Regolamento privacy

Regole di comportamento per il corretto trattamento dei dati personali ed utilizzo degli strumenti e sistemi di trattamento di Azienda Ambiente s.r.l.

1. SCOPO DEL PRESENTE DOCUMENTO

1.1 Lo scopo del presente documento (Regolamento Privacy) è definire un insieme di norme comportamentali cui tutti i dipendenti, i collaboratori ed eventuali terze parti, che operano Azienda Ambiente s.r.l. (da ora Azienda Ambiente) in coerenza con i vincoli normativi e regolatori dello specifico business, devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

1.2 Il presente Regolamento è realizzato in conformità alle richieste previste dal Regolamento generale sulla protezione dei dati (UE) 2016/679 - General Data Protection Regulation (di seguito anche GDPR) del D.Lgs 196/2003 e sue successive modifiche introdotte dal D.Lgs 101/2018 e dai Provvedimenti del Garante, costituendone la base per le lettere di nomina e autorizzazione.

1.3 Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, dirigenti, consulenti esterni nonché a tutti i collaboratori di Azienda Ambiente a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, ecc.).

2. DEFINIZIONI

DATI PERSONALI. I dati personali sono qualunque informazione relativa a persona fisica identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Si sottolinea l'importanza di comprendere quando un dato è considerato sensibile: a questi dati è infatti garantita una tutela più intensa, per cui sono imposti maggiori obblighi ed oneri nell'effettuare il trattamento e nella loro custodia.

I dati personali si suddividono nelle seguenti categorie:

- I dati particolari (*art. 9 GDPR*): sono i dati sensibili cioè i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale. Inoltre, appartengono a questa categoria i dati biometrici e genetici.
- I dati giudiziari (*art.10 GDPR*) sono i dati idonei a rilevare informazioni riguardo provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- I dati che presentano rischi specifici: Il trattamento dei dati diversi da quelli particolari e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
- I dati comuni: i dati identificativi diversi da particolari, giudiziari e rischiosi.

IL TRATTAMENTO DEI DATI PERSONALI corrisponde a qualunque operazione o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione mediante trasmissione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati. E' quindi indifferente che le

operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

LA COMUNICAZIONE DI DATI PERSONALI corrisponde nel dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile del trattamento, dal responsabile e dagli autorizzati al trattamento dei dati, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

LA DIFFUSIONE DI DATI PERSONALI avviene quando viene data conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

TITOLARE DEL TRATTAMENTO (TITOLARE) è l'organizzazione nel suo complesso nella persona del suo Legale Rappresentante che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

RESPONSABILE (INTERNO) DEL TRATTAMENTO è la persona fisica preposta dal Titolare - per finalità esclusivamente organizzative interne aziendali - al controllo delle procedure e modalità di trattamento dei dati personali in base alle scelte organizzative.

RESPONSABILE ESTERNO DEL TRATTAMENTO (art. 28 GDPR) è il fornitore esterno (outsourcer) a cui il Titolare ha affidato lo svolgimento di un'attività che comporta trattamento di dati personali.

AMMINISTRATORE DI SISTEMA: è la persona preposta dal Titolare cui spetta la gestione della sicurezza del sistema informatico.

AUTORIZZATO AL TRATTAMENTO: è la persona fisica autorizzata a compiere operazioni di trattamento dati in base alle regole definite dall'organizzazione.

TERZO: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

DATA PROTECTION OFFICER: persona fisica nominata dal Titolare che, ai sensi degli artt. 37-39 del succitato GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione privacy definite dal Titolare, assiste il Titolare sulla valutazione di impatto privacy e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

DATA BREACH: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

PROFILAZIONE: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

PSEUDONIMIZZAZIONE: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

ARCHIVIO: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

CONSENSO DELL'INTERESSATO: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

DATO AZIENDALE: tutti i dati e le informazioni aziendali (strutturati o destrutturati, in qualunque) non direttamente riferite a persona fisica, trattati da Azienda Ambiente. Tali dati e informazioni rappresentano una proprietà aziendale, patrimonio di Azienda Ambiente.

DATO COMMERCIALMENTE SENSIBILE dati e le informazioni commercialmente sensibili sono tutti i dati e le informazioni che, singolarmente o in forma aggregata, possono procurare anche solo potenzialmente ingiusto vantaggio competitivo a favore di uno o di alcuni operatori del mercato energetico (esercenti l'attività di produzione, di acquisto e vendita di energia elettrica e /o calore).

