Spett.le

CONSIGLIO REGIONALE DELLA BASILICATA
- Ufficio risorse strumentali, finanziarie e tecnologiche
PEC: cr-basilicata@cert.regione.basilicata.it

Alla c.a. del Dirigente
Alla c.a. del Referente DPO
Email: rocco.martorano@regione.basilicata.it

E p.c.

Alla c.a. dott.ssa Rossana Nardozza
Email: rossana.nardozza@regione.basilicata.it

Check Compliance GDPR

Multibusiness Srl – DPO

Nello svolgimento affidatoci, finalizzato a garantire l'adeguamento completo (c.d. "Compliance") dell'Ente alla vigente normativa privacy nazionale ed europea, a seguito all'audit fisico svolto presso la Vs sede nei giorni 12-13 settembre 2023, è stato aggiornato il documento di Check Compliance GDPR, quale verifica del livello di compliance e riscontro con la Gap Analysis precedentemente svolta, utilizzando il modello basato sull' ultima versione disponibile dello schema ISDP©10003:2020 (progettato e realizzato da *Stefano Posti*, su autorizzazione dello "scheme owner" *Riccardo Giannetti* e dell'organismo di certificazione *Inveo srl*.

Lì, 19/09/2023

per Multibusiness Srl

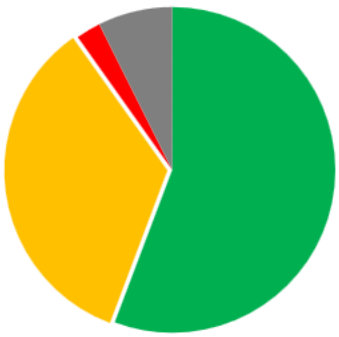
RISULTANZE DELLA REVISIONE E VERIFICA

Il presente documento è il risultato della verifica effettuata in relazione al Master Plan e Road Map progettate. Dalla verifica effettuata (vedi allegato) risulta un miglioramento netto ed evidente della conformità dell'Ente all'attuale normativa privacy in vigore, e quindi una corretta attuazione del Piano di miglioramento previsto; Il miglioramento è visibile dal confronto dei due "grafici a torta" di seguito, che mettono a confronto lo stato dell'arte dell'ente "Prima e dopo":

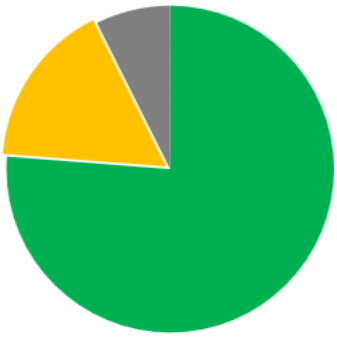
LEGENDA LIVELLO APPLICAZIONE OBIETTIVI DI CONTROLLO

Completamente applicato	*Il controllo è definito, documentato e messo in pratica / attuato con efficacia*
Parzialmente applicato	*Il controllo è messo in pratica / attuato senza adeguata documentazione, oppure è definito e documentato ma non applicato nella sostanza*
Non applicato	*Il controllo non è presente, non definito o comunque non messo in pratica*
Inapplicabile	*Il controllo non è applicabile (da non considerare) rispetto alla valutazione di conformità*

OVERVIEW APPLICAZIONE CONTROLLI GENERALE



Livello di applicazione dei 122 Controlli dello Schema ISDP10003 alla data dell'assessment.



Livello di applicazione dei 122 Controlli dello Schema ISDP10003 alla data dell'assessment.

"Prima" (08.11.2022)

"Dopo" (13.09.2023)

PROSSIME ATTIVITÀ

È necessario aggiornare le designazioni dei Responsabili del trattamento ex art. 28 GDPR; verificare se vi sono stati nuovi affidamenti, e effettuare audit anche da remoto agli attuali fornitori. A tal proposito, in virtù del cambio di Referente DPO, si ri-trasmettono i documenti relativi alla corretta designazione dei Responsabili ex art. 28 GDPR.

NON CONFORMITÀ - NOTE

Di importanza rilevante è l'attività di aggiornamento e verifica dei Responsabili del trattamento; Inoltre, bisogna effettuare la formazione ai "nuovi" dipendenti del Consiglio, o verificare le eventuali precedenti formazioni svolte e valutare un aggiornamento.

Rimane sempre da verificare i particolari ruoli di Corecom e Garante dei diritti della persona (che svolge/ingloba i compiti inerenti all'ufficio del Difensore civico, del Garante per l'infanzia e l'adolescenza, del Garante dei diritti dei detenuti e vittime di reato e del Garante regionale del diritto alla salute e delle persone con disabilità).

Nel complesso non sono rilevate conformità vere e proprie, ma dei miglioramenti e monitoraggi da svolgere; come si nota anche dai grafici sopra riportati il livello di conformità dell'Ente è ottimo.

GDPR COMPLIANCE ASSESSMENT

Autore: Stefano Posti

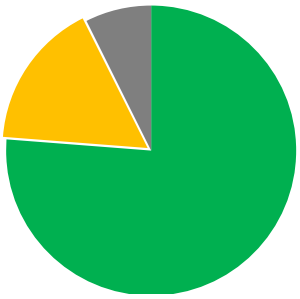
(basato sull'Annex A della norma ISDP©10003:2020) **Data Assessment: [13-09-2023]** **Eseguito da: [MULTIBUSINESS SRL - P.N.]**

ORGANIZZAZIONE - ENTE - SOCIETA'	CONSIGLIO REGIONALE DELLA BASILICATA
PROCESSO / SERVIZIO / PRODOTTO	TUTTE LE ATTIVITA' DELL'ENTE

CHECKLIST OBIETTIVI DI CONTROLLO ISDP©10003:2020

OVERVIEW APPLICAZIONE CONTROLLI GENERALE

MACRO PROCESSI DELLO SCHEMA DI VALUTAZIONE PER LA CONFORMITA' DEL TRATTAMENTO	Applicazione
A.1 *- POLITICA E OBBLIGAZIONI DEL TITOLARE*	10 / 0
A.2 *- SOGGETTI COINVOLTI NEL PROCESSO DEL TRATTAMENTO*	20 / 0
A.3 *- PRINCIPI APPLICABILI AL TRATTAMENTO E TUTELA DEI DIRITTI*	50 / 0
A.4 *- PROCESSI DI ADEGUAMENTO IN FASE DI IDEAZIONE ED ALL'ATTO DEL TRATTAMENTO (privacy by design e by default)*	10 / 0
A.5 *- OBBLIGHI GENERALI, GESTIONE DEL RISCHIO E SICUREZZA DEI DATI PERSONALI*	20 / 0
A.6 *- VALUTAZIONE D'IMPATTO*	10 / 0
A.7 *- TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI E CLOUD COMPUTING*	20 / 0



Livello di applicazione dei 122 Controlli dello Schema ISDP10003 alla data dell'assessment.

LEGENDA LIVELLO APPLICAZIONE OBIETTIVI DI CONTROLLO

Completamente applicato	*Il controllo è definito, documentato e messo in pratica / attuato con efficacia*
Parzialmente applicato	*Il controllo è messo in pratica / attuato senza adeguata documentazione, oppure è definito e documentato ma non applicato nella sostanza*
Non applicato	*Il controllo non è presente, non definito o comunque non messo in pratica*
Inapplicabile	*Il controllo non è applicabile (da non considerare) rispetto alla valutazione di conformità*

A.1 - POLITICA E OBBLIGAZIONI DEL TITOLARE

A.1.1 - Obblighi generali e consapevolezza del titolare
Obiettivo: Stabilire la corretta percezione e declinazione formale, del concetto di responsabilità generale del titolare del trattamento o del responsabile, se fornitore di un prodotto o servizio, per il trattamento di dati personali.

