Disciplinare per l'uso degli strumenti informatici, internet, posta elettronica e dei sistemi informativi

Attuazione dei principi del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

.

Sommario

Premessa

Le informazioni sono un bene che necessita di essere protetto adeguatamente, in quanto soggette ad un'ampia gamma di minacce
Le informazioni possono essere presenti in molte forme. Possono essere stampate o scritte su carta, memorizzate elettronicamente, trasmesse per posta o utilizzando altri mezzi elettronici, visualizzate su pellicole o trasmesse in una conversazione. Qualunque forma abbiano le informazioni o qualunque sia il mezzo su cui è condivisa o memorizzata una informazione, questa dovrebbe essere sempre protetta adeguatamente.
La sicurezza delle informazioni è definita come il mantenimento della:

a) riservatezza: l'assicurazione che le informazioni siano accessibili solo a coloro che sono autorizzati ad avere l'accesso;
b) integrità: salvaguardare la precisione e la completezza dell'informazione e del metodo di elaborazione;
c) disponibilità: l'assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e ai beni quando richiesto.

La sicurezza delle informazioni è ottenuta realizzando un insieme adatto di controlli, che potrebbero essere criteri, pratiche, procedure, strutture organizzative e funzioni software.

Oggetto

L'Agenzia per il Diritto allo Studio della Regione Puglia (**di seguito anche Adisu/Agenzia**) con il presente Disciplinare si propone di evitare che comportamenti inconsapevoli possano innescare problemi e/o minacce alla sicurezza nel trattamento dei dati personali di qualsivoglia tipo (personale, sensibile e giudiziario) e per richiamare le indicazioni e le misure necessarie ed opportune per il corretto utilizzo delle **risorse informatiche** in particolare dei personal computer (fissi e portatili), di smartphone, di internet, della posta elettronica, cioè dell'insieme degli strumenti/sistemi informatici, ed in generale dei vari sistemi informativi dell'Ente, procedure e programmi software in uso nei vari settori, definendone le modalità di utilizzo nell'ambito dell'attività lavorativa
Nel caso di autorizzazione da parte dell'Ente all'utilizzo per motivi di lavoro in **smart working** di dispositivi di proprietà personale (modello **BYOD – Bring your own device**) la presente policy aziendale di sicurezza è estesa anche a tali dispositivi, per quanto compatibile.
Il presente Disciplinare si inquadra nell'ambito delle misure tecniche ed organizzative adottate dall'Ente per fare fronte ad esigenze di sicurezza nel trattamento dei dati personali e per minimizzare il rischio di violazioni dei dati (data breach), nel rispetto del Regolamento Europeo 2016/679.
Inoltre, il presente disciplinare costituisce adeguata informazione sul trattamento dei dati personali, sulle modalità d'uso delle risorse informatiche e sull'effettuazione dei controlli, ai sensi del Regolamento Europeo 2016/679 e dell'art.4 della Legge 20.5.1970, n. 300.

Campo di applicazione

Il disciplinare si applica ad ogni Utente, cioè a tutti i lavoratori dipendenti, nonché a tutto il personale che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto di lavoro e/o utilizzazione con lo stesso intercorrente - presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso il titolare del trattamento o che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato e abilitato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche.

Riferimenti normativi e regolamentari

- Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", come modificato ed integrato dal D.Lgs.101/2018 e ss.mm.ii.;;
- Provvedimento del Garante per la protezione dei dati personali "Linee guida per posta elettronica e internet" del 01.03.2007" [1387522] (Gazzetta Ufficiale n. 58 del 10 marzo 2007);
- Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 [1577499] (G.U. n. 300 del 24 dicembre 2008);
- Provvedimento del Garante "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento" [1626595] del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009);
- Provvedimento del Garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali " [1571514] del 13 ottobre 2008 (Gazzetta Ufficiale n. 287 del 9 dicembre 2008);
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro";
- Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- Codice di Comportamento dell'ADISU PUGLIA approvato con Deliberazione del Consiglio di Amministrazione n. 60 del 18/12/2023
- Legge 90/2024 cybersicurezza

Destinatari e perimetro

Le risorse informatiche oggetto del presente Disciplinare sono in uso nell'Ente (in proprietà, noleggio, service, comodato o qualsiasi altra forma contrattuale) e sono messi a disposizione dei dipendenti al fine di permettere il quotidiano svolgimento delle proprie prestazioni lavorative.
Esse sono essenzialmente individuabili quali:

- computer, fissi o mobili; tablet e altri apparati mobili; server; sistemi di identificazione e di autenticazione informatica; smartphone concessi in uso dall'Ente;
- Internet, intranet e altri strumenti di scambio di comunicazioni e file, compresi quelli delocalizzati con tecnologia cloud; apparecchiature informatiche necessarie per l'uso di internet o intranet
- posta elettronica;
- vari sistemi informatici quali software gestionali (es. applicativo protocollo ed atti, applicativo amministrazione trasparente, ecc); software di produttività individuali (es. onedrive software di archiviazione e condivisione file)

E' responsabilità di tutti i soggetti che utilizzano le risorse informatiche messe a disposizione, di applicare e rispettare puntualmente le disposizioni del presente Disciplinare.

Gli amministratori di sistema hanno accesso e responsabilità significative sui sistemi informatici, compresi i dati personali trattati all'interno di tali sistemi. Il Garante stabilisce regole precise per garantire che gli amministratori di sistema gestiscano e proteggano i dati personali in conformità con le normative sulla privacy.

Le misure e gli accorgimenti prescritti nei vari provvedimenti del Garante hanno riguardato questioni come l'accesso limitato ai dati personali solo quando strettamente necessario per svolgere le proprie funzioni, la registrazione degli accessi per monitorare l'attività degli amministratori di sistema, la formazione e la sensibilizzazione del personale sugli obblighi di riservatezza e sicurezza dei dati, e altre disposizioni atte a garantire la protezione dei dati personali.

Per Amministratore di Sistema si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.
Devono essere nominati Amministratori di Sistema tutti coloro che, nell'espletamento delle loro consuete attività tecniche, sono "responsabili" di fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, quali ad esempio:

- gestione dei sistemi di autenticazione e di autorizzazione;
- custodia delle credenziali di autenticazione e di autorizzazione;
- salvataggio dei dati (backup/recovery);
- organizzazione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- manutenzione hardware.

Possono dunque qualificarsi quale Amministratori di sistema i seguenti soggetti:

- amministratori di sistemi di autenticazione e di autorizzazione;
- amministratori di server e pc;
- amministratori di apparati di rete;
- amministratori di base di dati;
- amministratori di apparati di sicurezza;
- amministratori di applicazioni

Nel caso di servizi di amministrazione di sistema affidati in outsourcing, quale Responsabile esterno del Trattamento, l'Ente dovrà impegnarsi a conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale di dipendenti, l'Ente è tenuto a rendere noto o conoscibile l'identità degli Amministratori di sistema nell'ambito della propria organizzazione.

Si rende noto che gli Amministratori di Sistema quale personale, interno ed esterno, opera per garantire la corretta configurazione e funzionamento del sistema informatico (nel seguito per brevità "**Servizio IT**").