3. ACCESSO ALLA SEDE, AGLI UFFICI ED AREE PROTETTE

L'accesso alla sede aziendale è permesso solo a personale in base a precise e motivate esigenze di lavoro.

Le terze parti (clienti, fornitori, consulenti, visitatori, esterni) potranno avere accesso alle aree aziendali non aperte al pubblico esclusivamente previo annuncio al personale di accettazione e/o sportello nelle modalità definite da apposita policy aziendale adottata in merito dalla Direzione.

4. CUSTODIA DELLE CHIAVI FISICHE AZIENDALI

Le chiavi fisiche di accesso alle aree ed agli uffici sono rilasciate ad alcune figure in base ad esigenze di lavoro, con firma dell'incaricato di ricevuta sull'apposito registro. La gestione di tali chiavi è di responsabilità del dipendente. Tali chiavi dovranno essere gestite secondo le seguenti indicazioni:

- non dovranno mai rimanere incustodite;
- non dovranno mai essere cedute a terzi esterni;
- non dovranno mai essere duplicate;
- non devono identificare il nome della società;
- il dipendente dovrà avvisare immediatamente la Direzione in caso di smarrimento o altra anomalia.

5. POSTAZIONE DI LAVORO FISICA

L'utilizzo della postazione di lavoro e il conseguente accesso ai documenti, atti e archivi è consentito nei limiti della propria funzione e dei propri incarichi assegnati.

Sulla propria postazione di lavoro non si devono lasciare documenti ed atti riservati e/o contenenti dati sensibili senza un proprio controllo all'accesso di terzi, in momenti di pausa, terminata la giornata di lavoro e/o in periodi di assenza.

6. GESTIONE DEI DATI E DELLE INFORMAZIONI

Ogni incaricato è responsabile dei dati e delle informazioni personali e aziendali delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza ed il corretto utilizzo.

Il trattamento di qualunque dato e informazione personale e aziendale nell'ambito della propria attività lavorativa, deve prevedere da parte del collaboratore incaricato, ogni ragionevole misura per assicurare l'integrità di tali dati. I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito della propria funzione e secondo le finalità connesse alla propria attività lavorativa.

È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del know-how ed alla redditività aziendale, che possano violare i vincoli contrattuali e di legge connessi al rapporto di lavoro e che possano ledere i diritti di riservatezza dell'interessato (diritto alla privacy).

È assolutamente vietata la divulgazione a terzi di informazioni sensibili, particolari o riservate o comunque di proprietà del Titolare, senza espressa autorizzazione della Direzione.

In caso di violazione il Titolare si riserva di avviare i relativi provvedimenti disciplinari, nonché le azioni civili e penali consentite.

7. MISURE FISICHE DI CUSTODIA DEI DOCUMENTI E ATTI CARTACEI

I dati cartacei ed i documenti necessari allo svolgimento delle attività lavorative devono essere custoditi nel proprio ufficio e/o nei luoghi deputati ad archivio. Tutti gli archivi cartacei sono ad accesso limitato, per cui è possibile accedervi nei limiti della necessità per prelevare e riporre i documenti ed i supporti informatici necessari per lo svolgimento delle proprie attività lavorative.

Gli archivi di documenti e atti contenenti dati personali particolari (Risorse Umane) dovranno essere custoditi in armadi chiusi a chiave.

L'eliminazione fisica di documenti cartacei contenenti dati e informazioni di natura particolare o riservata deve essere effettuata dopo aver distrutto/stracciato fisicamente il documento, eventualmente utilizzando l'apposito elimina-documenti.

8. POSTAZIONE DI LAVORO

L'accesso ai dati, programmi e risorse informatiche, è consentito nei limiti della propria funzione aziendale e della propria attività lavorativa. In generale la postazione di lavoro e sue periferiche (monitor e stampante) devono essere spenti ogni sera, prima di lasciare gli uffici, a maggior ragione in caso di assenze prolungate dall'ufficio e nel fine settimana.

È obbligatorio non lasciare incustodito o accessibile la propria postazione di lavoro durante una pausa di lavoro. Per questo motivo i dispositivi devono essere bloccati manualmente se lasciati incustoditi e devono inoltre essere dotati di uno screen saver, protetto da password, ad attivazione automatica.

Salvo preventiva espressa autorizzazione da parte della Direzione o degli Amministratori di sistema, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC o Notebook né procedere ad installare software, dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.) non autorizzate dall'Amministratore di Sistema.

