VALUTAZIONE DEL RISCHIO E MISURE DI SICUREZZA PER I DATI PERSONALI

Valutazione del livello di rischio per l'operazione di trattamento **realizzazione di prodotti multimediali da inserire su sito RAS e social media per promuovere le attività di Iscol@** e proposta di misure di sicurezza tecniche e organizzative appropriate.

Sezione I – Definizione e contesto dell'operazione di trattamento

DESCRIZIONE DELL'OPERAZIONE DI TRATTAMENTO	RISPOSTA	
Dati personali oggetto di trattamento	immagini	
Finalità del trattamento	promozione Unità di progetto iscol@ della Regione Autonoma della Sardegna	
Soggetti interessati	cittadini, alunni, insegnanti, ATA, liberi professionisti, genitori	
Strumenti impiegati nel trattamento	droni, macchine fotografiche, cineprese	
Destinatari dei dati	Interni	Dipendenti RAS
	Esterni	cittadini ed amministrazioni pubbliche locali
Responsabile del trattamento	Alessandra Berry	

Sezione II – Valutazione dell'impatto

Riservatezza impact assessment: Basso

Dati personali pubblicati su un forum internet o su un sito P2P (peer to peer)

Integrità impact assessment: Basso

Disponibilità impact assessment: Basso

VALUTAZIONE DELL'IMPATTO		
Riservatezza	**Integrità**	**Disponibilità**
Basso	Basso	Basso
	Valutazione globale di impatto	Basso

Sezione III – Analisi delle minacce per area di valutazione

Risorse di rete e tecniche threat probability: Medio

- **Qualche parte del trattamento dei dati personali viene eseguita tramite Internet? Sì**
  promozione on line delle attività di iscol@ dove sono ripresi gli alunni ed insegnanti o altro soggetto che popola la scuola
- **È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)? Sì**
  i filmati saranno inseriti nel sito RAS e altro social media
- **Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)? Sì**
  i filmati saranno inseriti nel sito RAS e altro social media
- **Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati? Sì**
  esternalizzazione realizzazione prodotto multimediale
- **Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi? Sì**
  tencologie on line

Processi / Procedure relativi all'operazione di trattamento dei dati threat probability: Medio

- **I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti? No**
  sono tutti identificati
- **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito? No**
  no
- **I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali? Sì**
  se il prodotto multimediale è on line certamente ogniuno pyò usare il proprio computer
- **I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione? No**
  i datii in origine no
- **Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro (es: log)? No**
  chi ha accesso ai dati originali è ben identificato

Parti / Persone coinvolte nel trattamento dei dati personali threat probability: Medio

- **Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti? Sì**
  i filmati e foto saranno on line
- **Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)? Sì**
  i filmati saranno on line
- **Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti? -**
  non esistyono ambiguità

- **Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni? Sì**
  tutti conoscono il problema privacy
- **Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali? No**
  alla fine dei 5 anni dalla pubblicazione i filmati e foto saranno distrutte

Settore di operatività e scala di trattamento threat probability: Medio

- **Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici? No**
  non si prevedono minacce
- **La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni? No**
  non ci sono stati attacchi informatici
- **Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno? No**
  non ci sono stati reclami
- **Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali? Sì**
  il sito RAS avrà molti utenti
- **Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite? No**
  non esistono best paraticts

AREA DI VALUTAZIONE	PROBABILITA	
Risorse di rete e tecniche	Medio	2
Processi / Procedure relativi all'operazione di trattamento dei dati	Medio	2
Parti / Persone coinvolte nel trattamento dei dati personali	Medio	2
Settore di operatività e scala di trattamento	Medio	2
Livello globale di probabilità di occorrenza della minaccia	Medio (8)	

Sezione IV – Valutazione del rischio

	LIVELLO DI IMPATTO			
PROBABILITÀ DI OCCORRENZA DELLA MINACCIA		Basso	Medio	Alto / Molto Alto
	Basso			
	Medio	X		
	Alto			

Sezione V – Misure di sicurezza organizzative

Va notato che l'abbinamento di misure a specifici livelli di rischio non dovrebbe essere percepito come assoluto. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare l'adozione di misure aggiuntive, anche se sono assegnate a un livello di rischio più elevato. Inoltre, l'elenco proposto di misure non tiene conto di altri requisiti di sicurezza specifici settoriali aggiunti, nonché di obblighi normativi specifici, derivanti ad esempio dalla direttiva e-privacy o dalla direttiva NIS. Nel tentativo di facilitare ulteriormente questa procedura è inclusa anche una mappatura del gruppo di misure proposto con i controlli di sicurezza ISO/IEC 27001:2013.