Il **servizio IT** è autorizzato a compiere interventi diretti a garantire la funzionalità, la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware ecc.). Detti interventi potranno anche comportare l'accesso in caso di effettiva necessità, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività, si applica anche in caso di assenza prolungata o impedimento dell'utente, in caso di effettiva necessità. Si precisa sin da ora che tali azioni saranno poste in essere solo se strettamente necessarie, prediligendo, caso per caso, interventi che non comportano trattamento dati, se non indispensabili.

Credenziali di autenticazione e profilo di accesso

Obiettivo fondamentale della sicurezza delle informazioni è quello di limitare l'accesso dei dati alle effettive e legittime necessità operative dell'Utente.

Tutti i sistemi informativi sono dotati della possibilità di definire profili di abilitazione mediante i quali dettagliare i privilegi dei diversi ruoli professionali in termini di funzionalità eseguibili e di dati accessibili nell'ambito dello specifico sistema hardware e software, in linea con le prescrizioni dettate dal Regolamento Europeo 2016/679 e dal Garante per la protezione dei dati personali.

Ad ogni Utente è, pertanto, assegnata una o più identità digitali aziendale (c.d. "credenziali di autenticazione"), con l'attribuzione di permessi di accesso ai dati in base al ruolo ed il reparto/servizio di appartenenza ed alle attività eseguite. Gli account Utente consentono l'autenticazione dell'operatore ai vari dispositivi ed ai vari sistemi informativi e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali.

Gli Utenti, anche in base a quanto indicato nell'articolo 14 relativo alle disposizioni relative all'utilizzo delle tecnologie informatiche del Codice di Comportamento dell'Agenzia, sono tenuti a rispettare le seguenti prescrizioni:

- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user-id), associato ad una parola chiave riservata (password), che dovrà essere custodita con la massima diligenza e non divulgata

- La password relativa alle credenziali di accesso ai vari software e dispositivi in uso dell'A.DI.S.U. - Puglia dovrà rispettare almeno i seguenti criteri:
    - Numero minimo di caratteri alfanumerici: 8;
    - Devono essere formate dalla combinazione di caratteri alfabetici (almeno un carattere minuscolo ed uno minuscolo), numerici (almeno un carattere) e di simboli come ad es. @, $£! (almeno un carattere);
    - Scadenza password: massimo 90 gg, ogni tre mesi, se i dati trattati sono particolari e/o giudiziari; per gli altri tipi di dati massimo 180 gg, ogni 6 mesi
    - La nuova password da impostare non può coincidere con la password da sostituire.
    - La composizione della password deve essere effettuata in modo da non contenere riferimenti facilmente riconducibili all'utente (data di nascita, nome, cognome, etc..).

  Dovrà essere cura del dipendente provvedere ad impostare le credenziali di accesso qualora il software non permetta di impostarli automaticamente. Laddove è possibile il rispetto dei criteri per la gestione password, secondo le indicazioni sopra fornite, sarà gestita in modo completamente automatizzato dal software.

- Le credenziali non dovranno essere rivelate a nessuno e per alcun motivo, a meno di nomina di un fiduciario ed/o un custode password che la conserverà in busta chiusa sigillata.

- Non deve essere conservato nessun appunto, e non deve essere inoltrato nessun messaggio (posta elettronica, cartaceo, sms) contenente le credenziali o riferimenti alla stessa, per evitare che altri ne vengano anche accidentalmente a conoscenza.

- Nel caso di sospetto che altri siano a conoscenza della propria password si dovrà modificare immediatamente le proprie credenziali e informare senza indugio il proprio superiore gerarchico.

- Il soggetto preposto al rilascio delle credenziali di autenticazione è il personale incaricato appositamente

nominato.

- Dove applicabile, sarà implementato il sistema di autenticazione a più fattori (MFA), che potrebbe includere metodi come l'invio di SMS, l'autorizzazione tramite impronta digitale e altri dati biometrici, allo scopo di mitigare il rischio derivante dal furto o dall'abuso delle credenziali di accesso. Con l'introduzione del MFA, gli utenti saranno tenuti a fornire una seconda forma di autenticazione, come SMS, chiamate, dati biometrici o codici monouso, in aggiunta alle normali credenziali di accesso, al fine di rafforzare ulteriormente la sicurezza degli accessi ai sistemi aziendali.

Le credenziali di autenticazione sono, altresì, revocate quando non sussiste più la necessità di disporre delle risorse e/o delle informazioni aziendali concesse (ad es. in caso di modifica delle mansioni o spostamento in altro servizio/ufficio).
In caso di interruzione a qualsiasi titolo del rapporto di lavoro con l'Ente, è vietato all'Utente di utilizzare il proprio Account e sarà disposta la cancellazione delle credenziali di autenticazione.

I vari sistemi informativi aziendali manterranno traccia di tutte le operazioni svolte dall'utente identificato con le sue credenziali di accesso, ivi compresi gli accessi da dispositivi remoti, registrando su di un apposito file Log ogni azione svolta dallo stesso (accesso ai dati, modifica dei dati, uso di risorse informatiche aziendali locali o remote, ecc.).

I Log possono essere oggetto di controllo attraverso l'Amministratore di sistema, in quanto consentono di ricostruire l'attività di un sistema informatico e di individuare eventuali responsabilità in caso di errore o violazioni di legge.

Strumenti informatici

Gli strumenti informatici sono il complesso di dispositivi fisici (PC, stampanti, lettori portatili, smartphone, ed altri devices) messi a disposizione dell'Utente dall'Agenzia per il perseguimento degli obiettivi aziendali.

Ogni Utente è responsabile dell'integrità e della custodia dei dispositivi fisici e delle informazioni/dati allo stesso affidati dall'Ente.

Ad ogni dispositivo è associato un numero di inventario, la collocazione fisica e l'Utente, allo scopo di curare il parco dispositivi aziendale e definire le responsabilità in caso di furto, smarrimento o guasto volontario.

Qualsiasi spostamento permanente del dispositivo (es. trasloco, assegnazione ad altro reparto, assegnazione ad altro professionista) deve essere concordato con il responsabile dell'Area del Patrimonio e con il Servizio IT allo scopo di consentirne la tracciabilità.
Ogni Utente ha specifiche credenziali di identificazione ed autenticazione per accedere ai dispositivi, e quindi alla rete aziendale e ad internet, pertanto i dispositivi possono essere utilizzati in condivisione con qualsiasi utente dell'ente, ciascuno con la propria sessione individuale di lavoro

Nell'uso dei dispositivi informatici, quali strumenti di lavoro, l'Utente è tenuto alle seguenti prescrizioni di carattere generale:

- utilizzare le risorse hardware e software secondo diligenza in modo appropriato e responsabile; (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia)

- non memorizzare file estranei all'attività di lavoro su hard disk o altri supporti di archiviazione forniti dall'Amministrazione; (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia)
- non utilizzare le risorse per scopi estranei all'attività di servizio e non modificare le configurazioni preimpostate, né installare dispositivi che compromettano l'integrità, l'operatività e la sicurezza delle risorse hardware e software; (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia)
- adottare ogni utile misura di sicurezza atta ad evitare che le credenziali di autenticazione, connesse all'utilizzo delle risorse del sistema informativo dell'Amministrazione associate al singolo dipendente, vengano a conoscenza di altri soggetti, anche lasciando incustodita l'attrezzatura informatica. (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia)
- è fatto assoluto di modificare la configurazione hardware e software del proprio dispositivo ovvero divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi ovvero divieto di rimuovere, danneggiare o asportare componenti hardware perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza
- custodire con cura e diligenza i dispositivi fisici per evitare la sottrazione, la distruzione o il danneggiamento; in caso di furto, smarrimento, malfunzionamento o guasto, effettuare la immediata segnalazione (al massimo entro 24 ore dalla conoscenza dell'evento) al Titolare, al Designato al trattamento ed al Responsabile della Protezione dei Dati, seguendo la procedura aziendale per il Data Breach pubblicata sul sito dell'Ente nella sezione privacy. Tale adempimento è necessario sia per ripristinare il dispositivo, sia per ottemperare agli obblighi imposti dal Regolamento Europeo 2016/679 (eventuale notifica al Garante entro 72 ore ed agli interessati), sia per effettuare le eventuali denunce agli Enti competenti (Autorità giudiziaria, ecc.)