9. GESTIONE DELLE CREDENZIALI DI ACCESSO ALLA RETE AZIENDALE (LOGIN E PASSWORD)

L'accesso alla rete aziendale attraverso i sistemi informatici può avvenire esclusivamente se preventivamente identificati ed autenticati, pervia verifica delle proprie credenziali di accesso di cui ogni utente dovrà averne cura.

È necessario prestare la massima attenzione nell'utilizzo, gestione e conservazione delle password necessarie all'accesso dei sistemi informatici assegnate dall'Amministratore di sistema.

La policy per la gestione della password per l'accesso al dominio è definita dall'Amministratore di sistema e deve essere applicata da ogni utente. Si compone dei seguenti criteri:

- utilizzare solamente password che rispettino i criteri di complessità previsti (8 caratteri alfanumerici);
- effettuare il cambio password ogni 6 mesi, come indicato dal sistema.

L'utente dovrà attenersi alle seguenti prescrizioni:

- la password è strettamente personale e non può essere comunicata a nessun altro utente/terza parte;
- non annotare la propria password all'interno dell'ufficio, o di conservarla on-line;
- nel caso qualcuno insista nel cercare di conoscere la propria password contattare la Direzione;
- in caso di dimenticanza e/o ripristino della password, dovrà essere inoltrata una richiesta all'Amministratore di sistema.

Nell'ambito della gestione delle credenziali di autenticazione e dei profili utente ricordiamo che è compito dell'Amministratore di sistema:

- verificare la correttezza degli accessi al sistema riportando eventuali abusi;
- verificare periodicamente la coerenza dei profili utente con le responsabilità/attività assegnate in collaborazione con la Direzione.

All'utente non è consentita la modifica della struttura di rete aziendale e l'uso per scopi personali.

10. SOFTWARE ANTIVIRUS

La gestione (installazione, aggiornamento, ecc..) del software antivirus è di competenza dell'Amministratore di sistema. Tuttavia, è necessario che ogni utente eviti di disabilitare, per qualsiasi motivo, il sistema antivirus.

In caso di segnalazione dal sistema antivirus del proprio PC o Notebook di eventuali anomalie e/o avvisi è necessario comunicare tali segnalazioni all'Amministratore di sistema.

11. GESTIONE DEL SOFTWARE

Ogni utente deve utilizzare esclusivamente i software e le applicazioni di cui dispone l'organizzazione.

Non è quindi consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare. Di conseguenza non è consentito all'utente installare autonomamente alcun programma informatico senza la previa autorizzazione della Direzione o dell'Amministratore di Sistema. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (*Decreto Legislativo 518/92 sulla Tutela giuridica del software e Legge 248/2000 Nuove*

norme di tutela del diritto d'autore). È inoltre vietato immettere sulla rete e server aziendali software dannoso per i sistemi o comunque non autorizzato.

12. GESTIONE DELLA POSTA ELETTRONICA AZIENDALE

L'assegnazione di una casella e-mail (personale o di gruppo) è finalizzata all'utilizzo della stessa esclusivamente per finalità legate alla attività lavorativa. Gli utenti della posta elettronica sono responsabili del corretto utilizzo della stessa e devono mantenere un corretto comportamento nell'utilizzo dello strumento di posta elettronica, sia nei messaggi inviati internamente che esternamente.

In particolare, devono essere seguite le seguenti disposizioni:

- la casella di posta elettronica aziendale (personale o di gruppo) non deve essere utilizzata per l'invio o la ricezione di messaggi personali al di fuori dalle finalità lavorative o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione della Direzione;
- non inviare né conservare messaggi di posta elettronica e/o allegati dal contenuto offensivo, molesto, volgare, blasfemo, xenofobo, razziale, pornografico o comunque inappropriato o illegale;
- deve essere prestata la massima attenzione nell'inoltro di mail riportanti contenuti e indirizzi e-mail di precedenti comunicazioni;
- in caso di assenza (ferie, malattia, aspettativa, attività fuori sede) l'utente deve prevedere delle opportune procedure in collaborazione con il suo responsabile di funzione, in grado di garantire la continuità delle attività.

Si avvisano gli utenti che:

- tutta la posta elettronica in entrata è controllata da un software antispam. È comunque possibile che alcune mail di spam superino i filtri impostati sul sistema centrale: quindi è necessario prestare la massima attenzione a e-mail sospette, avvisando l'Amministratore di sistema in caso di dubbi sulla provenienza/contenuto delle stesse.
- tutti i messaggi ricevuti, spediti o salvati, potranno essere letti della Direzione esclusivamente nei seguenti casi:

  a. in caso di improvvisa assenza dell'utente al fine di garantire una regolare continuità dell'attività lavorativa;

  b. per motivi di sicurezza informatica.

