenti che ne derivano;** **b) se il sito prevede l'utilizzo di cookie di profilazione o di terza parte (per i quali serve il consenso) è necessario modificare sia il banner che la cookie policy.** Il **banner** dovrà indicare quali sono i cookie presenti e: • esplicitare che il sito utilizza cookie tecnici e, previo consenso dell'utente, cookie di profilazione o altri strumenti di tracciamento indicando le relative finalità; • rinviare, tramite link, alla cookie policy contenente l'informativa completa, inclusi gli eventuali altri soggetti destinatari dei dati personali, i tempi di conservazione dei dati e l'esercizio dei diritti di cui al GDPR; • specificare che la chiusura del banner comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici; • contenere un comando (es. una X in alto a destra) per chiudere il banner senza prestare il consenso all'uso dei cookie o delle altre tecniche di profilazione mantenendo le impostazioni di default; • prevedere un comando per accettare tutti o alcuni cookie o altre tecniche di tracciamento; • esplicitare il link ad un'altra area nella quale poter scegliere in modo analitico le funzionalità, le terze parti e i cookie che si vogliono installare e poter prestare il consenso all'impiego di tutti i cookie se non dato in precedenza o revocarlo, anche in unica soluzione, se già espresso. La **cookie policy** dovrà essere integrata con: • tutte le indicazioni di cui agli artt. 12 e 13 del Regolamento con riguardo ai trattamenti derivanti dall'attivazione dei cookies; • il link ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, i soggetti cd. terze parti - il cui elenco deve essere tenuto costantemente aggiornato, siano essi raggiungibili tramite specifici link ovvero anche per il tramite del link al sito web di un soggetto intermediario che li rappresenti - ed i cookie, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.	nessuna