				EVIDENZE - RILIEVI - NOTE
A.1.1.1	Consapevolezza del titolare del trattamento	*Controllo:* Verificare la reale percezione del regolamento EU 2016/679 da parte del titolare del trattamento e come la stessa venga gestita all'interno del contesto organizzativo. Devono essere verificate tutte le azioni di formazione e stimolo alla cultura etica nella gestione del dato personale.	**Completamente applicato**	IL TITOLARE E TUTTI I SOGGETTI AUTORIZZATI SONO ADEGUATAMENTE FORMATI E INFORMATI
A.1.1.2	Adozione di un modello organizzativo privacy	*Controllo:* Verificare che il titolare abbiano redatto e mantengano aggiornato un documento sinottico, che descriva le politiche orhanizzative del titolare. Ogni singola procedura dovrà essere identificabile.	**Completamente applicato**	E' PRESENTE UN MODELLO ORGANIZZATIVO PRIVACY, QUESTO ANDRA' REVISIONATO E MIGLIORATO COSTANTEMENTE
A.1.1.3	Monitoraggio delle politiche attuate	*Controllo:* La politica della protezione dei dati deve essere riesaminata almeno una volta l'anno ovvero ogni qualvolta si verifichino cambiamenti significativi, normativi, di sistema, di personale.	**Completamente applicato**	VEDI PUNTO A.1.1.2
A.1.1.4	Assegnazione interna dei ruoli	*Controllo:* Verificare che ci sia una percezione e corretta assegnazione dei ruoli interni per la ripartizione delle responsabilità.	**Parzialmente applicato**	VEDI PUNTO A.1.1.2 - DA VERIFICARE I RUOLI DI CORECOM E GARANTE DEI DIRITTI DELLA PERSONA persona (che svolge/ingloba i compiti inerenti l'ufficio del Difensore civico, del Garante per l'infanzia e l'adolescenza, del Garante dei diritti dei detenuti e vittime di reato e del Garante regionale del diritto alla salute e delle persone con disabilita)
A.1.1.5	Riesame della direzione	*Controllo:* Verificare che le politiche di adeguamento e monitoraggio per la valutazione della conformità del trattamento dei dati personali, siano coerentemente valutate nel riesame della direzione.	**Completamente applicato**	VEDI PUNTO A.1.1.2

A.1.1.6	Comitato privacy	*Controllo:* Per una migliore garanzia di coordinamento fra le aree aziendali al fine di gestire collettivamente i rischi dei trattamenti di dati che coinvolgono più aree, verificare se il titolare ha costituito un comitato privacy.	**Completamente applicato**	NON E' FORMALMENTE COSTITUITO, MA VI SONO DUE REFERENTI CHE FUNGONO DA SUPPORTO AL DPO (ROSSANA NARDOZZA E ROCCO MARTORANO)
A.2 - SOGGETTI COINVOLTI NEL PROCESSO DEL TRATTAMENTO				
A.2.1 Titolare del trattamento *Obiettivo: Assicurare il rispetto delle norme vigenti da parte del titolare*				**EVIDENZE - RILIEVI - NOTE**
A.2.1.1	Titolarità del trattamento	*Controllo:* Verificare che sia efficacemente percepita e definita la titolarità dei trattamenti all'interno della struttura operativa.	**Completamente applicato**	IL TITOLARE E' CONSAPEVOLE DELL'IMPORTANZA DELL'ADEGUAMENTO NORMATIVO (A TAL PROPOSITO HA AFFIDATO IL SERVIZIO DI SUPPORTO ESTERNAMENTE),E VERIFICA LA CORRETTA APPLICAZIONE DEL MOP
A.2.1.2	Titolare del trattamento che non è stabilito nell'Unione Europea	*Controllo:* Verificare l'eventuale nomina scritta di un "Rappresentante" del titolare o del responsabile, stabilito in uno degli stati membri dove si trovano gli interessati.	**Inapplicabile**	N/A
A.2.1.3	Titolari, articolati in direzioni generali, dipartimenti o in sedi centrali periferiche	*Controllo:* Nei casi in cui il titolare è articolato in direzioni generali, dipartimenti o in sedi centrali, decentrate o periferiche e lo stesso esercita un potere decisionale reale e del tutto autonomo, non condizionato dalla sede centrale o di vertice, verificare che ci sia una definizione quale titolare autonomo o contitolare del trattamento.	**Inapplicabile**	DA VERIFICARE I RUOLI DEL CORECOM BASILICATA E DEL GARANTE DEI DIRITTI E DELLA PERSONA
A.2.2 Contitolari *Obiettivo: Stabilire e assicurare la corretta ripartizione delle responsabilità*				**EVIDENZE - RILIEVI - NOTE**
A.2.2.1	Contitolare del trattamento	*Controllo:* Il titolare del trattamento se stabilisce **finalità** e **mezzi** del trattamento congiuntamente con altri titolari, deve redigere un documento dove vengono chiaramente ripartite le responsabilità e le competenze.	**Parzialmente applicato**	DA VERIFICARE I RUOLI DEL CORECOM BASILICATA E DEL GARANTE DEI DIRITTI E DELLA PERSONA
A.2.2.2	Esercizio dei diritti e comunicazioni all'interessato nella Contitolarità del trattamento	*Controllo:* Quando sono presenti accordi di **contitolarità,** il titolare deve assicurarsi che l'interessato possa esercitare i suoi diritti.	**Parzialmente applicato**	VEDI PUNTI A.2.1.3 E A.2.2.1
A.2.2.3	Comunicazione dell'accordo di contitolarità all'interessato	*Controllo:* Verificare che, l'interessato sia messo a conoscenza del contenuto essenziale dell'accordo fra contitolari.	**Parzialmente applicato**	VEDI PUNTI A.2.1.3 E A.2.2.1
A.2.3 Responsabile del trattamento *Obiettivo: Assicurare il rispetto delle prescrizioni del titolare*				**EVIDENZE - RILIEVI - NOTE**