In ultimo si vuole sottolineare l'importanza del divieto di utilizzo di programmi non autorizzati, client e su web.
È assolutamente vietato l'uso di programmi diversi da quelli ufficialmente forniti dall'Ente, così come non è consentito agli utenti installare autonomamente programmi o strumenti provenienti dall'esterno. Tale pratica costituisce una violazione grave delle politiche aziendali e comporta seri rischi per la sicurezza informatica aziendale.

L'utilizzo di software non autorizzato può infatti introdurre virus informatici e/o compromettere la funzionalità delle applicazioni esistenti, mettendo a rischio l'integrità dei dati aziendali e dei sistemi informatici. L'inosservanza di questa disposizione espone l'organizzazione a gravi responsabilità civili e penali.

Si sottolinea inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software, che richiede la presenza nel sistema di software regolarmente licenziato o libero e quindi non protetto dal diritto d'autore, sono soggette a sanzioni penali.

È fondamentale che ogni utente rispetti scrupolosamente questa regola al fine di garantire la sicurezza e l'affidabilità dei sistemi informatici aziendali e per evitare conseguenze legali.

Dispositivi client: personal computer, pc portatili e tablet

Le prescrizioni per i dispositivi da seguire sono:

- non lasciare incustodita la postazione di lavoro con la sessione utente attiva, quindi in caso di allontanamento dalla propria postazione di lavoro o bloccare il dispositivo (manuale da tastiera, blocco dinamico quando ci si allontana, funzione salvaschermo/screensaver protetto da password) o disconnettersi effettuando il log-out dalla sessione o spegnere il PC;
- I PC portatili utilizzati all'esterno (convegni, visite in aziende esterne, ecc...), in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni e di regola devono essere o custoditi sottochiave o portati con sé
- In merito alle prescrizioni degli smartphone si faccia riferimento alla sezione relativa del disciplinare

Il personale del servizio IT è tenuto al controllo della sicurezza delle postazioni, negando o interrompendo l'accesso alla rete agli Utenti che utilizzino dispositivi non adeguatamente protetti e/o aggiornati che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

Al fine di garantire l'assistenza tecnica, il regolare svolgimento delle attività operative e la massima sicurezza contro virus, spyware, malware, ecc., il personale incaricato del Servizio ha la facoltà di raggiungere fisicamente la postazione PC dell'utente e intervenire direttamente, o di connettersi in remoto e operare sulla stessa

L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso all'utente e si procederà con la sua fattiva collaborazione.

Il personale del Servizio IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete, dandone comunicazione all'utente che ne ha effettuato la creazione e/o l'inserimento.

Gli utenti non possono collegare alla rete del titolare personal computer, notebook, smartphone, tablet, palmari o simili, provenienti dall'esterno, senza aver precedentemente ricevuto esplicita autorizzazione. **E' possibile previa richiesta del Dirigente competente e previa verifica del servizio IT. Il dispositivo deve essere preventivamente censito**.

A disposizione degli amministratori vi sono una serie di report e dashboard che consentono di visualizzare informazioni dettagliate sull'utilizzo dei dispositivi, lo stato di conformità, gli aggiornamenti delle app e altro ancora.

Per quanto riguarda gli event log sui dispositivi, quali Windows, essi includono una vasta gamma di informazioni. Questi log registrano una serie di eventi come avvisi, errori, informazioni di sistema, informazioni sulla sicurezza e altro ancora. Questi log possono essere utilizzati per diagnosticare problemi di sistema, monitorare l'utilizzo delle risorse, tracciare attività degli utenti e identificare potenziali minacce alla sicurezza. Gli amministratori di sistema spesso consultano gli event log per identificare e risolvere problemi di sistema e di sicurezza.

Telefoni fissi, Smartphone, fax e fotocopiatrici

Il telefono fisso affidato all'utente è uno strumento di lavoro, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.

I log dei telefoni fissi aziendali possono includere diverse informazioni utili per il monitoraggio e la gestione delle chiamate, ad esempio tracciamento di tutte le chiamate effettuate e ricevute, inclusi i numeri di telefono coinvolti, gli orari delle chiamate e la durata.

Qualora venisse assegnato all'Utente uno smartphone aziendale quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso, cioè è uno strumento di lavoro, non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza.
In particolare, salvo esplicita autorizzazione, è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere telefonate/SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, ivi compreso il salvataggio di immagini, informazioni, messaggi e l'installazione di app o software non autorizzati.
L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta ed in conformità alle istruzioni che saranno fornite dal reparto tecnico al riguardo.

Per quanto riguarda l'installazione e l'utilizzo delle app sul dispositivo aziendale, si applicano le seguenti disposizioni:

- L'installazione di app sullo smartphone aziendale è consentita solo per fini strettamente correlati all'attività lavorativa e previa autorizzazione del responsabile IT o del reparto tecnico.
- Le app installate devono essere approvate dall'Ente e devono rispettare le politiche di sicurezza e di gestione dei dati aziendali.
- È vietata l'installazione di app non autorizzate o non conformi alle politiche aziendali, comprese quelle che potrebbero compromettere la sicurezza del dispositivo o dei dati aziendali.
- L'uso delle app installate deve essere coerente con gli scopi aziendali e non devono essere utilizzate per scopi personali o non autorizzati.
- L'utente è tenuto a rispettare le linee guida fornite dal reparto tecnico o dal responsabile IT in merito all'utilizzo delle app e a segnalare eventuali problemi o violazioni delle politiche di sicurezza.

I log degli smartphone aziendali includere diverse informazioni utili per il monitoraggio e la gestione delle chiamate, ad esempio tiene traccia di tutte le chiamate effettuate e ricevute, inclusi i numeri di telefono coinvolti, gli orari delle chiamate e la durata; se le app consentono l'accesso a risorse aziendali, come file o servizi online, possono registrare gli accessi degli utenti a queste risorse, inclusi dettagli come l'orario dell'accesso, il tipo di risorsa accessa e l'azione compiuta; si possono registrare eventi di sicurezza rilevanti, come tentativi di accesso non autorizzati, violazioni della sicurezza dei dati o altri eventi correlati alla protezione delle informazioni aziendali.

È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, salvo preventiva ed esplicita autorizzazione.

I log del fax solitamente includono informazioni come: tutte le attività di invio e ricezione dei fax, inclusi i numeri di telefono coinvolti, gli orari e gli esiti delle operazioni; eventuali errori durante il processo di trasmissione o

ricezione dei fax, come errori di connessione, errori di ricezione, mancata risposta del destinatario, ecc;

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione.