In questi casi sarà data informazione all'utente dell'accesso eseguito.

13. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale è utilizzata esclusivamente dal Titolare della stessa. La Firma Digitale potrà essere utilizzata esclusivamente da coloro che sono stati preventivamente autorizzati di volta in volta dal Titolare stesso.

14. NAVIGAZIONE INTERNET

L'accesso ad Internet (*tramite PC, tablet o smartphone aziendali*) è fornito allo scopo di consentire l'accesso alle informazioni necessarie all'attività lavorativa. Essendo uno strumento di lavoro, gli utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo.

Si informa che il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati. La consultazione di tali registrazioni può avvenire solo in forma anonima e aggregata salvo i casi previsti dalla legge. Per prevenire eventuali abusi nell'uso di Internet il sistema è provvisto di filtri d'accesso.

Si devono comunque osservare le seguenti regole di navigazione della rete Internet:

- è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore, che siano essi appartenenti a persone o aziende, coperti da *copyright*, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non sia specificatamente licenziato per essere utilizzato all'interno dell'azienda;
- è tassativamente vietato navigare siti e scaricare materiale vietato o aventi contenuti illegali;
- è vietato effettuare copia non autorizzata di materiale coperto da copyright compreso, ma non limitato a, digitalizzazione e distribuzione di foto da riviste, libri o altre fonti, musica o materiale video;
- è vietata la condivisione di file in modalità peer-to-peer;
- è vietato scaricare programmi, anche se privi di licenza o in prova (*freeware e shareware*), se non in caso di espressa autorizzazione dell'Amministratore di sistema. Eseguire il download di file da Internet è infatti un'operazione pericolosa in quanto può essere il veicolo per l'introduzione di *virus e malware*.
- è vietato utilizzare l'infrastruttura tecnologica aziendale per procurarsi e diffondere materiale in violazione delle normative vigenti.
- è vietato eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati *all'host* dell'utente (*sniffing*);
- è vietato aggirare le procedure di autenticazione o la sicurezza di qualunque *host*, rete, *account*.

15. ACCESSO INTERNET PER TERZI ESTERNI – WIFI GUEST

È previsto un sistema per consentire l'accesso ad Internet a terzi esterni. L'accesso alla rete (*tramite PC, tablet o smartphone*) è fornito allo scopo di consentire la navigazione a clienti, fornitori, terzi esterni e non a utenti interni. Gli utenti cui si attribuisce l'accesso, sono responsabili del suo corretto utilizzo. Si informa che il numero, la durata ed il contenuto degli accessi ad Internet sono costantemente registrati. Per prevenire eventuali abusi nell'uso di Internet il sistema è provvisto di filtri d'accesso.

16. ACCESSO DA REMOTO - VPN

Il collegamento alla rete aziendale da remoto è autorizzato dalla Direzione per esigenze di lavoro nelle modalità previste dall'azienda attraverso VPN con credenziali personali. Per motivi di sicurezza tutti gli accessi realizzati dagli utenti da remoto sono registrati. Le registrazioni comprendono i riferimenti temporali di accesso.

17. COMUNICAZIONE DI DATI E INFORMAZIONI ATTRAVERSO SOCIAL MEDIA

È assolutamente vietato pubblicare in internet attraverso Social media personali, forum, chat, blog, siti internet, dati ed informazioni di carattere aziendale e personale dipendente (informazioni, documenti, appunti, commenti personali o di terzi, foto, video, audio, ecc..) non autorizzati dalla Direzione aziendale.

È invece autorizzata la divulgazione di informazioni già rese pubbliche dall'azienda.

18. GESTIONE DI DATI E INFORMAZIONI ATTRAVERSO SISTEMI WEB CLOUD

È vietato il salvataggio di dati e informazioni di carattere aziendale in sistemi *cloud* (per esempio *Dropbox, Google+, iCloud, Evernote, ecc..*) non autorizzati dalla Direzione e dall'Amministratore di sistema.

19. SISTEMI DI MONITORAGGIO RETE AZIENDALE

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/ sostituzione/ implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà del Titolare, tramite l'Amministratore di sistema, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali.

