Decreto dell'Amministratore Unico

n. 36/2021 del 15/03/2021

Oggetto: Approvazione Privacy Policy e Organigramma Policy dell'Ente

L' Amministratore Unico

Vista la L.R. n. 44/2019 "Norme per il riassetto del Consorzio per la Zona Industriale Apuana. Modifiche all'articolo 32 quater della l.r. 82/2015", pubblicata sul Bollettino Ufficiale n. 35, parte prima, del 24.07.2019;

Vista la delibera dell'Assemblea del Consorzio Z.I.A. del 31.01.2020 con la quale è stato nominato Amministratore Unico del Consorzio Z.I.A. il dott. Norberto Petriccioli;

Considerato che lo stesso Amministratore Unico è RUP del presente procedimento;

Premesso che il 25 maggio 2018 è entrato in vigore il Regolamento Europeo Privacy UE/2016/679 c.d. GDPR (General Data Protection Regulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati;

Considerato che con il Regolamento Europeo Privacy UE/2016/679 viene recepito nel nostro ordinamento giuridico il "principio di accountability" (obbligo di rendicontazione) che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati:

- di dimostrare di avere adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento, prevedendo, altresì, l'obbligo del titolare o del responsabile del trattamento della tenuta di apposito registro delle attività di trattamento, compresa la descrizione circa l'efficacia delle misure di sicurezza adottate;
- che il registro di cui al punto precedente, da tenersi in forma scritta - o anche in formato elettronico - deve contenere una descrizione generale delle misure di sicurezza tecniche e

organizzative e che, su richiesta, il titolare del trattamento o il responsabile del trattamento sono tenuti a mettere il registro a disposizione dell'autorità di controllo;

Considerato, inoltre, che detto Regolamento ha rafforzato i poteri delle Autorità Garanti nazionali ed inasprito le sanzioni amministrative a carico di imprese e pubbliche amministrazioni prevedendo, in particolare, in caso di violazioni dei principi e disposizioni del Regolamento, che le sanzioni, per le Pubbliche Amministrazioni, possono arrivare fino a 20 milioni di euro (art. 83);

Visto il Decreto dell'Amministratore Unico del Consorzio Z.I.A. n. 77 del 30/09/2020, e successivo n. 79 del 05.10.2020 "*Rettifica errore materiale Decreto A.U. n. 77 del 30.09.2020*", con il quale è stato affidato l'incarico di Responsabile Protezione Dati (Data Protection Officer – D.P.O.) all'Avv. Alessandro Caleo;

Visto il Decreto dell'Amministratore Unico n. 93 del 05/11/2020, recante "*Affidamento diretto incarico per attività di assistenza e formazione ai fini dell'adeguamento dell'organizzazione del Consorzio Zona Industriale alla vigente disciplina in materia di tutela dei dati personali (Regolamento UE 2016/679; Dlgs 196/2003 come aggiornato dal Dlgs 101/2018). Smart CIG ZA82E8AF95*";

Considerato che le attività di cui al precedente Decreto n.93 del 05/11/2020 sono quasi giunte al termine attraverso incontri di formazione ed aggiornamento con il personale dell'Ente, nonché mediante la predisposizione di un modello organizzativo dell'Ente in tema di Privacy, composto da:

- Documento di Privacy Policy;
- Organigramma dell'Ente in tema di Privacy;

Documenti entrambi allegati in allegato A e B al presente Decreto e costituente parte integrante e sostanziale dello stesso;

Ritenuto, pertanto, necessario provvedere ad approvare, con specifico atto amministrativo, i documenti di cui sopra ed in particolare:

- Documento di Privacy Policy;
- Organigramma dell'Ente in tema di Privacy;

Documenti entrambi allegati in allegato A e B al presente Decreto e costituente parte integrante e sostanziale dello stesso;

Tutto quanto premesso, visto, considerato e ritenuto

Decreta

– **Di approvare** i documenti di cui alle premesse ed in particolare:

- Documento di Privacy Policy;
- Organigramma dell'Ente in tema di Privacy;

Documenti entrambi allegati in allegato A e B al presente Decreto e costituenti parte integrante e sostanziale dello stesso;

- **Di dare atto** che il presente atto è soggetto a pubblicità sulla rete internet ai sensi del D.Lgs. n. 33/2013 e che lo stesso sarà, pertanto, pubblicato sul sito istituzionale del Consorzio Z.I.A. all'indirizzo www.consorzio.zia.ms.it, nella sezione "Amministrazione trasparente"; e sull'Albo Pretorio dello stesso;

L'Amministratore Unico

(Dott. Norberto Petriccioli)

Documento firmato digitalmente

Documento firmato
PETRICCIOLI NORBI
15.03.2021 09:06:0

PRIVACY POLICY

AZIENDALE

PREMESSA E NOZIONI

Il presente documento illustra le regole di condotta alle quali deve attenersi il personale dipendente, nell'espletamento di ogni attività che implica il trattamento di dati personali.

