Informazioni sul PIA

PIA

PIA_Amministrazione_ICAD

Nome autore

Prof. Andrea Arnone

Nome assessore

Prof. Ennio Antinio Carnevale

Nome convalidatore

Prof. Roberto Pacciani

Data di creazione

Nome DPO

Prof. Ennio Antonio Carnevale

Parere DPO

Il registro del trattamento dati deve essere revisionato in occasione di eventuali variazioni nelle modalità di gestione dei dati.

Ricerca del parere di persone interessate

Non è richiesto il parere di persone interessate.

Motivazione per cui il parere delle persone interessate non stato richiesto

Il rischio trascurabile della modalità di gestione dei dati interna non comporta la necessità di chiedere il parere delle persone interessate.

Contesto

Panoramica

Quale è il trattamento in considerazione?

Il trattamento riguarda i dati gestiti ad uso Amministrativo. La sua natura/ scopo è quella di gestire in maniera sicura tutti i dati personali trattati per l'amministrazione quotidiana della società. Si tratta di dati personali quali: nome, cognome, codice fiscale, partita iva, IBAN, email, recapiti telefonici.

Quali sono le responsabilità legate al trattamento?

Il titolare dei dati è l'amministratore dell'azienda che può incaricare per iscritto come responsabile del trattamento, un responsabile finanziario che opera nella gestione delle pratiche amministrative/finanziarie dell'azienda stessa.

Ci sono standard applicabili al trattamento?

L'azienda stabilisce necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Si rimanda al registro dei trattamenti dati da considerarsi parte integrante della presente scrittura.

Com'è il ciclo di vita del trattamento dei dati?

Si rimanda al registro dei trattamenti dati da considerarsi parte integrante della presente scrittura.

Quali sono le risorse di supporto ai dati?

I dati vengono perlo più recuperati per via informatica e registrati tramite terminali propri, coperti da user e password. La policy è quella che ciasun terminale privato sia munito di password la cui responsabilità è del suo proprietario\utente, password che deve in maniera obbligatoria essere periodicamente (almeno ogni 3 mesi) modificata. Viene eseguito giornalmente un back-up in automatico dei dati su dischi fisici conservati presso la sede operativa del Consorzio.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità, necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati in questione vengono trattati esclusivamente per gli adempimenti legati alla gestione del rapporto di lavoro (pagamento stipendi collaboratori e prestazioni dei soci) e dei contratti di fornitura (pagamento di forniture di soggetti terzi e comunicazioni legate allo svolgimento delle attività contrattuali). Per un maggior dettaglio, si rimanda al registro dei trattamenti dati da considerarsi parte integrante della presente scrittura.

Valutazione : Accettabile

Quali sono le basi legali che rendono il trattamento legittimo?

Come sopra specificato, le basi legali sono l'espletamento del rapporto di lavoro e degli obblighi legati alla contrattualistica con soggetti terzi esterni. prima dell'avvio di qualsiasi rapporto di lavoro o accensione di contratto con fornitori terzi viene espressamente richiesta il consenso al trattamento dei dati attraverso informativa allegata al contratto specifico. Si rimanda al registro dei trattamenti dati da considerarsi parte integrante della presente scrittura.

Valutazione : Accettabile

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

L'azienda si impegna a raccogliere esclusivamente i dati necessari all'adempimento degli obblighi contrattuali siano essi di rapporto di lavoro (consulenti, soci) o legati a fornitori esterni. Si rimanda al registro dei trattamenti dati da considerarsi parte integrante della presente scrittura.

Valutazione : Accettabile

I dati sono accurati e mantenuti aggiornati?

Il titolare si impegna a modificare immediatamente i dati personali gestiti ed in possesso dell'azienda in caso di comunicazione da parte dell'interessato di variazione, cancellazione e rettifica degli stessi. In qualunque momento l'interessato può richiedere tramite PEC di visionare i dati personali in possesso dell'azienda per verificarne l'accuratezza e la correttezza, come specificato nell'informativa allegata.

Valutazione : Accettabile

Quale è la durata della conservazione dei dati?

Si rimanda al registro dei trattamenti dati da considerarsi parte integrante della presente scrittura.

Controlli per proteggere i diritti personali dei soggetti interessati

I soggetti interessati come sono informati del trattamento?

I soggetti interessati vengono informati delle modalità di trattamento mediante informativa da visionare e firmare prima dell'attivazione del contratto e/o del rapporto di lavoro, di essi parte integrante. Si allega il modello di tale informativa.

Valutazione : Accettabile

Come si ottiene il consenso dei soggetti interessati?

Il consenso dei soggetti interessati si ottiene mediante apposizione di firma autografa sull'informativa, fornita all'interessato congiuntamente alla documentazione per l'attivazione del contratto/rapporto di lavoro.

Valutazione : Accettabile

I soggetti interessati come esercitano i loro diritti di accesso alla portabilità dei dati?

In qualunque momento l'interessato può richiedere tramite PEC di visionare i dati personali in possesso dell'azienda per verificarne l'accuratezza e la correttezza, come specificato nell'informativa allegata.

Valutazione : Accettabile

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

In qualunque momento l'interessato può richiedere tramite PEC di visionare i dati personali in possesso dell'azienda per verificarne l'accuratezza e la correttezza, come specificato nell'informativa allegata.

Valutazione : Accettabile

I soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

In qualunque momento l'interessato può richiedere tramite PEC di visionare i dati personali in possesso dell'azienda per verificarne l'accuratezza e la correttezza e/o specificare un utilizzo limitato rispetto a quello indicato nel consenso, come specificato nell'informativa allegata.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Il responsabile del trattamento dei dati legati agli adempimenti amministrativi è il Prof. Carnevale, membro del Consiglio Scientifico.