A.2.3.1	Garanzie sufficienti del Responsabile	*Controllo:* Verificare che il titolare abbia verificato le garanzie sufficienti del responsabile. Deve essere verificata la competenza e la conoscenza specialistica del Responsabile.	**Completamente applicato**	IL TITOLARE HA INDIVIDUATO E DESIGNATOE I FORNITORI RESPONSABILI DEL TRATTAMENTO ART. 28. E' NECESSARIO VERIFICARLI COSTANTEMENTE, ANCHE MEDIANTE AUDIT/ISPEZIONI (ANCHE A DISTANZA)
A.2.3.2	Adozione certificazioni o codici di condotta del Responsabile	*Controllo:* Verificare se, nell'ottica del principio di trasparenza, il responsabile applica codici di condotta o adotta meccanismi di certificazione al fine di comprovare le garanzie sufficienti.	**Completamente applicato**	NON ADOTTATI, NON OBBLIGATORI
A.2.3.3	Contratto con i Responsabili esterni	*Controllo:* Verificare che sia stato stipulato un contratto o altro atto giuridico, in forma scritta e che siano regolamentati almeno i seguenti punti: - Materia disciplinata - Durata del trattamento - Natura del trattamento - Finalità del trattamento - Tipo di dati personali - Categorie degli interessati - Misure di sicurezza adottate - Istruzioni operative	**Completamente applicato**	VEDI PUNTO A.2.3.1
A.2.3.4	Termine contrattuale della prestazione dei Responsabili	*Controllo:* Verificare che, per ogni singolo trattamento al termine del contratto, il Responsabile si attenga alle indicazioni del titolare circa la restituzione e/o la cancellazione dei dati personali trattati e delle copie esistenti.	**Completamente applicato**	VEDI PUNTO A.2.3.1
A.2.3.5	Audit programmati ai responsabili	*Controllo:* Verificare che, nel contratto o altro atto giuridico con il responsabile siano previsti audit programmati (audit di seconda parte). Verificare inoltre che il titolare e il responsabile tengano traccia degli audit eseguiti.	**Parzialmente applicato**	VEDI PUNTO A.2.3.1 - E' NECESSARIO PROGRAMMARE DELLE VERIFICHE ANCHE DA REMOTO TRAMITE RICHIESTA INFORMAZIONI
A.2.3.6	Individuazione e Qualifica dei Sub Responsabili	*Controllo:* Qualora il Responsabile del trattamento, ricorra ad altro responsabile (*sub responsabile*) del trattamento, verificare che il titolare abbia predisposto adeguate politiche di autorizzazione e monitoraggio.	**Completamente applicato**	VEDI PUNTO A.2.3.1
A.2.3.7	Monitoraggio e adeguatezza dei Sub-Responsabili	*Controllo:* Verificare **che** il responsabile applichi processi di monitoraggio ai sub-responsabili	**Completamente applicato**	VEDI PUNTO A.2.3.1
A.2.3.8	Autorizzazione dei sub-responsabili da parte del titolare	*Controllo:* Verificare che il responsabile abbia sottoposto ad autorizzazione scritta del titolare, l'elenco dei sub-responsabili coinvolti nel trattamento.	**Completamente applicato**	VEDI PUNTO A.2.3.1
A.2.4 Responsabile della protezione dei dati *Obiettivo: Verificare la correttezza delle valutazioni effettuate dal titolare o dal Responsabile in merito alla designazione, alla scelta e ai compiti attribuiti al responsabile della protezione dei dati (RPD.)*				**EVIDENZE - RILIEVI - NOTE**
A.2.4.1	Designazione del Responsabile della protezione dei dati (RPD) (DPO)	*Controllo:* Verificare che, in merito alla designazione e all'operato dell'RPD, siano state rispettate le indicazioni di norma.	**Completamente applicato**	E' STATO INDIVIDUATO IL DPO E COMUNICATO ALLL'AUTORITA' GARANTE
A.2.4.2	Designazione di un unico RPD (DPO) per un gruppo imprenditoriale	*Controllo:* In caso di scelta da parte di un gruppo imprenditoriale di nominare un unico RPD, verificare **che** tale scelta sia compatibile con l'agevole accessibilità da parte di ciascuno stabilimento.	**Inapplicabile**	N/A
A.2.4.3	Designazione di un unico RPD (DPO) da parte di più organismi o autorità pubbliche	*Controllo:* Nel caso in cui più organismi pubblici ricorrano alla nomina di un unico RPD (DPO), verificare che la scelta sia documentata e circostanziata nel rispetto della valutazione della struttura organizzativa e dimensionale.	**Inapplicabile**	N/A
A.2.4.4	Dati di Contatto dell'RPD (DPO)	*Controllo:* Verificare che nell'informativa, i dati di contatto dell'RPD (DPO) siano adeguati, chiari e ben declinati.	**Completamente applicato**	SONO PRESENTI I DATI DI CONTATTO (IL LINK CHE RIPORTA AI DATI DI CONTATTO) NELLA PRIVACY POLICY E NELLE INFORMATIVE PUBBLICATE SUL SITO WEB ISTITUZIONALE (SEZIONE PRIVACY); E' STATA CREATA APPOSITA CASELLA MAIL DEL TIPO DPO@_____
A.2.4.5	Qualifiche professionali dell'RPD (DPO)	*Controllo:* Verificare che la scelta dell'RPD (DPO), tenga conto delle conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.	**Completamente applicato**	VEDI PUNTO A.2.4.1
A.2.4.6	Indipendenza del Responsabile della protezione dei dati (RPD)	*Controllo:* Verificare che il Responsabile della protezione dei dati (RPD), dipendente o consulente del titolare, sia messo in condizioni di adempiere alle funzioni e ai compiti assegnategli in modo indipendente, senza condizionamento alcuno.	**Completamente applicato**	VEDI PUNTO A.2.4.1