Ai fini del presente codice di condotta, si tengano in considerazione le seguenti fondamentali nozioni e definizioni:

- ✓ diritto alla protezione dei dati personali: è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8). Oggi è tutelato, in particolare, dal Regolamento UE 679/2016 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), oltre che da vari altri atti normativi italiani e internazionali e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento UE 679/2016 tramite il D. L. 101/2018 ;
- ✓ 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;
- ✓ dati personali: le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica e simili;
- ✓ dati personali particolari: sono i dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale, i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- ✓ dati giudiziari: sono i dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.
- ✓ interessato: persona fisica alla quale si riferiscono i dati personali (quindi se un trattamento riguarda, ad esempio, l'indirizzo, il codice fiscale, ecc. di Mario Rossi, questa persona è l"interessato" (articolo 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

- ✓ titolare: è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);
- ✓ responsabile: è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati (articolo 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. "sub-responsabile" (articolo 28, paragrafo 2).
- ✓ incaricato o autorizzato: è il soggetto persona fisica che effettua il trattamento nel rispetto delle indicazioni e istruzioni impartite dal titolare.
- ✓ DPO o RPD Responsabile della protezione dei dati: è il soggetto nominato dal titolare del trattamento che, all'interno del Consorzio è tenuto a: a) sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità; b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA); c) informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati; d) cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento; e) supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento

1. REGOLE GENERALI (per il soggetto autorizzato al trattamento)

Preliminarmente, va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, il soggetto autorizzato al trattamento dati, deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- ✓ tutte le operazioni di *trattamento* devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- ✓ le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non

autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;

- ✓ in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc, password su screen saver) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- ✓ non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
- ✓ devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- ✓ deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Nei successivi paragrafi si riportano le norme che gli Incaricati devono adottare, sia che trattino dati in formato elettronico che cartaceo.

2. ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

La postazione di lavoro deve essere:

- ✓ utilizzata solo per scopi legati alla propria attività lavorativa;
- ✓ utilizzata in modo esclusivo (salvo che sia necessario condividerla con altri ovvero alternarsi nella postazione per esigenze legate alla attività);
- ✓ protetta, evitando che terzi possano accedere ai dati che si sta trattando.

L'incaricato/autorizzato è inoltre tenuto a:

- non utilizzare in Azienda risorse informatiche private (PC, periferiche, token, ecc..);
- non installare alcun software sui devices aziendali, salvo espressa autorizzazione o indicazione del Titolare del trattamento;
- non lasciare nella postazione di lavoro informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, ecc.);

- impostare lo screen saver con password in modo che dopo qualche minuto di inattività, si possa riaccedere solo con password
- non lasciare incustoditi cellulari e palmari;
- non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

3. GESTIONE DELLA PASSWORD

Ciascun autorizzato al trattamento che utilizza un terminale aziendale per espletare le proprie mansioni lavorative, per accedere allo stesso, si avvale di una password alfanumerica personalmente elaborata.

Ciascuno dei soggetti autorizzati è tenuto a mantenere segreta la password per l'accesso e a non rivelarla ad alcuno.

4. ANTIVIRUS

I Personal Computer (PC) in dotazione agli utenti, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.

5. PROTEZIONE DEI PC PORTATILI

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili, ciò ove vengano messi a disposizione del personale:

- ✓ conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;
- ✓ non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda;
- ✓ avvertire tempestivamente il titolare, che darà le opportune indicazioni, in caso di furto di un PC portatile;
- ✓ essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;
- ✓ operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti;

- ✓ verificare che la copia di back up quotidiana programmata in modo automatico all'orario stabilito con l'incaricato venga eseguita correttamente, avendo premura di avviarla manualmente se all'ora stabilita il pc non risultasse collegato alla rete aziendale.

6. USO DI INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno al Consorzio.

In particolare, l'utente dovrà osservare le seguenti regole:

- ✓ è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- ✓ non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
- ✓ non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa (e comunque solo subordinatamente alla autorizzazione del datore dei lavoro);
- ✓ non è consentito l'utilizzo funzioni di instant messaging, salvo dietro autorizzazione del titolare;
- ✓ è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un mittente non conosciuto);
- ✓ non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario;
- ✓ è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati personali particolari (tra questi i dati che attengono la salute delle persone), senza garantirne l'opportuna protezione;
- ✓ occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare;
- ✓ occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;
- ✓ è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dal Consorzio;

- ✓ è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna);
- ✓ al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema è necessario, seguendo le indicazioni impartite dall'esperto dei sistemi informatici, archiviare periodicamente i messaggi di posta elettronica e cancellare quelli inutili;
- ✓ va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), avvertendo immediatamente il titolare nel caso in cui siano rilevati virus.

L'utente, in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 5 giornate lavorative - deve attivare l'apposita funzionalità di sistema (cd. "fuori Sede") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.

Il Consorzio in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo del titolare, di accedere alla casella di posta elettronica dell'utente assente.

***

Nell'utilizzo della posta elettronica ciascun utente deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti del Consorzio. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.

La formulazione dei messaggi deve pertanto far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione del Consorzio.

