

	 ISTITUTO COMPRENSIVO AMANTEA CAMPORA – AIELLO CALABRO Infanzia – Primaria - Secondaria di I° grado Cod. Mecc. CSIC81800B – C.F. 86002270782 Sede Amministrativa Via delle Ginestre, snc - 87032 Campora S. Giovanni (Amantea) Tel/Fax 0982.46232 e-mail : csic81800b@istruzione.it PEC : csic81800b@pec.istruzione.it Codice IPA: icca– cod.fatt. UFKHDM - Sito WEB ISTITUTO _ http://www.comprensivocampora-aiello.edu.it/ Con SEZ. ASSOCIATE : CSAA818018 AMANTEA CAMPORA - CSAA818029 AIELLO C. - CSAA81804B CLETO CSEE81801D AMANTEA CAMPORA - CSEE81803G AIELLO C. - CSEE81804L CLETO CSMM81801C AMANTEA CAMPORA - CSMM81802D AIELLO C. - CSMM81803E CLETO	
--	--	---

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA*) PER L'ADOZIONE DEL LAVORO AGILE/LAVORO DA REMOTO

Titolare del Trattamento: Ente in intestazione

Responsabile della Valutazione: Giuseppe Cavallo

Posizione: Dirigente Scolastico

Responsabile Protezione Dati: Dott.ssa Anna CIMA

**DPIA realizzata in parte sulla base del modello messo a disposizione dalla CNIL (Autorità francese per la protezione dei dati) e tradotta in italiano con la collaborazione del Garante per la protezione dei dati. La Valutazione è stata redatta con il supporto del DPO di questo Istituto.*

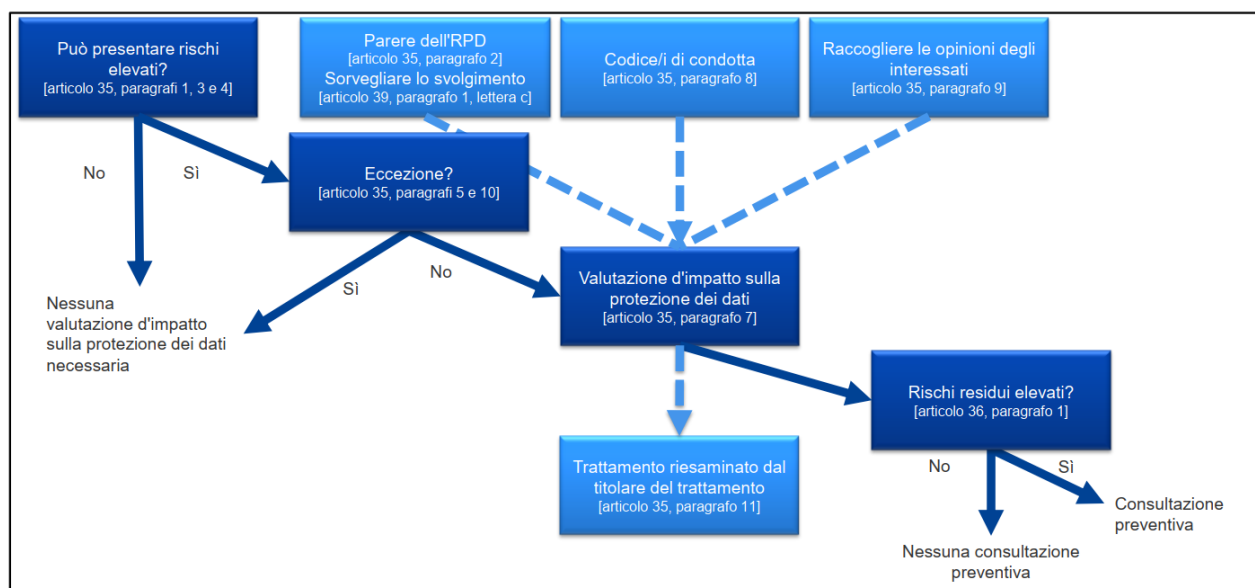
Oggetto della DPIA

Adozione del Lavoro Agile – Lavoro da remoto da parte del personale scolastico ATA dell'istituzione scolastica, ai sensi della L. 81/2017 e delle disposizioni normative successive, incluse quelle emanate in materia di pubblica amministrazione (D.L. 77/2021, Direttiva Min. PA n. 2/2020, Direttiva Min. PA n. 2/2022, L. 34/2026).