A.2.4.7	Compiti del responsabile della protezione dei dati	*Controllo:* Verificare che il Responsabile della protezione dei dati (RPD), abbia regolarmente adempiuto alle indicazioni a lui ascritte, compresa la valutazione dei rischi inerenti il trattamento	**Completamente applicato**	VEDI PUNTO A.2.4.1
A.3 - PRINCIPI APPLICABILI AL TRATTAMENTO E TUTELA DEI DIRITTI				
A.3.1 Responsabilizzazione *Obiettivo: Assicurare la corretta applicazione dei principi di trattamento e di qualità dei dati*				**EVIDENZE - RILIEVI - NOTE**
A.3.1.1	Finalità del trattamento	*Controllo:* Verificare che i dati vengano utilizzati solo per finalità determinate, esplicite e legittime. Verificare inoltre che il trattamento di dati personali avvenga in modo trasparente nei confronti dell'interessato.	**Completamente applicato**	IL TRATTAMENTO DEI DATI PERSONALI E' EFFETTUATO I MODO LECITO E PER FINALITA' DETERMINATE; SONO STATE REDATTE E PUBBLICATE LE INFORMATIVE EX ARTT. 13 E 14 GDPR
A.3.1.2	Compatibilità della Finalità	*Controllo:* Verificare che, laddove il titolare svolga un trattamento con finalità diverse da quelle per le quali i dati sono stati inizialmente raccolti, le due finalità siano compatibili. Le aspettative ragionevoli dell'interessato, in base alla relazione con il titolare, rappresentano la base di compatibilità.	**Completamente applicato**	VEDI PUNTO A.3.1.1
A.3.1.3	Pertinenza del trattamento	*Controllo:* Verificare che i dati trattati siano funzionali alla finalità dichiarata e perseguita.	**Completamente applicato**	VEDI PUNTO A.3.1.1
A.3.1.4	Qualità ed esattezza dei dati	*Controllo:* Verificare la presenza di procedure per la valutazione, rettifica o cancellazione dei dati inesatti o non più funzionali rispetto alle finalità.	**Completamente applicato**	VEDI PUNTO A.3.1.1
A.3.1.5	Dati personali acquisiti da soggetti terzi	*Controllo:* Il titolare del trattamento di dati personali acquisiti da soggetti terzi, deve verificare se i dati in oggetto presentano le garanzie di conformità necessarie al GDPR. Il responsabile può comprovare la propria conformità al GDPR anche mediante l'adesione a codici di condotta o meccanismi di certificazione approvati	**Completamente applicato**	VEDI SEZIONE A.2.3
A.3.1.6	Misura della qualità dei dati	*Controllo:* Verificare se è stato elaborato un algoritmo per il monitoraggio della qualità dei dati personali per ogni singolo trattamento.	**Inapplicabile**	NON OBBLIGATORIO
A.3.1.7	Minimizzazione e limitazione dei dati personali raccolti	*Controllo:* Il titolare deve documentare l'impostazione predefinita per la minimizzazione dei dati raccolti, limitandone la quantità in relazione alla finalità.	**Completamente applicato**	E' STATO REDATTO UN MOP; DA REVISIONARE COSTANTEMENTE, COMPRESE LE PROCEDURE E VADEMECUM TRASMESSI.
A.3.1.8	Conservazione dei dati personali	*Controllo:* Verificare che il periodo di conservazione dei dati personali degli interessati sia limitato al minimo necessario per realizzare le finalità per cui sono trattati.	**Completamente applicato**	E' PRESENTE ED AGGIORNATO IL REGISTRO DELLE ATTIVITA' DEI TRATTAMENTI EX ART. 30 GDPR
A.3.1.9	Riesame delle politiche per la valutazione della qualità ed esattezza dei dati	*Controllo:* Deve essere riesaminata almeno annualmente la politica di gestione dell'esattezza dati, anche in sede di riesame della direzione.	**Completamente applicato**	E' PRESENTE UN SERVIZIO DI SUPPORTO SPECIALISTICO
A.3.1.10	Correttezza e trasparenza	*Controllo:* Verificare che il titolare del trattamento applichi in maniera fattuale i principi di correttezza e trasparenza, a prescindere dalla base giuridica e per tutto il ciclo di vita del trattamento.	**Completamente applicato**	VEDI PUNTO 3.1.1
A.3.1.11	Politiche a garanzia dell'Integrità e della riservatezza	*Controllo:* Verificare che il titolare del trattamento, per qualsiasi trattamento di dati personali che egli direttamente effettui o che altri effettuino per suo conto, **abbia elaborato politiche e linee guida** per garantire un'adeguata sicurezza e riservatezza. Le politiche devono essere documentate e integrate nel modello organizzativo.	**Parzialmente applicato**	E' STATO REDATTO ED APPLICATO UN MODELLO ORGANIZZATIO PRIVACY CON ANNESSE PROCEDURE, LINEE GUIDE E VADEMECUM.
A.3.2 Requisiti di liceità del trattamento dei dati personali *Obiettivo: Valutare la corretta base giuridica del trattamento*				**EVIDENZE - RILIEVI - NOTE**
A.3.2.1	Base giuridica e principi del trattamento	*Controllo:* Verificare che il trattamento di dati personali, sia lecito, corretto e trasparente per le persone fisiche e sia basato su una corretta base giuridica, chiaramente declinata e resa comprensibile all'interessato.	**Completamente applicato**	IL TRATTAMENTO DEI DATI PERSONALI E' EFFETTUATO I MODO LECITO E PER FINALITA' DETERMINATE; SONO REDATTE E PUBBLICATE LE INFORMATIVE AI SENSI DEGLI ARTT. 13 E 14 DEL GDPR
A.3.2.2	Consenso al trattamento	*Controllo:* Verificare che qualora la base giuridica del trattamento è basata sul consenso dell'interessato, il titolare e il responsabile abbiano pianificato una politica di acquisizione dei consensi.	**Completamente applicato**	DI NORMA I TRATTAMENTI EFFETTUATI NON SI BASANO SUL CONSENSO DELL'INTERESSATI, E' NECESSARIO VERIFICARE COSTANTEMENTE EVENTUALI TRATTAMENTI IN CUI NECESSITA L'ACQUISIZIONE DEL CONSENSO (EX ART. 6 C.1 LETT. A GDPR)
A.3.2.3	Revocabilità del consenso	*Controllo:* Verificare che quando l'interessato abbia prestato il consenso per un trattamento, possa revocarlo agevolmente in qualsiasi momento.	**Completamente applicato**	VEDI PUNTO A.3.2.3
A.3.2.4	Consenso differenziato	*Controllo:* Verificare che qualora il trattamento abbia più finalità, il consenso sia prestato per tutte le finalità rilevate.	**Completamente applicato**	VEDI PUNTO A.3.2.3
A.3.2.5	Consenso dei minori	*Controllo:* Verificare che nel caso vegano trattati dati personali di minori, il consenso sia prestato o autorizzato dal titolare della potestà genitoriale sul minore, in considerazione delle tecnologie disponibili	**Completamente applicato**	VEDI PUNTO A.3.2.3
A.3.2.6	Tracciabilità dei consensi	*Controllo:* Qualora il consenso costituisca la base giuridica del trattamento, deve essere predisposta una procedura al fine di verificare **che** l'interessato abbia prestato il suo consenso o lo abbia revocato	**Parzialmente applicato**	VEDI PUNTO A.3.2.3
A.3.2.7	Libertà di espressione del consenso	*Controllo:* Verificare che non esista un evidente squilibrio tra l'interessato e il titolare del trattamento, tale da mettere nell'impossibilità l'interessato di rifiutare il consenso senza subire un pregiudizio.	**Completamente applicato**	VEDI PUNTO A.3.2.3
A.3.2.8	Legittimo interesse e valutazione del bilanciamento	*Controllo:* Verificare che, ove la base giuridica del trattamento sia il legittimo interesse, il titolare abbia correttamente svolto un "**test di bilanciamento di interesse"** per verificare che non prevalgano gli interessi propri, sui diritti e le libertà dell'interessato.	**Completamente applicato**	E' PRESENTE IL REGISTRO DEI TRATTAMENTI
A.3.3 Informativa *Obiettivo: Valutare la conformità dell'informativa e nel rispetto dei principi di correttezza e trasparenza, le politiche di rilascio all'interessato*				**EVIDENZE - RILIEVI - NOTE**
A.3.3.1	Consegna e contenuto dell'informativa direttamente all'interessato	*Controllo:* Verificare che l'interessatosia correttamente informato dell'esistenza del trattamento e delle sue finalità e che siano soddisfatte le condizioni previste.	**Completamente applicato**	SONO REDATTE E PUBBLICATE LE INFORMATIVE AI SENSI DEGLI ARTT. 13 E 14 DEL GDPR
A.3.3.2	Informazioni acquisite da altra fonte	*Controllo:* Verificare che, qualora i dati siano stati ottenuti da altra fonte e non direttamente dall'interessato, il titolare abbia provveduto ad adempiere all'obbligo di informare l'interessato entro un mese dall'ottenimento dei dati.	**Completamente applicato**	VEDI PUNTO A.3.3.1

