Fiemme Servizi

Regolamento privacy Fiemme Servizi S.p.A.

Regole di comportamento in materia di trattamento dei dati personali e aziendali, di utilizzo degli strumenti e dei sistemi informatici

0. SCOPO DEL PRESENTE DOCUMENTO

Lo scopo del presente documento è quello di definire un insieme di norme comportamentali cui tutti i dipendenti, i collaboratori ed eventuali terze parti che operano per **Fiemme Servizi S.p.A. (da ora Titolare)** devono uniformarsi nell'ambito delle attività che implicano un trattamento di dati ed informazioni.

Il Regolamento è realizzato in conformità alle richieste previste dal Regolamento EU 2016/679 – General Data Protection Regulation – (da ora GDPR), del Decreto Legislativo 196/2003 come modificato dal Decreto Legislativo 101/2018 e dai Provvedimenti del Garante per la Protezione dei dati Personali.

Il Regolamento si applica a tutti i dipendenti, come parte integrante delle Autorizzazioni al trattamento, senza distinzione di ruolo e/o livello, dirigenti, consulenti esterni nonché a tutti i collaboratori del Titolare a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, ecc.).

Si esplicita che tutti gli utenti nell'ambito della loro attività e dei loro diritti d'accesso sono nominati, in forma diretta dal Titolare oppure indiretta dal Responsabile del trattamento (aziende partner e fornitori nominati Responsabili del trattamento ai sensi dell'art. 28 del GDPR), quali "Autorizzati al trattamento dei dati ai sensi dell'art. 29 del GDPR" nei limiti dei compiti e delle abilitazioni attribuite.

1. DEFINIZIONI

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari (ex art. 9 del GDPR): sono 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. Fanno parte dei dati particolare anche:

- **dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
- **dati biometrici**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati giudiziari (ex art. 10 del 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.

Dati rischiosi: dati personali diversi da dai dati particolari e giudiziari che presentano 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.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione,

l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

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.

Anonimizzazione: processo mediante il quale i dati personali sono modificati in modo irreversibile così che il Titolare del trattamento, da solo o in collaborazione con altre parti, non possa più identificare direttamente o indirettamente l'interessato.

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.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Autorizzato al trattamento: è la persona fisica autorizzata a compiere operazioni di trattamento dati in base alle regole definite dall'organizzazione del Titolare.

Interessato del trattamento: è la persona fisica alla quale si riferiscono i dati personali oggetto di trattamento.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Violazione dei dati personali: la 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.

Dato aziendale: tutti i dati e le informazioni aziendali (strutturati o destrutturati, in qualunque) non riferite a persona fisica, trattati nell'ambito di **Fiemme Servizi**. Tali dati e informazioni rappresentano una proprietà aziendale, patrimonio di **Fiemme Servizi**.

2. ACCESSO ALLA SEDE, AGLI UFFICI ED AREE PROTETTE

L'accesso alla sede del Titolare avviene attraverso badge e/o chiave personale.

L'accesso agli uffici, alla Sala Server ed alle aree del Titolare è permesso solo a personale incaricato dalla Direzione in base a precise e motivate esigenze di accesso a tali ambienti ed esclusivamente per finalità lavorative.

Le terze parti (clienti, fornitori, consulenti, visitatori, esterni) potranno avere accesso alle aree del Titolare esclusivamente se accompagnati da personale interno a seguito di identificazione presso la segreteria.

Il personale interno e le terze parti dovranno rispettare gli accessi, la fruizione ed il controllo delle aree come definito dalla Direzione.

3. CUSTODIA DELLE CHIAVI FISICHE AZIENDALI E DEL BADGE

Le chiavi fisiche ed il badge di accesso alle aree ed agli uffici sono rilasciate agli incaricati, 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.

4. 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 scrivania 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.

5. 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.

6. 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 sensibili (Ufficio Affari Legali e Risorse Umane) dovranno essere custoditi in armadi chiusi a chiave.