I log della fotocopiatrice includono informazioni come: numero delle fotocopie; numero delle stampe fatte, da chi e quando; possono includere anche informazioni sul formato delle fotocopie e sulle impostazioni di stampa utilizzate; stato delle forniture, come il livello di toner o inchiostro rimanente e la durata delle parti di consumo come i rulli di alimentazione della carta; errori di sistema, le eccezioni e gli avvisi di manutenzione, come segnalazioni di guasti hardware o richieste di sostituzione delle parti.

Supporti rimovibili

I supporti rimovibili sono dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer, come CD-ROM, DVD, penne USB, hard disk portatili, ecc.

Dato che i supporti rimovibili possono contenere dati personali sensibili, inclusi dati particolari e giudiziari, è essenziale prevenire il furto, l'alterazione, la distruzione o il recupero non autorizzato dei dati memorizzati su di essi.

Per garantire la sicurezza dei dati sui supporti rimovibili, è necessario adottare le seguenti precauzioni:

- Prima dell'uso, effettuare una scansione preventiva di tutti i supporti rimovibili per verificarne l'integrità e la sicurezza.
- Gli utenti sono responsabili della custodia dei supporti e dei dati aziendali in essi contenuti, pertanto devono conservarli in luoghi sicuri come armadi o cassetti chiusi a chiave.
- Tutte le unità rimovibili devono essere adeguatamente crittografate per garantire la protezione dei dati anche in caso di smarrimento o furto del dispositivo.
- Per garantire la distruzione sicura dei dati sensibili sui supporti magnetici rimovibili, gli utenti devono contattare il proprio responsabile e seguire le istruzioni fornite, anche tramite il servizio IT.

L'utilizzo dei supporti rimovibili dovrebbe essere considerato un'opzione remota, poiché esistono alternative più sicure per la condivisione dei dati aziendali, come Onedrive e la posta elettronica, che offrono funzionalità avanzate per la condivisione sicura dei file.

Posta elettronica

Il software di posta elettronica è un'applicazione informatica che consente di inviare, ricevere e gestire messaggi di posta elettronica. Questo strumento è uno dei vari sistemi informativi aziendali utilizzati per la comunicazione interna ed esterna, consentendo di inviare messaggi rapidamente e in modo efficiente a colleghi, studenti e fornitori. Grazie alla sua flessibilità e alla possibilità di utilizzarlo da qualsiasi dispositivo connesso ad internet, il software di posta elettronica è diventato uno strumento indispensabile per la gestione delle comunicazioni aziendali.

Per garantire la sicurezza e la conformità alle politiche aziendali sulla gestione dei dati, è obbligatorio utilizzare le app client o le app su smartphone indicate dal Servizio IT per l'accesso alla posta elettronica aziendale. Le app

raccomandate sono quelle incluse nella suite Microsoft 365, poiché offrono un elevato livello di sicurezza e gestione delle informazioni riservate. Utilizzare altre app di posta elettronica o client di posta non autorizzati è vietato.

Gli indirizzi aziendali, individuali e di servizio, rappresentano due categorie fondamentali nell'ambito delle comunicazioni digitali a livello aziendale. Gli indirizzi individuali sono assegnati a singoli utenti e li identificano in modo univoco. Questi indirizzi individuali sono utilizzati sono sotto la responsabilità esclusiva dell'utente a cui sono stati assegnati. Gli indirizzi di servizio sono invece condivisi e utilizzati da più utenti all'interno di un servizio o di un settore dell'organizzazione. Vengano utilizzati da più persone ma la responsabilità per la gestione e la manutenzione di questi indirizzi ricade su un unico soggetto, responsabile del servizio o settore, che si occupa di garantire che la posta venga usata correttamente.

L'Utente è tenuto alle seguenti prescrizioni di carattere generale:

- Le caselle di posta elettronica dell'Ente, potrà contenere sia indicazioni dell'utilizzatore che del ruolo, sono del tipo: **<iniziale del nome>.<cognome>@adisupuglia.it**), **<nome_settore/sede/servizio>@adisupuglia.it**, **<nome_settore/sede/servizio>@pec.adisupuglia.it**
- La casella di posta elettronica aziendale, a dominio del Titolare, sono strumenti di lavoro, anche quella assegnata all'utente (contenenti nome e/o cognome). Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. E' consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Agenzia. (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia).
- Al fine di ribadire agli interlocutori la natura esclusivamente professionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato (fornito dal titolare), che non dovrà essere disattivato dall'utente, nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dal titolare potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella policy del titolare
- L'utilizzo di caselle di posta elettroniche personali è, di norma, evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia).
- È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia).
- È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica (non eseguire download di file eseguibili) o nel cliccare su link presenti nel testo del messaggio di mittenti o da siti web sconosciuti.
- Al fine di garantire la funzionalità del servizio di posta elettronica, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) potrà essere impostato per inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto dell'Agenzia. In tal caso, la funzionalità deve essere attivata dall'utente.
- In caso di assenza non programmata (ad es. per malattia) la procedura descritta nel punto precedente,

non potendo essere attivata dal lavoratore, verrà attivata dal responsabile del servizio o del settore tramite il servizio IT.

- Il responsabile di settore o di servizio, anche tramite incaricati del Servizio IT, potrà accedere alla casella di posta elettronica per le sole finalità relative al corretto svolgimento delle attività e funzioni lavorative, dandone in tali casi riscontro all'interessato.
- In caso di cessazione del rapporto di lavoro la password di accesso all'indirizzo di posta elettronica assegnata verrà modificata, proibendone in tal modo l'accesso all'ex dipendente.
- In caso di cessazione del rapporto di lavoro, oltre alla disattivazione della casella mail, si procederà ad impostare un sistema di risposta agli eventuali terzi che dovessero inviare messaggi allo specifico indirizzo. Tali risposte conterranno indicazioni concernenti altre forme di contatto del titolare del trattamento.
- Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenente impegni contrattuali o precontrattuali per il titolare ovvero contenente documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere rigirata all'ufficio competente.
- La trasmissione all'interno dell'Agenzia di file contenenti dati personali definiti particolari (stato di salute, dati sanitari, disabilità, L. 104/92 ecc…) o dati giudiziari, ai sensi degli artt. 9 e 10 del GDPR 679/2016, dovrà avvenire con la massima attenzione e cautela in ordine all'importanza e alla delicatezza degli stessi. Per l'invio a destinatari, soprattutto esterni, di messaggi contenenti allegati relativi a dati personali particolari o giudiziari, **l'Utente è tenuto a renderli preventivamente illeggibili, criptandoli** oppure caricare in Onedrive e condividere il collegamento piuttosto che semplicemente allegarli, secondo indicazioni del Servizio IT.
  Resta inteso che, in caso di eventuale trasmissione a terzi non destinatari di dati particolari e/o giudiziari, deve essere immediatamente coinvolto il responsabile della protezione dati (DPO) e si devono attendere opportune istruzioni.

Il contenuto dei messaggi di posta elettronica –come pure i dati esteriori delle comunicazioni e i file allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un´ulteriore protezione deriva dalle norme penali a tutela dell´inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell´amministrazione digitale).
Per monitorare la conformità e proteggere la sicurezza informatica a disposizione degli amministratori vi sono gli avvisi del sistema, inerenti la posta elettronica, ed i relativi log. I log della posta elettronica includono metadati come data/ora di invio, indirizzi email del mittente/destinatario, dimensioni messaggio e informazioni sulla consegna.