Introduzione e motivi della DPIA

La DPIA (Data Protection Impact Assessment), è una valutazione preliminare eseguita dal titolare del trattamento dei dati personali, relativa agli impatti e ai rischi determinati da un determinato trattamento dati.

Secondo il GDPR, non è necessario/obbligatorio svolgere una valutazione d'impatto per ciascun trattamento, ma solo per quelli che "possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35 Regolamento UE 2016/679)..



I criteri da prendere in considerazione per l'obbligo della DPIA (secondo il Gruppo art.29 "Comitato Europeo della protezione dei dati") sono i seguenti:

- Profilazione
- Decisioni automatizzate che producono significativi effetti giuridici
- Monitoraggio sistematico
- Trattamenti di dati sensibili, giudiziari o di natura estremamente personale
- Trattamenti di dati personali su larga scala
- Dati relativi a soggetti vulnerabili
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
- Trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto

In presenza di almeno due di questi criteri, la DPIA è necessaria.

Il lavoro agile nelle istituzioni scolastiche introduce nuove modalità di trattamento dati che coinvolgono personale dipendente, strumenti digitali remoti, sistemi di comunicazione a distanza e potenzialmente dati relativi ad alunni e famiglie trattati al di fuori della sede fisica dell'istituto. Tale scenario rientra in almeno due dei criteri sopra elencati (monitoraggio sistematico e utilizzo di nuove soluzioni tecnologiche/organizzative), rendendo la DPIA necessaria. Il presente Titolare ha ritenuto utile redigere la DPIA in considerazione delle specificità del contesto scolastico e delle indicazioni fornite dal MIM, dal Garante privacy e dal DPO dell'Istituto.

Contesto e descrizione del trattamento

L'introduzione del lavoro agile nel contesto scolastico comporta una trasformazione significativa delle modalità operative attraverso cui vengono trattati i dati personali. Le attività, tradizionalmente svolte all'interno dell'istituzione, vengono in parte delocalizzate, con accesso ai sistemi informativi da ambienti esterni, prevalentemente domestici.

Il trattamento non si caratterizza per nuove finalità, ma per una diversa modalità esecutiva delle stesse. Le attività interessate riguardano principalmente la gestione amministrativa, documentale e organizzativa della scuola, con possibile coinvolgimento anche di attività di supporto alla didattica.

I flussi informativi si sviluppano attraverso:

- accesso a piattaforme cloud istituzionali;
- collegamento a sistemi locali della scuola;
- utilizzo di strumenti di comunicazione e condivisione.

Questa configurazione determina un elemento di criticità strutturale: il trattamento avviene in ambienti che sfuggono al controllo diretto del titolare, con conseguente incremento dell'esposizione al rischio.

Processo di valutazione

Il processo che porta alla valutazione del rischio prevede alcune fasi, così riassunte:

Fase 1: identificazione dei trattamenti

Consiste nell'individuare tutti gli elementi del trattamento dati:

- Tipologia di dati
- Finalità
- Categorie di interessati
- Modalità di trattamento
- Misure tecniche/organizzative
- Destinatari
- Eventuale trasferimento extra UE (nel caso è necessario effettuare anche la TIA)

Fase 2: Panoramica dei rischi

Vengono individuati i potenziali rischi, cioè la probabilità con cui un evento dannoso possa verificarsi, e le relative conseguenze, determinando una scala di probabilità del rischio che va da "improbabile" a "quasi certo" e una scala di incidenza delle conseguenze che va da "trascurabili" a "gravissime".

Fase 3: Valutazione del rischio ed eventuali misure correttive

Si valutano rischi e conseguenze, determinando l'esito della DPIA.

Informazioni preliminari e descrizione del trattamento

Finalità: Il trattamento oggetto della presente valutazione si colloca nell'ambito delle attività istituzionali proprie dell'istituzione scolastica e si caratterizza per il fatto di essere svolto, in tutto o in parte, mediante modalità di lavoro agile. Le **finalità** perseguite non risultano nuove rispetto a **quelle già proprie dell'amministrazione**, ma si identificano nella necessità di garantire la continuità e l'efficienza dell'azione amministrativa e organizzativa della scuola, nonché il corretto svolgimento delle attività di supporto alla didattica e alla gestione del servizio scolastico. In tale prospettiva, **il trattamento è funzionale all'esecuzione di compiti di interesse pubblico** e alla gestione del rapporto di lavoro con il personale dipendente.