Politica di sicurezza e procedure per la protezione dei dati personali

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
A.1	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	
A.2	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	
	Pertinente alla certificazione ISO 27001:2013 - A.5 Politica di sicurezza	

Ruoli e responsabilità

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	
B.2	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	
	Pertinente alla certificazione ISO 27001:2013 - A.6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni	

Politica di controllo degli accessi

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
C.1	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	
	Pertinente alla certificazione ISO 27001:2013 - A.9.1.1 Politica di controllo degli accessi	

Gestione risorse/asset

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
D.1	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	
D.2	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	
	Pertinente alla certificazione ISO 27001:2013 - A.8 Gestione delle risorse	

Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
E.1	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	
E.2	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	
	Pertinente alla certificazione ISO 27001:2013 - A. 12.1 Procedure operative e responsabilità	

Responsabili del trattamento

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	
F.2	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	
F.3	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	
	Pertinente alla certificazione ISO 27001:2013 - A.15 Rapporti con i fornitori	

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
G.1	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	
G.2	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna.. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	
	Pertinente alla certificazione ISO 27001:2013 - A.16 Gestione degli incidenti di sicurezza delle informazioni	

Business continuity

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
H.1	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	
	Pertinente alla certificazione ISO 27001:2013 - A. 17 Aspetti di sicurezza nella gestione della continuità operativa	

Obblighi di confidenzialità imposti al personale

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
I.1	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.	
	Pertinente alla certificazione ISO 27001:2013 - A.7 Sicurezza delle risorse umane	

Formazione

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
J.1	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	
	Pertinente alla certificazione ISO 27001:2013 - A.7.2.2 Consapevolezza, educazione e formazione sulla sicurezza delle informazioni	

Controllo degli accessi e autenticazione

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	
K.2	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	
K.3	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	
K.4	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	
	Pertinente alla certificazione ISO 27001:2013 - A.9 Controllo degli accessi	

Generazione di file di log e monitoraggio

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
L.1	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	
L.2	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.	
	Pertinente alla certificazione ISO 27001:2013 - A.12.4 Generazione di file di log e monitoraggio	

Sicurezza di server e database

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
M.1	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	
M.2	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).	
	Pertinente alla certificazione ISO 27001:2013 - A. 12 Sicurezza delle operazioni	

Sicurezza delle Postazioni di lavoro

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
N.1	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	
N.2	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	
N.3	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
N.4	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	
N.5	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	
	Pertinente alla certificazione ISO 27001:2013 - A. 14.1 Requisiti di sicurezza dei sistemi informativi	

Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
O.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)	
	Pertinente alla certificazione ISO 27001:2013 - A.13 Sicurezza delle comunicazioni	

Back-ups

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
P.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	
P.2	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	
P.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	
P.4	I backup completi devono essere eseguiti regolarmente.	
	Pertinente alla certificazione ISO 27001:2013 - A.12.3 Back-Up	

Dispositivi mobili / portatili

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
Q.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	
Q.2	I dispositivi mobili, ai quali è consentito accedere al sistema informativo, dovrebbero essere pre-registrati e pre-autorizzati.	
Q.3	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	
	Pertinente alla certificazione ISO 27001:2013 - A. 6.2 Dispositivi mobili e telelavoro	

Sicurezza del ciclo di vita delle applicazioni

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
R.1	Durante il ciclo di vita dello sviluppo, dovrebbero essere seguite le best practice, lo stato dell'arte e ben noti pratiche di sviluppo sicuro, framework o standard.	
R.2	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	
R.3	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
R.4	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	
R.5	Durante le attività di sviluppo, dovrebbero essere eseguite attività di test e convalida dei requisiti di sicurezza inizialmente implementati.	
	Pertinente alla certificazione ISO 27001:2013 - A. 12.6 Gestione delle vulnerabilità tecniche e A. 14.2 Sicurezza nei processi di sviluppo e supporto	

Cancellazione / eliminazione dei dati

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
S.1	La sovrascrittura software dei dati dovrebbe essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), è necessario eseguire la distruzione fisica.	
S.2	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	
	Pertinente alla certificazione ISO 27001:2013 - A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura	

Sicurezza fisica

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
T.1	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	
	Pertinente alla certificazione ISO 27001:2013 - A.11 Sicurezza fisica e ambientale	