Navigazione Internet

Durante l'orario di lavoro, la navigazione su internet deve essere limitata all'attività lavorativa. Tuttavia, è consentito ai dipendenti utilizzare gli strumenti informatici forniti dall'Agenzia per poter assolvere alle incombenze personali senza allontanarsi dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali, come specificato nell'articolo 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento

dell'Agenzia

L'utilizzo della rete del titolare da parte di ospiti, qualora consentito, sarà soggetto a vincoli di accesso alle risorse (rete wifi distinta da quella cablata, inibita la possibilità di accesso alle stampanti di rete aziendali, velocità di navigazione limitata, ...).

È vietato scaricare o condividere materiale protetto da copyright, accedere a siti illegali o utilizzare programmi peer-to-peer.

Si sottolinea che è anche vietato utilizzare software non autorizzato, anche attraverso applicazioni web native, al fine di garantire la sicurezza informatica e prevenire l'introduzione di virus o malware. In caso di dubbi sull'uso di determinati software, è consigliabile consultare il servizio IT.

Al fine di garantire che la navigazione su Internet si limiti esclusivamente a siti pertinenti all'attività lavorativa e per proteggere la sicurezza informatica, prevenendo l'introduzione di virus, malware o l'accesso a software illegali, verrà implementato un sistema di blocco o filtro automatico attraverso il servizio IT.

Gli eventuali controlli, compiuti dal personale incaricato del Servizio IT, potranno avvenire anche attraverso sistemi quali ad esempio firewall, così come mediante verifica dei file log presenti sui singoli pc client. Il trattamento quindi sarà svolto in forma automatizzata e manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti a ciò appositamente autorizzati, in ottemperanza a quanto previsto dal regolamento europeo GDPR 679/16.

I dati raccolti per la navigazione su Internet sono proporzionati alle finalità del monitoraggio e includono identificativi utente non direttamente associabili alla persona fisica, insieme a informazioni come il giorno e l'ora della navigazione, gli indirizzi web visitati, il tempo di connessione, i criteri di filtro applicati con il relativo esito, il responso del server remoto e i byte trasmessi e ricevuti.

Social Media

I rapporti con i mezzi di informazione, sugli argomenti istituzionali, sono tenuti dai soggetti istituzionalmente individuati, nonché dai dipendenti espressamente incaricati. (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell'Agenzia).
L'unico Servizio autorizzato a gestire le attività e pubblicare notizie in merito all'Agenzia sui social media, quali ad esempio le pagine facebook instagram le dirette yuoutube ecc, è il Servizio Comunicazione Istituzionale e Segreteria della Direzione Generale o chi lavoro in supporto.

Il titolare ha altresì ritenuto di fornire al tutto il personale alcune indicazioni dirette a guidare un utilizzo responsabile dei social media, anche sui propri account personali, quali:

- Non pubblicare contenuti o materiali coperti da riservatezza o segreto;
- Quando ci si esprime nei social media, è essenziale ricordare sempre che si è responsabili delle proprie comunicazioni;
- Non pubblicare materiali o contenuti offensivi, illegali, vessatori, diffamanti, minacciosi, volgari, osceni, che ledano diritti di terzi e/o che incoraggino condotte contrarie alle vigenti normative, ai codici di condotta o simili;

- Nell’utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all’Agenzia (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell’Agenzia).
- Astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Agenzia o della pubblica amministrazione in generale (art. 14 "Disposizioni relative all'utilizzo delle tecnologie informatiche, ai rapporti con i mezzi d'informazione e con i media" del Codice di Comportamento dell’Agenzia).
- Se ci si imbatte in commenti sul conto dell’Agenzia:
    - Se i commenti sono positivi: interagire liberamente, ma nel pieno rispetto delle regole qui sopra elencate;
    - Se i commenti sono negativi: astenersi dall’interagire e contattare il superiore gerarchico per renderlo edotto sui fatti;
    - Se i commenti hanno ad oggetto argomenti che richiedono competenze specifiche: astenersi dall’interagire e contattare il superiore gerarchico per renderlo edotto sui fatti;
    - In caso di dubbi, astenersi dall’interagire e contattare il proprio superiore gerarchico per renderlo edotto sui fatti.

Tali controlli saranno effettuati in modo proporzionato e rispettoso della privacy dei dipendenti, e saranno limitati a quanto strettamente necessario per le finalità sopra indicate.

Si rammenta che si possono effettuare controlli sui profili social personali dei dipendenti, solo quando i profili sono pubblici e le informazioni sono pubblicate in modalità pubblica ed al fine di:

- Verificare il rispetto delle norme dell’Ente in materia di riservatezza, sicurezza informatica e condotta professionale.
- Proteggere l'immagine e la reputazione dell'Ente.
- Tutelare i propri interessi legittimi in caso di condotte illecite o dannose da parte dei dipendenti.

Sistemi informativi aziendali

I sistemi informativi aziendali sono l’insieme dei programmi (software), web e client, che consentono l’inserimento, l’archiviazione, l’elaborazione e la consultazione dei dati aziendali, sfruttando i dispositivi hardware le connessioni di rete/internet.

I sistemi informativi aziendali includono una vasta gamma di software dedicati alla gestione dei processi aziendali. Tra questi rientrano ad esempio i software per la gestione degli atti, del protocollo, della contabilità, degli stipendi e altri utilizzati nei vari settori dell'Ente. Tali applicativi sono fondamentali per l'inserimento, l'archiviazione, l'elaborazione e la consultazione dei dati aziendali e devono essere utilizzati secondo le procedure e le disposizioni stabilite dall'Ente.

In aggiunta, è importante menzionare la posta elettronica come uno strumento di comunicazione fondamentale nell'ambito aziendale. L'invio e la ricezione di email sono un aspetto critico della comunicazione interna ed esterna e devono essere gestiti in conformità con le politiche aziendali sulla sicurezza e la privacy dei dati così come

indicato nel capitolo relativo alla Posta Elettronica.

Infine, è essenziale considerare anche l'utilizzo di software di produttività aziendale ampiamente impiegati per la creazione e la gestione di documenti e fogli di calcolo aziendali. È fondamentale che gli utenti rispettino le norme di utilizzo stabilite per garantire la sicurezza e l'integrità dei dati aziendali anche durante l'utilizzo di tali software di produttività.

I sistemi informativi aziendali devono rispondere ai requisiti di confidenzialità, integrità, continuità del dato e riconducibilità al singolo Utente, come prescritto dal Regolamento Europeo 2016/679 per il trattamento dei dati personali.

Gli Utenti e gli Amministratori di sistema devono possedere le sole autorizzazioni strettamente necessarie ad effettuare il loro compito. In ogni caso, ciascuno deve astenersi da effettuare operazioni che, ancorché tecnicamente consentite dai sistemi, non rientrano nella propria mansione specifica.

Pertanto, gli applicativi software devono prevedere profili di autorizzazione di ambito diverso per diversi incaricati, in modo da consentire che solo alcuni di essi possano effettuare alcuni trattamenti o accedere a certi tipi di dato.