Valutazione : Accettabile

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

Non vengono effettuati trasferimenti di dati al di fuori dell'Unione Europea, come indicato anche nel registro allegato.

Valutazione : Accettabile

Rischi

Controlli esistenti o pianificati

Backup

Giornalmente viene eseguito automaticamente un back-up dei dati archiviati su dischi esterni removibili conservati in armadi chiusi a chiave presso la sede operativa dell'azienda.

La ridondanza dei dati ottenuti col mirroring sui device terminali e su più dischi removibili, conservati separatamente, permette di garantire in caso di guasto/rottura, opportuna strategia per evitare la perdita dei dati.

La cancellazione accidentale del dato da terminale, è ripristinabile da dischi esterni removibili tramite procedura di salvataggio copie sovrascritte.

L'aggiornamento del backup è automatizzata con periodicità giornaliera. Pertanto l'ultimo stato valido sulla memoria di

backup esterna risale al giorno precedente. I dati aggiornati in tempo reale risiedono su dischi e sui terminali dai quali avviene l'aggiornamento/creazione dei file.

Valutazione : Accettabile

Controllo degli accessi

I dati personali vengono archiviati su terminali protetti da password e dischi esterni removibili (copie di back-up). Viene richiesto la modifica periodica della password (almeno ogni 12 mesi).

Valutazione : Accettabile

Integrare la protezione della privacy nei progetti

Al momento dell'attivazione di un nuovo rapporto di lavoro e/o contratto viene richiesta obbligatoriamente la firma dell'informativa sul trattamento dei dati (allegata alla presente).

Valutazione : Accettabile

Sicurezza dei documenti cartacei

I documenti cartacei prodotti nell'ambito delle attività amministrative sono conservati in faldoni cartacei presso la stanza dedicata all'amministrazione aziendale. L'accesso all'archivio è tramite armadi protetti con serratura a chiave tradizionale. L'accesso alla stanza è riservato agli addetti all'amministrazione che hanno copia delle chiavi.

Una copia di riserva delle chiavi è lasciata alla segreteria del Dipartimento nei cui locali è ubicata la sede operativa dell'azienda.

Valutazione : Accettabile

Sicurezza della rete

La rete aziendale su cui sono installati i terminali presenta un router standard con modalità di firewall attivo. I terminali montano sistemi operativi iOS/windows con protezione attiva per la protezione da virus e minacce. L'impiego di terminali con sistemi operativi differenti (Linux/Linux) dovranno essere pianificati con relativa fornitura delle credenziali di accesso alla rete (Ip statico e DHCP).

Valutazione : Accettabile

Gestione postazioni

I singoli terminali sono protetti da password definita dall'utente stesso e periodicamente aggiornata.

Valutazione : Accettabile

Lotta contro il malware

I terminali utilizzano sistemi con protezione attiva, antivirus e firewall del sistema operativo.

Valutazione : Accettabile

Evitare le fonti di rischio

I device sono tenuti all'interno di ambienti conformi all'utilizzo da ufficio e quindi opportunamente muniti di sicurezza contro agenti atmosferici ricontrabili.

Valutazione : Accettabile

Accesso illegittimo ai dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?

Furto di identità, Generazione di account fasulli, invio di email da account di terze persone

Quali sono le principali minacce che potrebbero concretizzare il rischio?

La cessione volontaria o involontaria delle proprie user e password dell'accesso personale ai terminali, Lasciare sbloccato ed incustodito il terminale fino a blocco automatico

Quali sono le fonti di rischio?

Dipendente malintenzionato, Soggetto esterno malintenzionato

Quali dei controlli identificati contribuiscono a gestire il rischio?

Sicurezza della rete, Controllo degli accessi, Sicurezza dei documenti cartacei, Gestione postazioni

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?

Trascurabile, I dati gestiti sono facilmente recuperabili su altri canali quali social.

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli pianificati?

Limitata, Per l'attuale struttura operante in termini di personale.

Valutazione : Accettabile

Modifiche indesiderate dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?

Perdita di tempo nel ripetere le procedure o di aspettarle.

Quali sono le principali minacce che possono portare al rischio?

Postazioni incustodite senza il blocco dell'account

Quali sono le fonti di rischio?

Dipendente malintenzionato, Soggetto esterno malintenzionato, Attacco informatico

Quali dei controlli identificati contribuiscono a gestire il rischio?

Backup, Controllo degli accessi, Gestione postazioni

Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

Trascurabile, Perdita di tempo nel ripetere le procedure o di aspettarle

Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

Trascurabile, Per l'attuale struttura operante in termini di personale.

Valutazione : Accettabile

Scomparsa di dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?

Perdita di tempo nel recuperare i dati dai dischi esterni removibili di backup

Quali sono le minacce che potrebbero portare al rischio?

Lasciare libero l'accesso all'ambiente dove si trovano i dischi removibili esterni, Lasciare i terminali incustoditi fino al blocco automatico

Quali sono le fonti di rischio?

Dipendente malintenzionato, Ladro

Quali dei controlli identificati contribuisce a gestire il rischio?

Backup, Gestione postazioni, Sicurezza della rete, Evitare le fonti di rischio

Come stimeresti la gravità del rischio, specialmente riguardo il potenziale impatto e i controlli pianificati?

Trascurabile, Perdita di tempo nel ripetere le procedure

Come stimeresti la probabilità del rischio, specialmente rispetto le minacce, fonti di rischio e i controlli pianificati?

Trascurabile, Per l'attuale struttura operante in termini di personale.

Valutazione : Accettabile

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Controlli esistenti o pianificati

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.