A.3.3.3	Requisiti dell'informativa	*Controllo:* Verificare che l'informativa rispetti i requisiti previsti dalle norme vigenti. Deve essere garantita la corretta informazione agli interessati.	**Completamente applicato**	VEDI PUNTO A.3.3.1
A.3.3.4	Esenzione dall'informativa	*Controllo:* Verificare se il caso di specie rientri nelle ipotesi di deroga all'obbligo di fornire l'informativa all'interessato.	**Completamente applicato**	VEDI PUNTO A.3.3.1
A.3.3.5	Informazioni intellegibili	*Controllo:* Verificare che l'informativa sia realmente comprensibile ai soggetti interessati a cui essa è rivolta. In particolare deve risultare comprensibile se i soggetti sono minori, pazienti o soggetti anziani.	**Completamente applicato**	VEDI PUNTO A.3.3.1
A.3.3.6	Informativa concisa	*Controllo:* Verificare che, seppur nel rispetto degli obblighi previsti, il titolare del trattamento presenti le informazioni/comunicazioni all'interessato, in maniera efficace e succinta al fine di evitare un sovraccarico informativo.	**Completamente applicato**	VEDI PUNTO A.3.3.1
A.3.3.7	Informativa trasparente	*Controllo:* Verificare che attraverso l'informativa, l'interessato sia realmente in condizione di imputare la responsabilità al titolare e di esercitare il controllo sui dati personali.	**Completamente applicato**	VEDI PUNTO A.3.3.1
A.3.4 Diritti dell'interessato Obiettivo: Valutare il corretto rispetto dell'esercizio dei diritti dell'interessato				**EVIDENZE - RILIEVI - NOTE**
A.3.4.1	Esercizio dei diritti dell'interessato	*Controllo:* Verificare che siano state predisposte adeguate procedure per raccogliere e catalogare le richieste di esercizio dei diritti degli interessati.	**Completamente applicato**	E' REDATTA UNA POLICY PER L'EVASIONE DEI DIRITTI GDPR E PUBBLICATA LA RELATIVA MODULISTICA (INTERNA ED ESTERNA), COMPRESO UN MODELLO PER L'INTERESSATO E UN REGISTRO INTERNO
A.3.4.2	Necessità di Riscontro	*Controllo:* Verificare che sia fornito all'interessato un riscontro al più tardi entro un mese; il titolare e il responsabile devono elaborare e documentare politiche adeguate allo scopo.	**Completamente applicato**	VEDI PUNTO A.3.4.2
A.3.4.3	Diritto di rettifica e diritto alla cancellazione (Oblio)	*Controllo:* Verificare che il titolare abbia attuato politiche adeguate per consentire all'interessato di ottenere la rettifica e l'eventuale cancellazione (oblio) dei dati personali che lo riguardano, qualora ne ricorrano le condizioni.	**Completamente applicato**	VEDI PUNTO A.3.4.2
A.3.4.4	Diritto alla portabilità	*Controllo:* Se i dati sono trattati con mezzi automatizzati, sono trattati in virtù del consenso dell'interessato o in base a contratto e sono stati da questo forniti al titolare, **verificare che** il titolare abbia predisposto idonee procedure per consentire all'interessato di ricevere i propri dati personali o di ottenerne il trasferimento ad altro titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico.	**Inapplicabile**	NON VI SONO CASISTICHE APPLICABILI AL DIRITTO DI CUI ALL'ART. 20 DEL GDPR
A.3.4.5	Diritto di limitazione del trattamento (cancellazione) dei dati dell'interessato, da parte del titolare	*Controllo:* Verificare che benché il titolare non abbia più bisogno dei dati dell'interessato, essendo venuta meno la finalità, al fine di evitare un **automatismo di cancellazione** da parte del titolare che potrebbe risultare pregiudizievole per l'interessato, l'interessato possa esercitare il diritto di limitazione del trattamento (cancellazione) ai fini probatori in sede giudiziaria. L'esercizio del diritto non è automatico ma deve giungere al titolare che deve dimostrare di aver adempiuto all'atto.	**Completamente applicato**	VEDI PUNTO A.3.4.1
A.3.5 Limitazione del trattamento *Obiettivo: Assicurare una corretta applicazione di diritti particolari*				**EVIDENZE - RILIEVI - NOTE**
A.3.5.1	Opposizione al trattamento	*Controllo:* Verificare che il titolare del trattamento attraverso idonee politiche aziendali, abbia messo in condizioni gli interessati, **di opporsi sia al trattamento iniziale** che quello ulteriore. Il controllo non si applica qualora il titolare dimostri motivi legittimi cogenti.	**Completamente applicato**	VEDI PUNTO A.3.4.2
A.3.5.2	Limitazione del trattamento	*Controllo:* Il titolare deve porsi nella condizione di recepire le istanze di limitazione del trattamento presentate dal soggetto interessato sui dati che lo riguardano, sussistendone i presupposti di legge. Verificare, pertanto, l'esistenza di procedure specifiche che ne consentano l'attuazione nonché la formazione del personale addetto.	**Completamente applicato**	VEDI PUNTO A.3.4.2
A.3.5.3	Diritto di opposizione al marketing diretto e alla profilazione	*Controllo:* Verificare che l'interessato possa correttamente e liberamente esercitare la volontà di non essere sottoposto ad attività di marketing diretto e ad una decisione basata unicamente sul trattamento automatizzato, compresa la **profilazione**, fatte salve le eccezioni previste dal regolamento.	**Inapplicabile**	NON PRESENTI
A.4 - PROCESSI DI ADEGUAMENTO IN FASE DI IDEAZIONE ED ALL'ATTO DEL TRATTAMENTO (privacy by design e by default)				
A.4.1 Tutela dei diritti sin dalla progettazione *Obiettivo: Dimostrare la conformità del titolare o del responsabile, se fornitore di un prodotto o servizio per il trattamento di dati personali, attraverso l'adozione di politiche interne a tutela dei dati personali sin dalla progettazione e della impostazione predefinita, nel rispetto del principio di trasparenza.*				**EVIDENZE - RILIEVI - NOTE**
A.4.1.1	Adozione delle politiche di tutela dei dati sin dalla progettazione	*Controllo:* Verificare che il titolare (o il responsabile in caso di progettazione, fornitura o erogazione di un prodotto/servizio), abbia adottato politiche interne aziendali, di protezione dei dati fin dalla progettazione. Le misure attuate devono tutelare i dati personali sia nella fase di progettazione dei prodotti e servizi che all'atto del trattamento.	**Parzialmente applicato**	SONO IMPOSTATE DELLE POLITICHE, AUTORIZZAZIONI, ISTRUZIONI E FORMAZIONE;
A.4.1.2	Politiche di monitoraggio della privacy by design e by default	*Controllo:* Verificare che il titolare (o il responsabile in caso di progettazione, fornitura o erogazione di un prodotto/servizio), sia dotato di un sistema di monitoraggio delle politiche adottate, affinché le stesse possano adeguarsi ai mutamenti tecnologici e all'insorgere di nuovi rischi.	**Parzialmente applicato**	E' PRESENTE UN SERVIZIO DI ASSISTENZA TECNOLOGICO, E' IMPOSTATO UN MOP E PREVISTI DEGLI AUDIT PERIODICI DI MONITORAGGIO;
A.4.1.3	Rischi per i diritti e le libertà degli interessati	*Controllo:* Verificare che il titolare (o il responsabile in caso di progettazione, fornitura o erogazione di un prodotto/servizio) abbia valutato adeguatamente i rischi per i diritti e le libertà degli interessati sia al momento di determinare i mezzi che all'atto del trattamento.	**Completamente applicato**	E' STATA EFFETTUATA L ANALISI DEI RISCHI E LA DPIA PER LA VIDEOSORVEGLIANZA
A.4.1.4	Impostazione minima predefinita	*Controllo:* Verificare che il titolare (o il responsabile in caso di progettazione, fornitura o erogazione di un prodotto/servizio) abbiano strutturato le relative operazioni in modo da rendere **minimo** il trattamento dei dati personali.	**Completamente applicato**	APPLICATO IL MOP
A.4.1.5	Gestione del rischio e delle politiche di protezione dei dati, da parte del Responsabile del trattamento, in fase di progettazione e sviluppo.	*Controllo:* Verificare se al titolare del trattamento può **configurare** e/o modificare le caratteristiche di sicurezza del prodotto o servizio fornito o erogato per adeguarlo alle proprie politiche di protezione dei dati e di mitigazione dei rischi.	**Completamente applicato**	APPLICATO IL MOP