- Gestione e documentazione delle attività lavorative svolte in modalità agile
- Monitoraggio della presenza e della reperibilità del personale in lavoro agile
- Erogazione di servizi amministrativi e didattici da remoto
- Comunicazioni istituzionali tra personale, famiglie e dirigenza
- Accesso a piattaforme e sistemi informativi dell'istituto da postazione remota
- Gestione delle istanze e dei procedimenti amministrativi in modalità digitale
- Eventuale supporto per l'erogazione di attività didattiche a distanza (DAD/DID)

Parere degli interessati: in relazione al coinvolgimento degli interessati, non si è proceduto alla richiesta di un parere specifico, in quanto il trattamento non introduce nuove finalità né incide in modo autonomo sulla posizione giuridica degli stessi, ma si limita a modificare le modalità operative interne dell'amministrazione. Tale scelta appare coerente con la natura organizzativa del trattamento; resta comunque ferma la possibilità di acquisire eventuali osservazioni da parte dell'utenza scolastica e del personale, qualora emergano criticità o esigenze di aggiornamento della presente valutazione.

Categorie di interessati: le categorie di interessati coinvolte nel trattamento comprendono, in primo luogo, gli alunni e le rispettive famiglie, i cui dati sono trattati nell'ambito delle attività amministrative e organizzative connesse al servizio di istruzione. A tali soggetti si affianca il personale scolastico, sia docente che amministrativo, i cui dati sono trattati per finalità di gestione del rapporto di lavoro e per l'organizzazione delle attività istituzionali. In via indiretta, possono essere coinvolti anche soggetti terzi che intrattengono rapporti con l'istituzione scolastica, quali fornitori o enti pubblici.

Categorie di dati trattati: quanto alle categorie di dati trattati, il lavoro agile comporta il trattamento delle medesime tipologie di dati già gestite in presenza, ma con un diverso grado di esposizione al rischio. In

particolare, vengono trattati dati personali comuni, quali dati anagrafici e di contatto, nonché dati relativi al percorso scolastico degli studenti e alla posizione lavorativa del personale. In taluni casi, il trattamento può riguardare anche dati appartenenti a categorie particolari, quali quelli relativi alla salute o alle condizioni di disabilità degli alunni, nonché dati relativi a procedimenti disciplinari o situazioni che richiedono una particolare tutela della riservatezza. Proprio la presenza di tali dati impone un approccio particolarmente prudente nella definizione delle modalità operative del lavoro agile, al fine di garantire il rispetto dei principi di minimizzazione e di integrità e riservatezza del trattamento.

Natura dei dati e ciclo di vita del trattamento

Il lavoro agile non introduce nuove categorie di dati, ma espone a un diverso livello di rischio dati già trattati nell'ambito scolastico. Tra questi assumono particolare rilievo:

- dati relativi agli alunni, spesso minori;
- dati del personale;
- dati appartenenti a categorie particolari.

Il ciclo di vita dei dati resta formalmente invariato, ma la fase di accesso e trattamento diventa più critica. La conservazione continua ad avvenire secondo le regole archivistiche proprie della pubblica amministrazione, ma la fase di utilizzo si colloca in un contesto meno controllato.

Questo scarto tra luogo di conservazione e luogo di trattamento rappresenta uno degli elementi centrali della valutazione del rischio.

La gestione deve rispettare tre pilastri normativi:

1. Le regole tecniche dell'AGID sulla conservazione digitale;
2. Le Linee Guida specifiche per le scuole.
3. I piani di conservazione e scarto stabiliti dal Ministero della Cultura.

Procedure di archiviazione e sicurezza

L'archiviazione dei documenti deve avvenire seguendo le istruzioni della scuola, utilizzando principalmente il software di segreteria in cloud o altri strumenti autorizzati per l'accesso a distanza.

Per garantire la sicurezza, il sistema deve essere configurato in modo che i documenti riservati siano consultabili **solo dal personale autorizzato** che ne ha effettivamente bisogno per le proprie mansioni.

Diritti degli Interessati

Chiunque desideri accedere ai propri dati, modificarli o cancellarli, deve presentare una richiesta scritta. Tuttavia, tali richieste non devono ostacolare le finalità principali del trattamento, che restano sempre legate al regolare svolgimento delle attività didattiche.

Dati di servizio e attività lavorativa

Per quanto riguarda i dati relativi alle attività svolte dagli utenti, il periodo di conservazione è limitato al tempo strettamente necessario per gestire e verificare la prestazione lavorativa del dipendente, in conformità con le direttive della Presidenza del Consiglio sul lavoro agile (Direttiva n. 3/2017).