Periodicamente e in presenza di anomalie (intervento antivirus, segnalazione di rallentamenti del computer, utilizzo aziendalmente eccessivo dell'accesso Internet, dimensione elevata della casella di posta elettronica o dello spazio disco utilizzato, etc.), l'amministratore di sistema effettuerà verifiche di funzionalità approfondite che potranno determinare segnalazione ed avvisi generalizzati diretti ai dipendenti della funzione in cui è stata rilevata l'anomalia stessa e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

20. UTILIZZO DI SMARTPHONE E TELEFONI AZIENDALI

L'utilizzo del telefono fisso aziendale deve essere limitato allo svolgimento delle attività lavorative salvo autorizzazione della Direzione.

L'utilizzo di *Smartphone* o *Tablet* è di responsabilità dell'utente e deve avvenire attraverso l'attivazione di una password o un PIN personale (attivazione dello screen saver automatico). Si raccomanda la massima attenzione nell'utilizzo di *App* sul proprio dispositivo, in relazione all'eccessivo consumo di traffico dati ed alla sicurezza del proprio apparato.

21. UTILIZZO DELLE STAMPANTI

È vietato l'utilizzo per fini personali dei sistemi multifunzione (sistemi di stampa, copia ed invio fax) e dei sistemi fax e aziendali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte della Direzione.

Si raccomanda di non lasciare documenti incustoditi presso i suddetti dispositivi.

In caso di stampa di documenti contenenti informazioni riservate e/o particolari presso dispositivi collocati in aree comuni è necessario l'impiego del sistema di protezione della stampa mediante impostazione di codice di sblocco attivabile dal dispositivo stesso.

L'utilizzo delle stampe PDF su carta intestata mediante generazione di file in cartella pubblica comporta l'obbligo da parte dell'utente di prelevare e cancellare immediatamente il file generato dalla cartella pubblica di destinazione.

22. UTILIZZO DEI SUPPORTI DI MEMORIZZAZIONE

Al termine dell'utilizzo dei supporti di memorizzazione contenenti dati (chiavette USB, Hard Disk interni ed esterni), questi dovranno essere cancellati, per eliminare ogni informazione contenuta prima di autorizzarne qualunque tipo di nuovo utilizzo. In caso di smaltimento di DVD e CD è obbligo la distruzione fisica del supporto.

23. CUSTODIA DI STRUMENTI INFORMATICI PORTATILI

Gli strumenti informatici portatili (*notebook, tablet, smartphone*, supporti di memorizzazione, ecc..) devono essere custoditi dall'utente con cura e diligenza, prevenendo possibili danneggiamenti che ne compromettano il corretto funzionamento, evitando di lasciarli incustoditi in ambienti pubblici (ristoranti, treni, automobili, ecc..). Inoltre, di norma, non ne deve essere consentito l'utilizzo da parte di terzi (famigliari, amici, etc.).

24. GESTIONE DELLE VIOLAZIONI DATI PERSONALI – DATA BREACH

La rilevazione di un evento che possa configurarsi come una violazione di dati personali, deve essere comunicata senza ritardo via e-mail all'indirizzo di posta elettronica interno dedicato: privacy@aziendaambiente.it per una sua valutazione, quindi eventuale applicazione della procedura di gestione della violazione.

25. SPECIFICI DIVIETI

E' vietato specificatamente quanto segue:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;

- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico di soggetti, pubblici o privati, le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;
- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
- caricare programmi non provenienti da una fonte certa e autorizzata dalla Società;
- acquistare licenze software da una fonte (rivenditore o altro) non certificata e non in grado di fornire garanzie in merito all'originalità/autenticità del software;
- detenere supporti di memorizzazione di programmi non originali (DVD\CD\floppy);
- installare un numero di copie di ciascun programma ottenuto in licenza superiore alle copie autorizzate dalla licenza stessa, al fine di evitare di ricadere in possibili situazioni di underlicensing;
- utilizzare illegalmente password di computer, codici di accesso o informazioni simili per compiere una delle condotte sopra indicate;
- utilizzare strumenti o apparecchiature, inclusi programmi informatici, per decriptare software o altri dati informatici;
- distribuire il software aziendale a soggetti terzi;
- realizzare codice software che violi copyright di terzi;
- accedere illegalmente e duplicare banche dati.

26. PRESCRIZIONE RESIDUALE

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati e delle informazioni personali e aziendali, nonché sulle modalità di utilizzo degli strumenti di trattamento, è possibile chiedere alla Direzione o all'Amministratore di sistema per ricevere le opportune istruzioni.

27. SANZIONI

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite

28. AGGIORNAMENTO E REVISIONE

Il presente Regolamento è soggetto a revisione periodica, opportunamente comunicata al personale.

Data

_____

La Direzione