A.4.1.6	Certificazione del processo di privacy by design e by default	*Controllo:* Verificare **se** il titolare (o il responsabile in caso di progettazione, fornitura o erogazione di un prodotto/servizio) abbia adottato un meccanismo di certificazioni ai sensi dell'art. 42 per dimostrare la conformità al regolamento generale.	**Inapplicabile**	NON E' OBBLIGATORIO
A.4.1.7	Valutazione in fase di selezione e utilizzo di un prodotto o servizio	*Controllo:* Verificare **che** in fase di selezione o già di utilizzo di un prodotto o servizio, il titolare abbia effettuato la selezione del prodotto o servizio valutando il rispetto dei principi di privacy by design.	**Completamente applicato**	SONO REDATTE APPOSITE PROCEDURE
A.4.1.8	Controllo da parte dell'interessato	*Controllo:* Verificare **che** l'interessato sia messo in condizione di **avere un reale controllo** sul trattamento dei propri dati, nell'ambito del prodotto o servizio.	**Completamente applicato**	VEDI PUNTO A.3.4.2
A.4.1.9	Trasparenza sulle funzioni del prodotto/servizio e sul trattamento dei dati personali	*Controllo:* Verificare **che**, fra le misure adottate dal responsabile del trattamento, sia offerta reale trasparenza agli interessati delle funzioni e del trattamento dei dati personali, mediante idonea documentazione resa accessibile. il titolare deve essere pienamente consapevole della conformità al trattamento.	**Completamente applicato**	E' PRESENTE UNA PROCEDURA PER LA DESIGNAZIONE DEI RESPONSABILI DEL TRATTAMENTO EX ART. 28 ED E' PRESENTE UN MOP
A.4.1.10	Appalti pubblici	*Controllo:* Nel caso in cui il titolare è una pubblica autorità, amministrazione o servizio, assoggettato ad appalti pubblici per forniture di prodotti e servizi, **verificare se** i principi di protezione dei dati fin dalla progettazione siano stati inseriti all'interno dei bandi di gara.	**Completamente applicato**	E' PRESENTE UNA PROCEDURA PER LA DESIGNAZIONE DEI RESPONSABILI DEL TRATTAMENTO EX ART. 28 ED E' PRESENTE UN MOP
A.5 – OBBLIGHI GENERALI, GESTIONE DEL RISCHIO E SICUREZZA DEI DATI PERSONALI				
A.5.1 – Mappatura e Registri del trattamento *Obiettivo: Censire e descrivere le caratteristiche fondamentali dell'attività del titolare o del responsabile del trattamento allo scopo di disporre di un quadro aggiornato dei trattamenti in essere.*				**EVIDENZE - RILIEVI - NOTE**
A.5.1.1	Mappatura delle categorie di attività di trattamento dei dati personali	*Controllo:* Verificare se sia stata predisposta una mappatura sistematica dei trattamenti dei dati personali. La mappatura dovrà avere un livello di dettaglio tale da consentire la verifica di quali siano le operazioni di trattamento per le quali ogni unità operativa può ritenersi responsabile e quali strumenti siano impiegati dalle stesse.	**Completamente applicato**	E' PRESENTE UNA MAPPATURA DEI TRATTAMENTI, E DI CONSEGUENZA E' PRESENTE IL REGISTRO DELLE ATTIVITA' (EX ART. 30 C.1 GDPR);
A.5.1.2	Predisposizione del registro dei trattamenti	*Controllo:* Verificare che il titolare e il responsabile abbiano redatto un registro del trattamento.	**Completamente applicato**	VEDI PUNTO A.5.1.2
A.5.1.3	Mancata redazione del registro	*Controllo:* Nel caso in cui ne ricorrano i presupposti e il titolare e il responsabile abbiano valutato la non necessità di redigere un registro, verificare che tale decisione sia coerente e adeguatamente documentata.	**Completamente applicato**	E' UN ADEMPIMENTO OBBLIGATORIO
A.5.1.4	Informazioni contenute nel registro del titolare	*Controllo:* Verificare che nel registro del titolare, siano presenti almeno le seguenti informazioni: - nome del titolare - dati di contatto del titolare o del contitolari e del DPO (se nominato) - finalità - descrizione delle categorie di interessati - descrizione delle categorie di dati personali - categorie di destinatari - trasferimento pressi paesi terzi, compreso l'identificazione e le adeguate garanzie - trasferimento presso un'organizzazione internazionale - termine ultimo per la cancellazione per le diverse categorie di dati - descrizione misure di sicurezza	**Completamente applicato**	VEDI PUNTO A.5.1.2 -
A.5.1.5	Valutazione del Registro del Responsabile	*Controllo:* Verificare che nel registro del Responsabile, siano presenti le almeno seguenti informazioni: - Il nome e i dati di contatto del responsabile/i di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento - Le categorie di trattamenti effettuate per conto di ogni titolare - I trasferimenti dei dati verso un paese terzo - L'identificazione del paese terzo e le adeguate garanzie - Descrizione delle misure di sicurezza adottate	**Completamente applicato**	ATTUALMENTE NON NECESSARIO (OVVERO IL TITOLARE NON FUNGE DA RESPONSABILE ART. 28 PER ALTRI TITOLARI)
A.5.1.6	Conservazione e accesso ai registri	*Controllo:* Verificare che le modalità di accesso ai registri in formato elettronico o di conservazione per quelli in formato cartaceo, siano dotate di controllo di accesso o verifica.	**Completamente applicato**	VEDI PUNTO A.5.1.2 (IL REGISTRO E' REPERIBILE SULL'AREA RISERVATA CREATA AD HOC DAL SERVIZIO DI SUPPORTO SPECIALISTICO, INOLTRE VERRA' ABILITATO UN SW APPLICATIVO MULTI-UTENTE)
A.5.2 Sicurezza del trattamento *Obiettivo: Assicurare che il titolare e il responsabile del trattamento operino in maniera da garantire un'adeguata sicurezza dei dati personali (per una corretta applicazione dei **controlli** i vedere il § 0.3 note 1 e 2).*				**EVIDENZE - RILIEVI - NOTE**
A.5.2.1	Misure di sicurezza	*Controllo:* Verificare che a seguito **della valutazione dei rischi,** il titolare e il responsabile del trattamento, abbiano adottato misure tecniche e organizzative adeguate e compatibili per impedire qualsiasi forma illecita di trattamento, garantendo l'Integrità, la confidenzialità, la disponibilità e resilienza dei sistemi che trattano i dati.	**Parzialmente applicato**	E' STATA EFFETTUATA/DOCUMENTATA UN'ANALISI DEI RISCHI, E' PRESENTE UN MOP; VA IMPLEMENTATA TALE ANALISI
A.5.2.2	Prevenzione della perdita dei dati personali	*Controllo:* Verificare gli strumenti e le procedure adottate per prevenire la perdita di dati personali.	**Parzialmente applicato**	VEDI PUNTO A.5.2.1
A.5.2.3	Amministratori di Sistema	*Controllo:* Verificare la misure e le cautele adottate dal titolare e dal responsabile del trattamento nel controllare le attività svolte dagli amministratori di sistema.	**Inapplicabile**	NON E' OBBLIGATORIO
A.5.2.4	Violazione dei dati personali (Data Breaches)	*Controllo:* Verificare **che** siano state redatte dal titolare del trattamento adeguate **politiche e procedure** per la corretta gestione delle violazioni di dati personali Nel caso di responsabili del trattamento, verificare la presenza di politiche di segnalazione e collaborazione con il titolare per la corretta gestione degli incidenti.	**Completamente applicato**	E' PRESENTE UNA POLICY DATA BREACH
A.5.2.5	Registro delle violazioni (Data Breaches)	*Controllo:* Verificare **se** il titolare ha predisposto un registro delle violazioni dove riportare le segnalazioni che, secondo il principio di responsabilizzazione, ritiene improbabile presentino un **rischio** per i diritti e le libertà.	**Completamente applicato**	VEDI PUNTO A.5.2.4