Principi di liceità, necessità e proporzionalità

Il trattamento si fonda sull'esecuzione di compiti di interesse pubblico e sulla gestione del rapporto di lavoro. Tuttavia, la legittimità del lavoro agile non può essere considerata automatica.

Affinché il trattamento sia conforme ai principi del GDPR, è necessario che:

- le attività svolte da remoto siano effettivamente compatibili con tale modalità;
- l'accesso ai dati sia limitato a quanto strettamente necessario;
- il trattamento di dati particolarmente delicati sia ridotto o evitato.

La proporzionalità non si misura solo rispetto alla finalità, ma anche rispetto al contesto operativo: ciò che è lecito in presenza può non esserlo in ambiente remoto.

Contesto

Panoramica

Qual è il trattamento in considerazione?

Il trattamento riguarda lo svolgimento dell'attività lavorativa del personale scolastico al di fuori dei locali dell'istituzione scolastica, nell'ambito degli istituti del lavoro agile (L. 81/2017). Ciò comporta l'accesso remoto ai sistemi informativi dell'istituto, l'utilizzo di piattaforme di comunicazione e collaborazione a distanza, la gestione di documenti e procedure amministrative in formato digitale.

L'attività lavorativa in modalità agile può avvenire dal domicilio del dipendente o da altro luogo concordato, attraverso strumenti messi a disposizione dal titolare del trattamento (pc, tablet, VPN) o tramite dispositivi propri del lavoratore (BYOD – Bring Your Own Device), secondo quanto previsto nell'accordo individuale di lavoro agile.

Quali sono le responsabilità connesse al trattamento?

I soggetti coinvolti nel trattamento dati sono diversi, con funzioni complementari:

Il Titolare del trattamento è l'Amministrazione scolastica legalmente rappresentata dal Dirigente Scolastico, che determina quali dati trattare, per quali finalità, con quali strumenti e modalità, anche nell'ambito dell'organizzazione del lavoro agile.

Il Responsabile del trattamento è il fornitore delle piattaforme e degli strumenti digitali utilizzati per il lavoro agile (es. segreteria digitale, piattaforme di videoconferenza, gestori di posta istituzionale), che tratta i dati per conto del titolare in base ad apposito Data Processing Agreement.

Il DSGA e il personale ATA in lavoro agile o da remoto svolge attività amministrative, contabili e di supporto organizzativo da remoto, accedendo ai gestionali scolastici e ai documenti istituzionali attraverso connessioni sicure.

La dirigenza e le figure di staff coordinano l'organizzazione del lavoro agile, verificano la reperibilità del personale, gestiscono accordi individuali e monitorano il rispetto delle disposizioni normative e regolamentari.

Il Responsabile della Protezione dei Dati svolge una funzione di supporto, contribuendo alla valutazione dei rischi.

Ci sono standard applicabili al trattamento?

La scelta degli strumenti per il lavoro agile è stata effettuata tenendo in considerazione le disposizioni del Codice dell'Amministrazione Digitale (CAD), le indicazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN, ex AGID) sui servizi cloud abilitati per le PA e le Direttive ministeriali sul lavoro agile nelle pubbliche amministrazioni. Sono periodicamente consultate le raccomandazioni dell'EDPB (Comitato Europeo per la Protezione dei Dati) sui requisiti di sicurezza dei servizi cloud adottati dalle PA. L'istituto si è dotato di un regolamento interno per il lavoro agile e di accordi individuali conformi alla L. 81/2017 e alla contrattazione collettiva di riferimento (CCNL Comparto Istruzione e Ricerca).

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati nell'ambito del lavoro agile del personale scolastico riguardano sia la gestione amministrativa del rapporto di lavoro (dati identificativi, contrattuali, di rendicontazione dell'attività) sia l'accesso ai sistemi informativi dell'istituto da remoto (dati tecnici, log di accesso, credenziali). Possono altresì essere oggetto di trattamento dati relativi ad alunni e famiglie, ove il personale in lavoro agile svolga attività che comportino il trattamento di tali informazioni (comunicazioni, preparazione documentazione scolastica).