Il Consorzio formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

- ✓ conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative da parte del cliente e/o fornitore;

- ✓ prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque non pertinente al contesto lavorativo.

In tali casi gli utenti devono in particolare:

- ✓ visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio;
- ✓ una volta aperto il messaggio, evitare di aprire gli allegati o cliccare sui "link" eventualmente presenti;
- ✓ cancellare il messaggio e svuotare il "cestino" della posta;
- ✓ segnalare l'accaduto al titolare del trattamento;
- ✓ evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione;
- ✓ in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, veicolati attraverso lo strumento di posta elettronica :
- ✓ adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio; in particolare l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa,
- ✓ utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di social engineering,
- ✓ in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa. Si raccomanda, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca.
- ✓ in caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia;
- ✓ evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

7. TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto richiesto.

Si invita a limitare l'utilizzo del fax sia per il ricezione dei documenti contenti dati personali (chiedendo al mittente di prediligere altri strumenti di invio), sia per l'invio di documenti. Nei casi in cui sia necessario l'utilizzo del fax, si raccomanda – in caso di ricezione – di ritirare il documento con tempestività; in caso di invio, di assicurarsi che il destinatario lo ritiri prontamente.

Nei casi in cui debbano essere inviati per posta elettronica o SMS, documenti contenenti dati personali, si raccomanda di:

- ✓ prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail del destinatario ed immessi siano corretti;
- ✓ nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file corretto;

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

8. ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

In caso di trattamento di dati particolari (condizione di salute, documenti che rilevino l'appartenenza ad associazioni sindacali, ecc.), tutta la documentazione cartacea deve essere

conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L'accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato per scritto nella lettera di incarico.

9. ACCESSO AI DATI DELL'UTENTE

Il Titolare può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware), fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.

10. CONTROLLI DA PARTE DEL TITOLARE DEL TRATTAMENTO

Il titolare del trattamento, può effettuare, in qualsiasi momento, controlli sugli strumenti informatici anche per preservare la sicurezza informatica dei dati personali in esse contenuti.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica, inclusi gli eventuali telefoni e tablet aziendali messi a disposizione dal titolare, nonché quanto con essa creato, è di proprietà del Consorzio, in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli del Consorzio stesso.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dal Consorzio nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti nonché delle regole inserite nella presente Privacy Policy.

11. USO PRIVATO DEI SOCIAL MEDIA

Il personale dipendente del Consorzio, attivo con propri profili privati all'interno di piattaforme di Social Media, nell'utilizzo degli stessi deve tenere presente che può essere identificato come un dipendente del Consorzio stesso; tanto premesso, il dipendente dovrà avere cura di mantenere un comportamento corretto e responsabile in ogni interazione.

Il personale dipendente, nell'utilizzo dei propri accounts privati sui Social Network dovrà attenersi alle seguenti regole di condotta:

- con riferimento a tematiche concernenti l'attività del Consorzio, considerare lo spazio virtuale del Social Network come uno spazio pubblico e non come uno spazio privato;
- il dipendente, nelle sue interazioni sui Social Networks che abbiano attinenza con l'attività del Consorzio, è tenuto a specificare che le opinioni espresse hanno carattere personale e non impegnano in alcun modo il Consorzio stesso;
- il personale dipendente è tenuto ad osservare un comportamento pubblico rispettoso dell'organizzazione aziendale, e, di conseguenza a non divulgare informazioni riservate delle quali è a conoscenza in ragione della propria mansione, informazioni relative a progetti o deliberazioni non ancora rese note;
- il dipendente è chiamato a rispettare la privacy dei colleghi, e pertanto deve evitare di rendere note informazioni concernenti l'attività di questi ultimi all'interno della realtà aziendale ed eventuali procedimenti disciplinari a carico degli stessi; è tenuto, inoltre, a non divulgare materiale audio e video senza l'esplicita autorizzazione dei soggetti coinvolti;
- fermo restando l'insopprimibile esercizio del diritto di critica e delle libertà sindacali, il dipendente deve astenersi dal pubblicare o condividere immagini, video, audio o scritti, dichiarazioni offensive o lesive della reputazione e dell'immagine aziendale.

La violazione di tali regole di condotta potrà determinare l'irrogazione di una sanzione disciplinare da parte del Consorzio nei confronti del dipendente, in base alla gravità della stessa, fermo restando che i fatti potranno essere considerati fonte di responsabilità civile, penale, ammnistrativa e contabile in base all'applicazione delle norme vigenti.

Il personale dipendente è autorizzato ad accedere ai propri account personali sui Social media, nel corso dell'orario lavorativo, esclusivamente durante le pause, o in alternativa, a fronte di espressa autorizzazione del Responsabile privacy aziendale.

Il personale dipendente è autorizzato a condividere sul proprio profilo privato i contenuti diffusi dai canali social del Consorzio, sempre ne rigoroso rispetto delle indicazioni che precedono.

*****

Massa, Marzo 2021

ORGANIGRAMMA PRIVACY