A.5.2.6	Notifica delle violazioni (Data Breaches)	*Controllo:* Verificare che il titolare, in caso di violazione di dati personali, abbia predisposto idonee politiche di notificazione entro i termini previsti. In caso di mancata notificazione, verificare che dall'analisi della determinazione della **probabilità** il rischio per i diritti e le libertà dell'interessato **non risulti elevato**.	**Completamente applicato**	VEDI PUNTO A.5.2.4
A.5.2.7	Comunicazioni all'interessato delle violazioni (Data Breaches)	*Controllo:* Verificare che qualora la violazione sia suscettibile di presentare un **rischio elevato** per i diritti e le libertà dell'interessato, quest'ultimo venga correttamente informato, salvo non ricorrano le condizioni di esclusione previste dal regolamento generale.	**Completamente applicato**	VEDI PUNTO A.5.2.4
A.5.3 – Misure organizzative per la protezione dei dati personali *Obiettivo: Stabilire se il titolare e/o il responsabile hanno adottato le politiche **adeguate**, per garantire l'applicazione dei principi di protezione dei dati personali, compresa la formazione, tenendo conto della gestione del rischio.*				**EVIDENZE - RILIEVI - NOTE**
A.5.3.1	Impegni del titolare e del responsabile del trattamento per la sicurezza dei dati personali	*Controllo:* Verificare che il titolare e il responsabile del trattamento abbiano redatto politiche e procedure per informare, monitorare e dimostrare, il supporto attivo di una politica di gestione della sicurezza del trattamento dei dati personali.	**Completamente applicato**	VEDI SEZIONE A.2.3
A.5.3.2	Coordinamento per le politiche della sicurezza	*Controllo:* Il titolare ed il responsabile del trattamento deve strutturare un **modello organizzativo** con figure e ruoli, operativi e di coordinamento nell'ambito della sicurezza. Devono essere effettuate riunioni di coordinamento per l'attuazione delle procedure di controllo stabilite, con cadenza regolare. almeno annuale.	**Completamente applicato**	VEDI SEZIONE A.2.3
A.5.3.3	Valutazione del rischio	*Controllo:* Il titolare ed il responsabile del trattamento devono redigere un documento di valutazione del rischio del trattamento che riporti l'identificazione, l'analisi, la ponderazione, il trattamento del rischio stesso.	**Parzialmente applicato**	E' STATA SVOLTA/DOCUMENTATA UN'ANALISI DEI RISCHI, VA AGGIONATA E MIGLIORATA SUL PIANO INFORMATICO
A.5.3.4	Identificazione del rischio e calcolo del rischio accettabile	*Controllo:* Nell'identificazione dei rischi, deve essere valutato se il rischio incombe su uno o più trattamenti o su parti di esso e, se del caso, descrivere quali. Verificare se il titolare e il responsabile abbiano definito per ogni singolo trattamento il livello di rischio accettabile **(Ra)**	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.5	Modello per la rappresentazione della valutazione dei rischi inerenti	*Controllo:* Il modello analitico di rappresentazione del rischio inerente **(RI)** deve prevedere dei criteri di misurazione oggettiva. Verificare la reale coerenza del modello e dei criteri di rischio sulla base della tipologia di struttura e dei trattamenti svolti.	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.6	Ponderazione del rischio	*Controllo:* Verificare che, a seguito di un processo di analisi, Il titolare ed il responsabile del trattamento confrontino il livello di rischio inerente con il rischio accettabile al fine di garantire un livello di sicurezza del trattamento, adeguato al rischio.	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.7	Trattamento e mitigazione del rischio	*Controllo:* Nel caso in cui i criteri utilizzati evidenzino un rischio inerente superiore al rischio accettabile, Il titolare ed il responsabile del trattamento devono attuare misure tecniche e organizzative che riducano il livello di rischio. Verificare **che** le mitigazioni dei rischi attuate siano sostenibili e coerenti con i risultati previsti.	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.8	Consapevolezza del rischio da parte del personale della struttura operativa	*Controllo:* Il titolare e il responsabile del trattamento devono assicurarsi che tutto il personale della struttura di riferimento abbia una corretta percezione del rischio rispetto al trattamento dei dati personali.	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.9	Rischio residuo	*Controllo:* Verificare che il rischio residuo, risultante dalle operazioni di mitigazione, sia coerente con le politiche identificate dal titolare pertanto minore del rischio accettabile.	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.10	Riesame del rischio residuo	*Controllo:* Il titolare o il responsabile del trattamento devono pianificare, in modo regolare, un processo di sorveglianza dei rischi.	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.11	Registro dei rischi	*Controllo:* Verificare se il titolare ed il responsabile del trattamento abbiano redatto un registro dei rischi con cui monitorare l'incremento o il decremento del livello di rischio per ogni trattamento	**Parzialmente applicato**	VEDI PUNTO A.5.3.3
A.5.3.12	Formazione	*Controllo:* Verificare **che** il titolare e il responsabile attuino piani formativi periodici ai propri autorizzati, **adeguati** al livello di rischio.	**Completamente applicato**	E' STATA SVOLTA LA FORMAZIONE DEGLI AUTORIZZATI
A.5.4 – Misure tecniche per la protezione dei dati personali *Obiettivo: Assicurare la corretta applicazione di misure tecniche adeguate per verificare e valutare se le politiche adottate garantiscano la sicurezza del trattamento.*				**EVIDENZE - RILIEVI - NOTE**
A.5.4.1	Protezione del trattamento	*Controllo:* Verificare se il trattamento è stato progettato per rispondere ai requisiti di contesto e finalità definiti dal trattamento.	**Completamente applicato**	E' STATA SVOLTA/DOCUMENTATA UN'ANALISI DEI RISCHI, E' PRESENTE UN MOP, E' STATA ESEGUITA LA FORMAZIONE DEGLI AUTORIZZATI. N.B.: E' PRESENTE UN AFFIDAMENTO PER LA MANUTENZIONE E ASSISTENZA DELL'INFRASTRUTTURA DI RETE
A.5.4.2	Pseudonimizzazione dei dati	*Controllo:* Verificare **che,** il titolare e il responsabile del trattamento, abbiano previsto la pseudonimizzazione dei dati personali, in modo particolare nei nuovi prodotti informatici progettati by design e che la tabella di transcodifica degli stessi sia conservata separatamente, adottando misure adeguate ai rischi. In caso negativo deve essere prevista una procedura per l'integrazione quanto più rapida possibile.	**Completamente applicato**	VEDI PUNTO A.5.4.1
A.5.4.3	Cifratura dei dati	*Controllo:* Verificare, ove applicabile, che il titolare e il responsabile abbia pianificato, descritto e adottato algoritmi di cifratura per garantire un livello di sicurezza adeguato al rischio.	**Completamente applicato**	VEDI PUNTO A.5.4.1
A.5.4.4	Limitazione di accesso ai dati personali	*Controllo:* Verificare **che** i dati personali oggetto del trattamento siano accessibili solo mediante accesso controllato e definito per impostazione predefinita lungo tutta la filiera del trattamento.	**Completamente applicato**	VEDI PUNTO A.5.4.1
A.5.4.5	Standard internazionali a presidio della Riservatezza Integrità e disponibilità	*Controllo:* Verificare se Il titolare e il responsabile del trattamento, per il rispetto dei presupposti di integrità, riservatezza e disponibilità delle informazioni, si basino su standard e/o le migliori prassi internazionali per il loro presidio.	**Completamente applicato**	VEDI PUNTO A.5.4.1