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

L'accesso ai sistemi in modalità agile è subordinato alla stipula di un accordo individuale di lavoro agile e all'assegnazione di credenziali di accesso sicure. Il personale ATA gestisce pratiche amministrative, corrispondenza istituzionale e procedure contabili attraverso i gestionali scolastici accessibili da remoto. La dirigenza monitora la reperibilità del personale negli orari concordati e verifica la corretta esecuzione delle

attività assegnate, nel rispetto dei limiti imposti dalla normativa sul lavoro agile (divieto di sorveglianza continuativa a distanza, diritto alla disconnessione, rispetto dei tempi di riposo).

Nelle attività di natura organizzativa/amministrativa, sono predisposti canali di comunicazione istituzionale (email, piattaforme di collaborazione) per la condivisione di documenti e informazioni funzionali allo svolgimento delle attività lavorative in modalità agile.

Quali sono le risorse di supporto ai dati?

Le risorse tecnologiche a supporto del lavoro agile comprendono: dispositivi digitali (pc, tablet forniti dall'istituto o dispositivi personali del lavoratore), connessione internet, VPN o accesso sicuro ai sistemi gestionali, piattaforme di videoconferenza e collaborazione a distanza, posta elettronica istituzionale, segreteria digitale, sito web, piattaforme ministeriali, accesso al registro elettronico e ai sistemi di archiviazione documentale. Tali strumenti sono configurati e gestiti secondo le indicazioni del responsabile informatico dell'istituto e nel rispetto delle policy di sicurezza adottate.

Principi fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono quelli di perseguire le finalità istituzionali del titolare del trattamento, tra le quali rientra la corretta organizzazione del lavoro in modalità agile ai sensi della L. 81/2017 e delle successive disposizioni applicabili alle pubbliche amministrazioni. Il CAD prevede la transizione digitale delle PA per efficientare i servizi, e l'adozione del lavoro agile rappresenta uno degli strumenti di modernizzazione organizzativa promossi dal Piano Nazionale di Ripresa e Resilienza (PNRR) e dalle Direttive del Ministro per la Pubblica Amministrazione. Il trattamento è esplicitamente comunicato agli interessati tramite specifica informativa, che definisce tutti gli aspetti del trattamento e la legittimità dello stesso da parte del titolare.

Quali sono le basi legali che rendono lecito il trattamento?

L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6, par. 1, lett. e GDPR). In particolare: l'organizzazione del lavoro agile è disciplinata dalla L. 81/2017 e dal CCNL Comparto Istruzione e Ricerca; la gestione del rapporto di lavoro è riconducibile all'art. 88 GDPR (trattamento nel contesto del rapporto di lavoro); l'eventuale trattamento di categorie particolari di dati (es. stato di salute) trova base nel combinato disposto dell'art. 9, par. 2, lett. b) GDPR e dell'art. 88 GDPR. Il trattamento dei dati tecnici di accesso ai sistemi è giustificato dalle esigenze di sicurezza informatica, nel rispetto dei limiti previsti dalla normativa lavoristica e dalle indicazioni del Garante.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati trattati nell'ambito del lavoro agile sono strettamente limitati a quelli necessari per la gestione del rapporto di lavoro in modalità remota e per garantire la sicurezza dei sistemi informativi dell'istituto. Sono adottate misure per evitare forme di controllo eccessivo o non proporzionato dell'attività lavorativa a distanza, nel rispetto del divieto di sorveglianza continuativa previsto dalla L. 81/2017 e dallo Statuto dei Lavoratori. I dati oggetto di trattamento in modalità agile sono quelli raccolti dall'amministrazione per lo svolgimento dell'ordinaria attività lavorativa in presenza e sono utilizzati nel rispetto dei principi di adeguatezza, pertinenza e minimizzazione.

I dati sono esatti e aggiornati?

I dati vengono verificati e aggiornati periodicamente, in virtù della natura stessa e delle funzionalità dei trattamenti..

Qual è il periodo di conservazione dei dati?

La conservazione dei dati è effettuata per il periodo necessario al perseguimento delle finalità. Successivamente, per i documenti rilevanti ai fini didattici/amministrativi, si procede all'archiviazione dai

dati per il tempo previsto dalla normativa di riferimento. L'archiviazione deve rispettare i tempi previsti dalla circolare n.44 del 2005 della Direzione Generale degli Archivi. Per Registro elettronico almeno 5 anni e per le Comunicazioni con famiglie 1 anno, salvo obblighi di legge.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati del trattamento dati con specifica e dettagliata informativa (art. 13 GDPR), contenente i dettagli e le caratteristiche del trattamento. L'informativa sulla sicurezza è consegnata contestualmente alla stipula dell'accordo individuale, quella sul trattamento dati agli interessati è pubblicata sul sito web dell'istituto e su RE.