Periodicamente, con cadenza almeno annuale, sono aggiornati gli ambiti del trattamento consentito agli addetti, a cura degli Amministratori di sistema con il supporto dei vari responsabili dell'Ente.

Per un corretto utilizzo degli applicativi aziendali l'Utente deve:

- garantire la correttezza del dato, prevenendo il rischio di trattamenti impropri (inserimento di dati non corretti, mancato inserimento di dati, accesso a dati non pertinenti, ecc.);
- non utilizzare account assegnati ad altri Utenti;
- non comunicare ad altri le proprie credenziali personali di autenticazione, anche se solo temporaneamente;
- effettuare la pronta segnalazione di qualsiasi malfunzionamento.

L'abilitazione e disabilitazione dell'utente agli applicativi aziendali avviene solo su esplicita richiesta avanzata dal Responsabile del Servizio/Settore all'Amministratore di sistema o al Referente informatico, per il documentale da parte del responsabile della gestione documentale.

Per i sistemi informativi aziendali vi sono svariati tipi di log, quali:

- Log di autenticazione: Registrano l'accesso e l'uscita degli utenti dai sistemi informatici aziendali, comprese le informazioni su data, ora, dispositivo utilizzato e indirizzo IP.

- Log di attività: Registrano le azioni compiute dagli utenti all'interno dei sistemi informatici aziendali, come ad esempio l'apertura di file, l'invio di email, la modifica di dati.

- Log di sistema: Registrano eventi e anomalie che si verificano sui sistemi informatici aziendali, come ad esempio errori di software, intrusioni esterne o malfunzionamenti hardware.

Smart-working

Durante il lavoro in modalità smart-working, sia utilizzando dispositivi aziendali che personali, è fondamentale rispettare le prescrizioni di sicurezza indicate nel presente disciplinare. I dispositivi in questione includono PC, portatili e smartphone.

Se l'Utente lavora con un dispositivo aziendale, è tenuto a:

- Individuare uno spazio idoneo per predisporre la propria postazione lavorativa da utilizzare in modo esclusivo, ponendo ogni cura per evitare che ai dati possano accedere persone non autorizzate.
- Non lasciare mai incustodita la postazione di lavoro.
- Usare meccanismi come la cifratura dei dati per le pen-drive ed hard disk, e utilizzare password per gli account utenti del dispositivo al fine di impedire l'accesso non autorizzato.
- Bloccare il dispositivo quando ci si allontana dalla postazione di lavoro, anche per brevi periodi.
- Effettuare sempre il log-out dai servizi, portali utilizzati e dal PC al termine della sessione lavorativa.
- Riporre gli strumenti di lavoro in luoghi sicuri al termine di ogni sessione lavorativa.
- Conservare o distruggere con cura i documenti eventualmente stampati al termine della giornata lavorativa.

Se l'Utente utilizza un proprio dispositivo, deve inoltre:

- Utilizzare solo sistemi operativi raccomandati dal Servizio IT dell'Ente e mantenere costantemente aggiornati gli aggiornamenti.
- Installare un antivirus/antimalware raccomandato dal Servizio IT dell'Ente e mantenerlo sempre aggiornato.
- Effettuare regolarmente gli aggiornamenti di sicurezza del sistema operativo e del software antivirus.
- Utilizzare un account separato e una password sicura per l'uso lavorativo, evitando l'installazione di software non autorizzato.

È obbligatorio utilizzare software di produttività forniti dall'Ente, come Microsoft 365, quando si lavora con dati aziendali, sia su dispositivi aziendali che personali. L'utilizzo di software di condivisione e produttività diversi da quelli aziendali costituisce una grave violazione delle politiche aziendali e comporta seri rischi per il patrimonio informativo aziendale.

Per quanto riguarda l'uso di dispositivi non personali o di terzi:

- Evitare di utilizzare dispositivi non sicuri o di cui si ha dubbi sulla sicurezza.
- Assicurarsi che il PC disponga di un antivirus aggiornato.
- Utilizzare esclusivamente app web per le attività lavorative, evitando di memorizzare password nel browser.
- Eliminare definitivamente eventuali file di tipo aziendale scaricati sul PC di terzi.
- Disconnettersi da tutte le app al termine dell'utilizzo.

Sicurezza delle risorse informatiche

Nel contesto dell'evoluzione tecnologica e dell'aumento delle minacce informatiche, l'Ente adotta un approccio olistico alla sicurezza delle risorse informatiche, comprensivo di diverse pratiche e protocolli per garantire la protezione dei dati aziendali e la continuità operativa. Tra i principali pilastri di questa strategia, vi sono:

Zero Trust (fiducia zero)

Con l'evoluzione della tecnologia e l'aumento delle minacce informatiche è necessario adottare il modello **zero**

trust. Questo approccio alla sicurezza informatica si basa sulla premessa che ogni richiesta di accesso alla rete o ai dati aziendali debba essere sempre verificata, **indipendentemente dal fatto che provenga da una fonte esterna o interna all'Ente**. Per implementare il modello zero trust, l'Ente adotterà un insieme di soluzioni tecnologiche avanzate per identificare, autenticare e autorizzare gli utenti, i dispositivi e le applicazioni. Inoltre, l'Ente sta rivedendo e rafforzando le politiche di sicurezza per garantire che ogni utente e ogni dispositivo abbia solo l'accesso necessario per svolgere il proprio lavoro. Questo approccio alla sicurezza è proattivo e mira a garantire la protezione continua dei dati aziendali, garantendo allo stesso tempo un accesso sicuro e affidabile per i dipendenti e i vari portatori d'interesse (stakeholder).

Autenticazione a più fattori (MFA)

Al fine di garantire un elevato livello di sicurezza per gli accessi agli applicativi aziendali, si sta introducendo nell'Ente l'autenticazione a più fattori (Multi Factor Authenticator MFA). Laddove possibile, si utilizzerà questo sistema per proteggere l'accesso agli applicativi aziendali e per prevenire eventuali attacchi informatici. Con l'introduzione del MFA, agli Utenti sarà richiesto di fornire una seconda forma di autenticazione, come SMS o chiamate o dati biometrici o passcode monouso, oltre alle normali credenziali di accesso. Inoltre, in conformità con le direttive governative e le migliori pratiche di sicurezza informatica, l'Ente promuove attivamente l'adozione di metodi di autenticazione elettronica riconosciuti a livello nazionale come SPID e CIE. Queste soluzioni consentono agli Utenti di accedere agli applicativi aziendali utilizzando credenziali digitali ufficialmente riconosciute, aggiungendo un ulteriore strato di sicurezza e semplificando il processo di autenticazione. Laddove applicabile e appropriato, verrà incoraggiato l'utilizzo di tali metodi insieme al MFA, al fine di garantire una protezione robusta degli accessi e una user experience ottimizzata.