A.5.4.6	Anonimizzazione dei dati	*Controllo:* Verificare se il titolare e il responsabile del trattamento abbiano predisposto politiche e procedure per eliminare la correlazione tra i dati personali e una determinata persona fisica interessata (de-identificazione), rendendo impossibile l'identificazione della stessa.	**Completamente applicato**	VEDI PUNTO A.5.4.1
A.6 - VALUTAZIONE D'IMPATTO				
A.6.1 Necessità e metodologie per lo svolgimento della Valutazione d'Impatto (DPIA) *Obiettivo: Assicurare il rispetto del regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche.*				**EVIDENZE - RILIEVI - NOTE**
A.6.1.1	Svolgimento della Valutazione d'impatto	*Controllo:* Verificare che il titolare e il responsabile del trattamento abbiano efficacemente analizzato e documentato la scelta di effettuare o di non effettuare una valutazione d'impatto prima di procedere al trattamento.	**Completamente applicato**	E' STATA SVOLTA/DOCUMENTATA UN'ANALISI DEI RISCHI, E' PRESENTE UNA POLICY/LINEE GUIDA PER LA REDAZIONE DI UNA DPIA,E' PRESENTE UN REGISTRO DEI TRATTAMENTI E DI CONSEGUNZA UN MOP. E' STATA SVOLTA LA DPIA SUI SISTEMI DI VIDEOSORVEGLIANZA E SUL WHISTLEBLOWING
A.6.1.2	Supporto del Responsabile della protezione dei dati	*Controllo:* Verificare che al momento dello svolgimento della Valutazione d'Impatto (DPIA), il titolare si sia consultato con il DPO qualora designato. Tale consultazione e conseguenti decisioni devono avere un'evidenza scritta.	**Completamente applicato**	VEDI PUNTO A.6.1.1
A.6.1.3	Opinioni degli interessati o dei loro rappresentanti	*Controllo:* Verificare che il titolare e il responsabile del trattamento, ove ne ricorrano i presupposti, abbia consultato o meno, gli interessati o i loro rappresentanti.	**Completamente applicato**	VEDI PUNTO A.6.1.1
A.6.1.4	Esaustività della forma	*Controllo:* Verificare che nel documento di DPIA relativo al trattamento sia descritto in maniera chiara ed esaustiva almeno il contenuto minimo richiesto dal regolamento.	**Completamente applicato**	VEDI PUNTO A.6.1.1
A.6.1.5	Consequenzialità e integrazione documentale fra Valutazione del rischio e DPIA	*Controllo:* Verificare che la Valutazione d'Impatto venga effettuato oltre che nei casi previsti del Regolamento, ogni volta che da una valutazione oggettiva e misurabile evidenzi un rischio elevato per ogni trattamento o per gruppi di trattamenti simili.	**Completamente applicato**	VEDI PUNTO A.6.1.1
A.6.1.6	Riesame programmato e costante della DPIA	*Controllo:* Verificare che il titolare proceda a riesami regolari e costanti della DPIA, per valutare se i trattamenti siano effettuati conformemente, o allorquando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.	**Completamente applicato**	VEDI PUNTO A.6.1.1
A.6.1.7	Pubblicazione della DPIA	*Controllo:* Verificare se il titolare ha pubblicato una sintesi o un estratto delle conclusioni della valutazione d'impatto, nel rispetto dei segreti industriali.	**Completamente applicato**	VEDI PUNTO A.6.1.1
A.7 TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI E CLOUD COMPUTING				
A.7.1 Corretta modalità di trasferimento dei dati fuori dall'EU *Obiettivo: Valutare la conformità delle modalità adottate per trasferire i dati fuori dall'UE*				**EVIDENZE - RILIEVI - NOTE**
A.7.1.1	Trasferimento di dati personali verso un paese terzo	*Controllo:* Nel caso di trasferimento dei dati verso paesi extra EU, verificare che il titolare abbia rispettato le condizioni previste dal regolamento, conducendo preliminarmente tutte le valutazioni necessarie e che le stesse siano documentate.	**Completamente applicato**	E' PRESENTE IL REGISTRO DEI TRATTAMENTI, E' PRESENTE UNA MAPPATURA DEI RESPONSABILI DEL TRATTAMENTO ART. 28. N.B.: PER LE ATTIVITA' SVOLTE DAL TITOLARE DI NORMA NON VENGONO TRASFERITI DATI FUORI DALL'UE (SALVO I CASI DI COMUNICAZIONE OBBLIGATORIA AD AUTONOMI TITOLARI DEL TRATTAMENTO)
A.7.1.2	Trasferimento in base a garanzie adeguate	*Controllo:* Quando un trasferimento di dati personali avviene fuori dall'unione europea e tale trasferimento avviene in base a garanzie adeguate, verificare che l'applicazione effettiva delle garanzie, sia adeguatamente verificata.	**Completamente applicato**	VEDI PUNTO A.7.1.2
A.7.1.3	Trasferimento in base alle Norme vincolanti d'impresa (BCR)	*Controllo:* Verificare che il titolare e il responsabile del trattamento siano dotatati di adeguati meccanismi di vigilanza sul rispetto - suo e degli altri membri del medesimo gruppo imprenditoriale non stabiliti nel territorio dell'Unione - dei vincoli assunti mediante le Norme Vincolanti d'Impresa sottoscritte da tutti i membri interessati del gruppo di imprese, compresi i loro dipendenti.	**Completamente applicato**	VEDI PUNTO A.7.1.2
A.7.1.4	Ruolo del DPO nelle Norme vincolanti d'Impresa	*Controllo:* Verificare i compiti e il ruolo attribuito al DPO nelle norme vincolanti di impresa.	**Completamente applicato**	VEDI PUNTO A.7.1.2
A.7.1.5	Clausole contrattuali ad hoc	*Controllo:* Al di fuori del ricorso a modelli contrattuali approvati dalla Commissione UE oppure ad accordi amministrativi stipulati fra autorità pubbliche, nel caso in cui il titolare del trattamento desidera utilizzare clausole, verificare che tali clausole siano oggetto di approvazione da parte della competente autorità di supervisione (es. BCR).	**Completamente applicato**	VEDI PUNTO A.7.1.2
A.7.1.6	Deroghe particolari	*Controllo:* In caso di trasferimenti di dati personali in paesi extra UE, in deroga agli artt. 45, 46 e 47, verificare se le condizioni individuate dal titolare siano correttamente impostate e applicate e se è presente una procedura adeguata.	**Completamente applicato**	VEDI PUNTO A.7.1.2
A.7.2 Corretta gestione del cloud *Obiettivo: Gestione dei dati personali su Cloud computing*				**EVIDENZE - RILIEVI - NOTE**
A.7.2.1	Ponderazione dei rischi e dei benefici dell'utilizzo del cloud	*Controllo:* Verificare che il titolare e il responsabile del trattamento abbiano effettuato una approfondita comparazione fra rischi e benefici per il suo impiego. La valutazione deve limitare le tipologie di dati da conservare in cloud in relazione al rischio.	**Completamente applicato**	E' PRESENTE UN REGISTRO DEI TRATTAMENTI, E' PRESENTE UNA MAPPATURA DEI RESPONSABILI DEL TRATTAMENTO ART. 28. N.B.: E' PRESENTE UN AFFIDAMENTO PER LA MANUTENZIONE E ASSISTENZA DELL'INFRASTRUTTURA DI RETE. DA REVISIONARE L'ANALISI DEI RISCHI
A.7.2.2	Affidabilità del fornitore di cloud computing	*Controllo:* Verificare che il titolare e il responsabile abbia constatato le garanzie di capacità e affidabilità del fornitore, unitamente alle misure adottate per garantire la confidenzialità dei dati e la continuità operativa.	**Completamente applicato**	VEDI PUNTO A.7.2.1
A.7.2.3	Residenza fisica dei server	*Controllo:* Verificare che il titolare e il responsabile sia a conoscenza di dove risiedano fisicamente i server e che abbia constatato che il trasferimento dei dati fra diversi paesi sia tutelato dalle misure di salvaguardia prescritte dal regolamento.	**Completamente applicato**	VEDI PUNTO A.7.2.1
A.7.2.4	Clausole contrattuali	*Controllo:* Valutare se e come verificare che il titolare e il responsabile abbia verificato l'idoneità delle condizioni contrattuali per l'erogazione dei servizi di cloud computing, in particolare riguardo la previsione di garanzie in materia di dati personali.	**Completamente applicato**	VEDI PUNTO A.7.2.1
A.7.2.5	Tempi di persistenza dei dati	*Controllo:* Verificare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati.	**Completamente applicato**	VEDI PUNTO A.7.2.1

A.7.2.6	Sicurezza del servizio utilizzato	*Controllo:* Verificare che il titolare e il responsabile, prima di adottare il servizio di cloud computing, abbia valutato le misure di sicurezza adottate dal fornitore del servizio.	**Completamente applicato**	VEDI PUNTO A.7.2.1
A.7.2.7	Personale preposto all'uso del cloud computing	*Controllo:* Verificare che il personale aziendale preposto all'utilizzo del cloud sia stato autorizzato, ricevuto istruzioni e sottoposto a specifiche attività formative, documentate.	**Completamente applicato**	