Come fanno gli interessati ad esercitare i propri diritti?

Gli interessati possono esercitare i propri diritti contattando gli uffici del titolare del trattamento, chiedendo informazioni sui propri dati o l'esercizio di un diritto di cui agli artt. 15 a 23 del GDPR, nella misura in cui applicabili alla tipologia di trattamento.. Per le categorie particolari di dati eventualmente trattate nell'ambito del rapporto di lavoro, si applicano le disposizioni specifiche previste dalla normativa lavoristica.

Gli obblighi dei Responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I fornitori degli strumenti e delle piattaforme utilizzate svolgono il ruolo di Responsabili del trattamento e trattano i dati per conto del titolare in base ad apposito Data Processing Agreement (DPA), nel quale sono specificati gli obblighi in carico al Responsabile del trattamento. I fornitori selezionati sono inseriti nell'elenco dei servizi cloud abilitati dall'Agenzia per la Cybersicurezza Nazionale (ACN) e sono stati valutati in merito ai requisiti di sicurezza e affidabilità informatica. Il Contratto prevede che l'Istituto scolastico è il titolare del trattamento e il fornitore è il Responsabile del trattamento, con precisi obblighi di riservatezza, sicurezza e limitazione delle finalità di utilizzo dei dati.

Rischi

Come abbiamo visto all'inizio di questa DPIA, alla Fase 1 "Identificazione dei trattamenti", seguono la Fase 2 "Panoramica dei rischi" e la Fase 3 "Valutazione del rischio ed eventuali misure correttive".

Misure esistenti o pianificate

Controllo degli accessi

Gli accessi ai sistemi informativi dell'istituto in modalità remota avvengono attraverso credenziali individuali assegnate ad ogni dipendente autorizzato, con eventuali limitazioni in base alla tipologia di utente e alle funzioni svolte. È adottata, ove possibile, l'autenticazione a due fattori (2FA) per l'accesso ai sistemi più sensibili. Gli account di dipendenti non più in servizio o non più autorizzati al lavoro agile vengono tempestivamente disattivati.

Minimizzare la quantità di dati personali

I dati personali vengono minimizzati più possibile, compatibilmente con il perseguimento delle finalità lavorative e organizzative. Sono adottate misure per limitare l'accesso del lavoratore agile ai soli dati strettamente necessari allo svolgimento delle attività assegnate, evitando accessi a banche dati o archivi non pertinenti con le mansioni svolte in modalità remota.

Anonimizzazione dei dati

L'utente è identificato in chiaro sui sistemi istituzionali, in quanto l'identificazione univoca è necessaria per la corretta gestione del rapporto di lavoro e la responsabilità delle attività svolte.

Misure di sicurezza informatica

I dispositivi forniti dall'istituto per il lavoro agile sono configurati con software antivirus, anti-malware e firewall aggiornati, e sono dotati di credenziali per l'accesso. Per i dispositivi personali del lavoratore (BYOD), sono fornite precise indicazioni sull'adozione di misure di sicurezza minime (antivirus, aggiornamenti del sistema operativo, password sicure). Le comunicazioni tra i dispositivi remoti e i sistemi dell'istituto avvengono, ove possibile, tramite VPN o connessioni cifrate. Le misure di sicurezza proprie delle piattaforme utilizzate sono attuate direttamente dai rispettivi fornitori/responsabili del servizio.

Istruzioni agli utenti

Il personale autorizzato al lavoro agile è stato istruito sul corretto utilizzo degli strumenti digitali e sul trattamento dei dati nell'ambito del lavoro remoto, attraverso strumenti informativi dedicati, regolamenti interni e policy specifiche. Sono state fornite indicazioni sia di natura tecnica (uso corretto degli strumenti, gestione delle credenziali, comportamenti da evitare) sia di natura normativa (obblighi di riservatezza, limitazioni al trattamento di dati di terzi al di fuori dei locali scolastici, rispetto della normativa sulla protezione dei dati). Il personale è informato del diritto alla disconnessione e dei limiti al controllo a distanza dell'attività lavorativa.