Backup e ripristino dati

Tutti i dati di lavoro su pc d'ufficio, ad esempio sul desktop documenti ed immagini, devono essere messi sotto backup in tempo reale tramite l'utilizzo di un servizio di cloud storage dell'Ente (es. Onedrive di Microsoft). Questo significa che i file importanti saranno al sicuro e potranno essere facilmente recuperati in caso di perdita o danneggiamento.
L'Utente pertanto deve:

- salvare tutti i dati importanti sulle cartelle sottoposte a backup in modo che siano protetti, e tenuto a cancellare file non più necessari
- deve monitorare il corretto funzionamento del servizio di cloud storage dall'app dalla barra delle applicazioni, verificando lo stato di sincronizzazione dei file, leggendo le notifiche su eventuali problemi e segnalando eventuali anomalie al Servizio IT

Cifratura dei dati

La sicurezza dei dati aziendali è una priorità assoluta per il nostro Ente e per questo motivo, si sta introducendo una politica di crittografia dei dispositivi per tutti i computer portatili e fissi. La crittografia dei dispositivi è una tecnologia che rende i dati dell'Ente illeggibili per chiunque non abbia l'autorizzazione per accedervi. In caso di smarrimento o furto del dispositivo, la crittografia garantisce che i dati sensibili dell'Ente non possano essere letti o utilizzati da terze parti non autorizzate. Il personale del Servizio IT custodirà le chiavi private per la decodifica.

Tutti i supporti rimovibili devono essere adeguatamente salvaguardati attraverso un sistema di criptazione.

Per l'invio a destinatari esterni di messaggi contenenti allegati relativi a dati personali particolari o giudiziari,

l'Utente è tenuto a renderli preventivamente illeggibili, criptandoli secondo indicazioni del Servizio IT.

Protezione antivirus

Tutti i dispositivi sono protetti da un unico software antivirus/antimalware dell'Ente, il quale viene aggiornato quotidianamente. È responsabilità di ogni utente verificare il corretto funzionamento del software antivirus installato sul proprio dispositivo e segnalare immediatamente qualsiasi malfunzionamento al Servizio IT.
Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà prontamente segnalare l'accaduto al servizio IT. In assenza di personale IT disponibile, l'utente deve spegnere il dispositivo infetto per prevenire la diffusione del virus.

Ogni dispositivo magnetico esterno al computer (pen-drive, hard disk ecc…) dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, non dovrà essere utilizzato. Si ricorda che l'utilizzo di dispositivi esterni non forniti direttamente dall'Ente richiede autorizzazione preventiva.

Ogni utente è tenuto ad adottare comportamenti atti a minimizzare il rischio di attacchi informatici e a collaborare attivamente per mantenere l'integrità del sistema informatico aziendale.

Sospensione automatica delle sessioni di lavoro.

La sospensione automatica della sessione di lavoro dopo un tempo minimo di inattività deve essere attivata su ogni postazione di lavoro (es. impostare timeout schermo o "screensaver" protetto da password) questo per permette, in caso di allontanamento dalla propria postazione di lavoro e dimenticanza di blocco manuale del dispositivo (WIN + L), di bloccare in automatico il proprio dispositivo e quindi di non lasciare incustodito il proprio dispositivo con le sessioni utenti attive. Ogni utente deve verificare il corretto funzionamento della sospensione automatica sul proprio dispositivo e segnalare qualsiasi malfunzionamento al Servizio IT.

Sanificazione digitale

Per il reimpiego e smaltimento di rifiuti di apparecchiature elettroniche occorre osservare un'adeguata politica di cancellazione per prevenire accessi non consentiti ai dati personali in esse contenuti.
Pertanto, per ottemperare agli obblighi imposti dal Regolamento UE 2016/679 e dal Garante per la protezione dei dati con provvedimento del 13 ottobre 2008, in caso di dismissione o cessione di apparecchiature IT, occorre cancellare in modo sicuro, definitivo e permanente tutte le informazioni in essi presenti, utilizzando misure tecniche che consentano di garantire la loro non intelligibilità o l´effettiva cancellazione dei dati.
Per quanto riguarda i supporti rimovibili contenenti dati particolari o dati giudiziari, gli stessi, se non utilizzati, devono essere distrutti o resi inutilizzabili; pertanto possono essere riutilizzati da altri soggetti solo se le informazioni precedentemente in essi contenute non sono più intelligibili, né in alcun modo tecnicamente ricostruibili.
E' compito dell'Amministratore di sistema (o Servizio IT) di curare la suddetta attività di sanificazione digitale.

Controlli e privacy dei lavoratori

Gli eventuali controlli saranno eseguiti in conformità della normativa vigente, con particolare riferimento al Regolamento Europeo 2016/679, al D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, all'articolo 4 comma 2 della della Legge 300/1970, come modificato dal D.Lgs. 14/09/2015 n°151 ed ai provvedimenti emanati dal Garante.
L'articolo 23 del D.lgs. 14 settembre 2015 n. 151 ("Jobs Act") ha modificato il contenuto dell'articolo 4 della Legge 300/1970, ora rubricato "Impianti audiovisivi e altri strumenti di controllo".

L'ADISU, al momento attuale, **non intende** dotarsi di strumenti **per controllare a distanza dell'attività lavorativa, e quindi la prestazione lavorativa,** sapendo che se ricorresse tale esigenza potrà avvenire solo tramite accordo sindacale o autorizzazione dell'ispettorato del lavoro così come il presente disciplinare sarà soggetto a revisione.
L'Agenzia, quindi, potrà effettuare controlli solo sulla strumentazione informatica elencata nel disciplinare utilizzata dal lavoratore **solo per rendere la prestazione lavorativa**.

A tale riguardo fornisce al lavoratore un'adeguata **informazione** ed **informativa** sugli strumenti, sulle regole previste per l'utilizzo lavorativo, ed eventualmente personale, degli strumenti di cui si tratta ed infine sulle modalità e i casi in cui potranno essere effettuati i controlli, a partire dai log o dagli strumenti di controllo di cui l'Ente si dota.

A tale scopo, con il presente Disciplinare, all'Utente è fornita adeguata informazione in ordine alla modalità d'uso degli strumenti e di effettuazione dei controlli, così come rende informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento UE 2016/679 (vedi successivo articolo sull'Informativa agli Utenti).
Il Titolare si riserva inoltre di aggiornare il presente disciplinare e la presente informativa in caso di modifiche alle modalità di monitoraggio o alle normative applicabili.

Al fine di mantenere la massima trasparenza ai lavoratori, in ottemperanza al GDPR, rispetto a quanto già indicato nel presente Disciplinare, il Titolare si impegna a comunicare, tramite i canali aziendali, informazioni relative ai controlli sui vari strumenti **per rendere la prestazione lavorativa** di cui si doterà e che saranno via via implementati nell'ambito dell'Agenzia nella cornice normativa di quanto indicato. Per tali strumenti di controllo si indicheranno, oltre al funzionamento, anche la tipologia di dati dei log ed i relativi tempi di conservazione sempre con l'obiettivo di esprimere chiaramente e in modo particolareggiato l'utilizzo di tali strumenti di controllo.

I controlli sull'uso degli strumenti elettronici, **per rendere la prestazione lavorativa,** saranno tali da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori e di soggetti esterni.
Gli eventuali controlli saranno commisurati allo scopo e saranno effettuati nel rispetto dei principi di necessità, pertinenza e non eccedenza, proporzionalità e gradualità; così come l'Agenzia, in qualità di datore di lavoro, si riserva la facoltà di effettuare controlli, anche saltuari o occasionali, che in nessun caso saranno prolungati, costanti o indiscriminati.
Di seguito si elencano le varie tipologie di controllo, indicando le ragioni legittime, specifiche e non generiche, per cui verranno effettuati questi controlli e le relative modalità

In caso di anomalie o malfunzionamenti, il personale incaricato effettuerà, mediante l'ausilio dei sistemi installati, **controlli graduali**, cioè controlli anonimi che si concluderanno con avvisi generalizzati diretti agli incaricati dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Solo

in caso di successive ulteriori anomalie, successive all'invio dell'avviso generalizzato, potranno essere computi controlli su base individuale (cfr., 6.1 Graduazione dei controlli - Linee Guida dell'Autorità Garante del 1° marzo 2007 – doc. web. 1387522).