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

7. 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 al massimo dopo 15 minuti di inattività.

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.

8. 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. Qualunque variazione delle credenziali di accesso alla rete aziendale/applicazioni/data base/archivi/cartelle/risorse dei sistemi dovrà essere concordata ed autorizzata dalla Direzione e resa operativa dall'Amministratore di sistema.

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.

9. 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.

10. 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.

11. GESTIONE DELLA POSTA ELETTRONICA AZIENDALE

L'assegnazione di una casella email (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 email di precedenti comunicazioni;
- in caso di assenza prolungata (ferie, malattia, aspettativa, lunga attività fuori sede) l'utente deve prevedere delle opportune procedure in collaborazione con l'Amministratore di sistema, 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 email 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.

12. UTILIZZO DELLA FIRMA DIGITALE

La Firma Digitale è utilizzata esclusivamente dalla Direzione. Potrà essere utilizzata esclusivamente da coloro che sono stati preventivamente autorizzati dalla Direzione.

13. CRITTOGRAFIA

È vietate forme di utilizzo della cifratura (crittografia) che rendano illeggibili informazioni aziendali o che possano causare il blocco di applicazioni, senza che tale tecnica sia stata condivisa ed autorizzata dalla Direzione.

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

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.

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. MISURE DI RISERVATEZZA PER LA REALIZZAZIONE DI VIDEO-CONFERENZE

La realizzazione di una riunione in videoconferenza deve essere realizzata in un ambiente riservato, attraverso gli strumenti definiti dal Titolare (o eventualmente attraverso gli strumenti richiesti dal Cliente o dal Fornitore).

È assolutamente vietato effettuare registrazioni audio/video o fare fotografie durante le attività di videoconferenza, che possano interessare le persone collegate in video o in audio.

25. SISTEMA DI VIDEOSORVEGLIANZA

Il sistema di videosorveglianza è realizzato in alcune aree delle sedi del Titolare (perimetro esterno dell'azienda, magazzino e area ingressi) con finalità di sicurezza e controllo da accessi non autorizzati, per tutelare il patrimonio della società contro atti vandalici, comportamenti illeciti e/o fraudolenti. L'accesso alle immagini videoregistrate è permesso esclusivamente per le finalità sopra indicate ad incaricati del trattamento del Titolare ed in caso di necessità agli organi di polizia preposti.

26. SISTEMI DI GEOLOCALIZZAZIONE

Il sistema di geolocalizzazione installato sulla flotta impiegata nel servizio di raccolta rifiuti risponde unicamente ad esigenze organizzative e produttive del processo di raccolta rifiuti, oltre ad esigenze di tutela del patrimonio aziendale. Il sistema informativo installato sui mezzi non deve essere manomesso o modificato. L'eventuale associazione del mezzo, del percorso realizzato e dell'identità del personale presente sui mezzi (dati presenti su altro data base informatico) potrà essere posto in essere solo al verificarsi di eventi che ne richiedano la necessità di incrocio dei dati:

a) concreta ricorrenza di anomalie nel percorso o nel processo di raccolta rifiuti;

b) richiesta di controllo percorso da parte degli utenti del servizio di pubblica utilità (cittadini titolari di utenza);

c) verificarsi di eventi di sicurezza sulla flotta che richiedono al Titolare di verificare il percorso realizzato dai mezzi.

27. SEGNALAZIONE E GESTIONE VIOLAZIONI PRIVACY

La rilevazione di un evento che possa configurarsi come una violazione dei dati personali (violazione della privacy di clienti o dipendenti o fornitori) deve prevedere la pronta segnalazione dell'evento al Data Protection Officer di Fiemme Servizi attraverso e-mail dedicata: privacy@fiemmeservizi.it , cui seguirà la presa in carico dell'evento.

28. 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.

29. 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.

30. AGGIORNAMENTO E REVISIONE

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

Data, 23/06/2022

La Direzione