Accesso illegittimo ai dati

Fonti del rischio

Il rischio di un accesso illegittimo ai dati può avvenire per cause dolose o colpose/accidentali:

- Utilizzo di reti Wi-Fi pubbliche o non sicure per l'accesso ai sistemi istituzionali
- Cessione a terzi non autorizzati delle proprie credenziali di accesso
- Uso di dispositivi personali non adeguatamente protetti (BYOD)
- Azione dolosa di hackeraggio sulla piattaforma o sui dispositivi remoti
- Accesso da parte di conviventi o familiari ai dispositivi del lavoratore agile
- Condivisione di documenti contenenti dati personali tramite canali non istituzionali

Misure per mitigare il rischio

Le misure tecniche e organizzative utili a mitigare il rischio di un accesso illegittimo sono le seguenti (elenco in continuo aggiornamento):

- Utilizzo di VPN o connessioni cifrate per l'accesso remoto ai sistemi
- Autenticazione a due fattori (2FA) per i sistemi più sensibili
- Informazione tecnica e normativa agli utenti del lavoro agile
- Definizione delle policy sul trattamento dati in modalità remota
- Verifica periodica degli utenti attivi e di quelli da disattivare
- Controllo degli accessi logici con profilazione per ruolo
- Periodici appelli per una corretta gestione delle credenziali di accesso
- Obbligo di utilizzo di password robuste e cambio periodico
- Sistema firewall e software di sicurezza aggiornati

Modifiche indesiderate ai dati

Fonti del rischio

Il rischio di una modifica indesiderata ai dati può avvenire per cause dolose o colpose/accidentali:

- Errore umano (es. modifica di dati errati nel giusto documento o modifica di dati esatti nel documento sbagliato, facilitata dalla distanza fisica dall'ufficio)
- Volontà/dolo di un dipendente in lavoro agile di modificare dati per i quali non è autorizzato ad agire
- Volontà/dolo di un soggetto esterno che riesce ad accedere ai sistemi sfruttando le vulnerabilità del lavoro remoto

Misure per mitigare il rischio

Le misure tecniche e organizzative utili a mitigare questo rischio sono le seguenti (elenco in continuo aggiornamento):

- Profilazione degli accessi ai sistemi in base al ruolo e alle mansioni assegnate
- Sistemi di verifica per le modifiche ai documenti istituzionali
- Formazione tecnica agli utenti
- Definizione delle policy sul trattamento dati
- Verifica periodica degli utenti attivi e di quelli da disattivare
- Controllo degli accessi logici
- Archiviazione/Razionalizzazione dei documenti e Backup periodico

Perdita di dati

Fonti del rischio

Il rischio di una perdita dati può avvenire per cause dolose o colpose/accidentali:

- Errore umano (es. cancellazione accidentale di dati o file da parte del lavoratore agile)
- Malfunzionamenti tecnici dei dispositivi utilizzati per il lavoro agile
- Attacchi ransomware o malware su dispositivi remoti non adeguatamente protetti
- Perdita o furto del dispositivo utilizzato per il lavoro agile
- Interruzione della connessione durante operazioni critiche sui dati

Misure per mitigare il rischio

Le misure tecniche e organizzative utili a mitigare il rischio di una perdita dati sono le seguenti (elenco in continuo aggiornamento):

- Backup automatico e periodico dei dati sui sistemi centralizzati dell'istituto
- Divieto di conservazione di dati istituzionali esclusivamente su dispositivi locali del lavoratore agile
- Obbligo di lavorare sui sistemi cloud/server istituzionali, non su copie locali
- Formazione tecnica agli utenti
- Sistemi anti-malware e firewall aggiornati
- Procedure di segnalazione tempestiva in caso di perdita o furto del dispositivo

Stima della probabilità e della gravità del rischio

Sulla base delle misure adottate (che vengono costantemente monitorate e implementate se necessario) e delle indicazioni agli utenti sulla corretta gestione degli strumenti di lavoro agile:

Rischio	Fonte	Impatto potenziale	Conseguenza	Probabilità
Accesso non autorizzato ai dati del lavoratore agile	Uso di dispositivi personali non protetti o reti non sicure	Violazione della riservatezza dei dati personali e lavorativi	Alta	Media
Perdita o distruzione dei dati	Malfunzionamenti tecnici, attacchi ransomware, mancanza di backup	Inaccessibilità degli strumenti di lavoro e perdita di dati sensibili	Alta	Bassa
Trattamento eccessivo o scorretto	Configurazione errata degli strumenti di monitoraggio da remoto	Violazione dei principi di minimizzazione e proporzionalità	Alta	Bassa
Monitoraggio indebito del lavoratore	Uso non conforme degli strumenti di supervisione a distanza	Lesione della dignità e della privacy del dipendente	Alta	Bassa