I **controlli su base individuale** potranno essere effettuati in via eccezionale e tassativa, oltre che nell'ipotesi sopra menzionata indicata nel Controllo graduale, anche ove ricorra una o più delle seguenti ipotesi:

- quando venga presentata una specifica richiesta di informazioni da parte dell'Autorità giudiziaria;
- se imposta da una norma specifica di legge
- quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato e necessario intervento;

I dati raccolti dai predetti controlli potranno essere utilizzati per tutte le finalità connesse al rapporto di lavoro, nel rispetto della normativa sulla privacy e dello statuto dei lavoratori vigente.

Informativa agli Utenti ex art. 13 regolamento UE 2016/679

La presente informativa viene resa agli utenti assegnatari di strumentazione informatica abilitati ad internet, posta elettronica e sistemi informativi aziendali ai sensi del Codice in materia di protezione dei dati personali (GDPR 679/2016) e del Regolamento privacy ADISU.

1) Dati identificativi

Il titolare del trattamento dei dati è l'Adisu Puglia, in via G. Fortunato, 4/G – 70125 Bari, mail: direzionegenerale@adisupuglia.it

Il responsabile della protezione dei dati (RPD o DPO) a cui gli interessati possono rivolgersi per esercitare i propri diritti previsti nel GDPR è reperibile all'indirizzo mail: dpo@adisupuglia.it.

2) Finalità del trattamento e categorie di dati trattati

I dati personali degli Utenti (ad es. nome utente, indirizzo IP, registrazione degli accessi in file Log che comprendono gli orari in cui le operazioni vengono effettuate all'Utente ed altre informazioni relative agli accessi alle risorse informatiche) saranno trattati esclusivamente per le seguenti finalità:

- esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale (ad es. sicurezza del sistema informativo, assistenza tecnica e sistemistica, controllo e programmazione dei costi aziendali, ecc.);
- effettuazione di controlli per verificare il rispetto delle regole dettate con il ~~presente Regolamento interno~~; Disciplinare per l'uso degli strumenti informatici, internet, posta elettronica e dei sistemi informativi e tutte le comunicazioni, tramite i canali aziendali, sulle informazioni relative ai controlli sui vari strumenti per rendere la prestazione lavorativa;
- finalità difensive.

I dati personali raccolti per le finalità indicate nel Regolamento dell'Agenzia formeranno oggetto di trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali.

In particolare, il trattamento dei dati sarà improntato al rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati (i dati raccolti saranno adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati), esattezza, integrità e riservatezza.

3) Base giuridica del trattamento
Il trattamento dei dati personali è necessario per:

- l'esecuzione del contratto di cui l'interessato è parte;
- l'esecuzione di un compito di interesse pubblico;
- l'adempimento degli obblighi e l'esercizio dei diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro, in conformità alle norme vigenti in materia.

4) Modalità di trattamento
Il trattamento dei dati per le finalità esposte ha luogo con modalità sia automatizzate, su supporto elettronico o magnetico, sia non automatizzate, su supporto cartaceo, nel rispetto delle regole di riservatezza e di sicurezza previste dalla legge, dai regolamenti conseguenti e da disposizioni interne.

5) Natura del conferimento
Il conferimento dei dati personali è obbligatorio per le finalità sopra indicate. Nel caso di opposizione al trattamento non potrà essere consentito l'uso della strumentazione informatica di lavoro.

6) Processo decisionale automatizzato
Non esiste alcun processo decisionale automatizzato. I dati non saranno oggetto di profilazione.

7) Destinatari e categorie di destinatari
I dati saranno trattati da personale dipendente o da altri soggetti che collaborano con l'Agenzia, tutti debitamente a ciò autorizzati dal Titolare o da un suo delegato, nonché da soggetti appositamente designati dal Titolare quali Responsabili del trattamento dei dati personali.
I dati personali non verranno in alcun modo diffusi e potranno essere comunicati all'Autorità Giudiziaria e/o all'Autorità di Pubblica Sicurezza ed ad altri Soggetti, nei casi previsti dalla legge.

8) Trasferimento dei dati all'estero
I dati vengono attualmente trattati ed archiviati presso la sede, per la funzione, in via G. Fortunato 4/G - 70125 Bari. I dati personali non saranno comunicati presso Paesi Terzi non europei.

9) Tempi di conservazione dei dati
I dati personali saranno conservati conformemente ai principi di cui all'art. 5 GDPR 2016/679, per un arco di tempo non superiore al conseguimento delle finalità per cui sono stati raccolti con specifico riguardo al principio di limitazione della conservazione dello stesso articolo, in tutte le fasi del rapporto con gli utenti (assunzione/attivazione, gestione, cessazione). Come da regola generale, le informazioni saranno trattate per la sola durata del rapporto di lavoro.
Tempi maggiori di conservazione potranno essere applicati:

- per assicurare continuità operativa immediatamente dopo la cessazione del rapporto di lavoro;
- quando si prospetta la necessità di far valere o difendere diritti in sede giudiziaria Suoi, del Titolare o di terzi;
- per fini amministrativi e fiscali;
- quando richiesto da autorità esterne o da normative speciali (per es. nel caso della conservazione del file di log ai soli fini di giustizia).

In ogni caso, dopo la cessazione del rapporto di lavoro si applicherà il principio di minimizzazione e anonimizzazione, quando tecnicamente possibile.

10) Diritti dell'interessato
Lei ha il diritto di chiedere ad A.D.I.S.U. – Puglia, in qualunque momento, l'accesso ai suoi dati personali, qualora

intenda operare una rettifica o la cancellazione degli stessi o di opporsi al loro trattamento; ha diritto, altresì, di richiedere la limitazione del trattamento nei casi previsti dall'art. 18 del Regolamento, nonché di ottenerne copia in un format strutturato, semplice e facilmente consultabile da dispositivo automatico in tutti i casi previsti dall'art. 20 del medesimo Regolamento. Le summenzionate e motivate richieste potranno essere rivolte all'indirizzo di posta elettronica dpo@adisupuglia.it . In ogni caso, qualora riscontri che sia stato leso un Suo diritto sulla privatezza dei suoi dati, potrà proporre reclamo all'autorità di controllo competente (Garante per la Protezione dei Dati Personali), ai sensi dell'art. 77 del Regolamento.

Norme finali

Le disposizioni del presente Regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete aziendale da postazioni esterne all'Agenzia.
Si applicano, altresì, per quanto compatibili, alla modalità di lavoro agile **(smart-working)**, anche nel caso sia consentito l'utilizzo di strumenti propri dell'Utente.

Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del documento principale "Regolamento generale per il trattamento e la protezione dei dati personali".

Pubblicazione

Il presente disciplinare è pubblicato sull'Albo Pretorio e sul sito web dell'Agenzia. Una copia è trasmessa, tramite e-mail, a cura degli Uffici competenti, a tutti i lavoratori, garantendo la piena diffusione delle informazioni in esso contenute.