Rischio	Fonte	Impatto potenziale	Conseguenza	Probabilità
Errore umano nella gestione dei dati	Inserimento o trasmissione errata di informazioni riservate	Dati inaccurati o diffusi a destinatari non autorizzati	Media	Media
Uso di credenziali deboli o condivise	Scarsa cultura della sicurezza tra il personale scolastico	Furto d'identità o accesso indebito ai sistemi istituzionali	Alta	Bassa
Accesso da dispositivi non sicuri (BYOD)	Uso di dispositivi personali senza adeguata protezione	Compromissione dei dati istituzionali e personali	Alta	Media
Mancata informazione al personale	Assenza di formazione periodica sul lavoro agile	Errori nel trattamento dei dati e violazioni involontarie	Media	Media
Comunicazioni non cifrate	Uso di canali di comunicazione non sicuri o non istituzionali	Intercettazione o acquisizione non autorizzata dei dati	Alta	Bassa
Conservazione eccessiva dei dati	Assenza di politiche di retention per i log di accesso remoto	Violazione del principio di limitazione della conservazione	Media	Bassa
Accesso inappropriato da parte di terzi conviventi	Svolgimento del lavoro in ambienti domestici condivisi	Violazione della riservatezza di dati di alunni o colleghi	Alta	Media
Mancato aggiornamento del software	Negligenza nella manutenzione dei dispositivi utilizzati a distanza	Esposizione a vulnerabilità informatiche note	Alta	Media

Il livello del rischio può essere misurato numericamente utilizzando due valori:

- 1) Probabilità di accadimento (P)
- 2) Conseguenze (C)

Il Livello di Rischio (LR) è dato dunque dalla relazione: $LR = P \times C$

Alla probabilità P e alle conseguenze C sono associati valori numerici in relazione alla loro incidenza:

P	Probabilità di accadimento	C	Conseguenza
1	Bassa	1	Bassa
2	Media	2	Media
3	Alta	3	Alta
4	Certo	4	Altissima

Il livello di rischio LR, dunque, potrà variare da un valore minimo 1 a un valore massimo 16, così valutabile:

Entità del rischio	Valori di riferimento
Poco rilevante	$1 \geq LR \leq 3$
Basso	$4 \geq LR \leq 7$
Alto	$8 \geq LR \leq 12$
Altissimo	$13 \geq LR \leq 16$

Così è possibile ricavare, per ogni attività di trattamento, il Livello di Rischio di potenziale accesso illegittimo, modifica, perdita, distruzione di dati non autorizzata.

I livelli P e C vengono chiaramente stimati e assegnati ai rischi dal titolare in relazione ad una valutazione generale dei propri trattamenti, alla luce di tutti i parametri specificati nel corso di questa DPIA.

Sintesi della valutazione dei rischi

Livello di Rischio (LR)

Rischio	Probabilità (P)	Conseguenze (C)	Livello di Rischio (LR)	Entità rischio
Accesso illegittimo ai dati	2	3	6	Basso
Modifiche di dati	2	2	4	Basso
Perdita di dati	2	3	6	Basso

Esito DPIA e conclusioni

La valutazione d'impatto svolta per l'adozione del lavoro agile da parte del personale delle istituzioni scolastiche ha consentito di prendere in esame i vari aspetti del trattamento per valutarne eventuali criticità.

La correlazione tra le misure tecniche e organizzative adottate, le tipologie di rischi che si possono presentare, le probabilità che essi si verifichino e la gravità delle eventuali conseguenze, consente di giungere ad una "misurazione" del livello di rischio connesso al trattamento che, in conclusione di questa DPIA, può ritenersi Accettabile.

Per quanto sopra esposto, analizzato e valutato, in considerazione delle finalità istituzionali perseguite, delle garanzie offerte dai fornitori dei servizi digitali utilizzati (Responsabili del trattamento), del rispetto dei diritti del lavoratore previsti dalla L. 81/2017 e dalla normativa sulla protezione dei dati,, sentito il DPO che ha collaborato alla stesura di questo documento, si ritiene che il lavoro agile possa essere adottato dall'istituzione scolastica nel rispetto delle condizioni e delle misure descritte nella presente DPIA.

La presente DPIA sarà sottoposta a revisione periodica o in occasione di variazioni significative nelle modalità di svolgimento del lavoro agile, nell'organizzazione dell'istituto, nella normativa di riferimento o nelle soluzioni tecnologiche adottate.

Giuseppe
Cavallo
17.04.2026
17:05:39
GMT+02:00

