	REGOLAMENTI GENERALI DELL'AMMINISTRAZIONE REGOLAMENTO CONCERNENTE L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA DELL'ENTE[1], DELLA RETE INTERNET LA POSTA ELETTRONICA E L'ADOZIONE DI ADEGUATE PROCEDURE COMPORTAMENTALI	**RG. PERS.** Rev.: 0 Del: 29.06.2022

INDICE

CAPO I - I PRINCIPI

Art. 1

Introduzione, definizioni e finalità

Il presente disciplinare interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori ecc.), nonché l'adozione di adeguate procedure comportamentali, al fine di tutelare i beni dell'Ente ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Ente a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare l'Ente ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.
A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento UE n. 2016/679, alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provv. 1 marzo 2007).

Art. 2

Ambito di applicazione

Il presente disciplinare interno si applica ad ogni Utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza dell' Ente.
Per **Utente** si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.
Per **Ente** si intende, invece, l'Azienda Speciale Don Moschetta, con sede legale in Viale Michelangelo Buonarroti, 10 30021 Caorle, Venezia – Italia. che riveste altresì la qualifica di Titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art. 3

Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali rientranti nel patrimonio dell'Ente e sono da considerarsi di esclusiva proprietà dell'Ente.
Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti all'attività svolta per l'Ente), e comunque per l'esclusivo interesse aziendale.

A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Ente, sarà dallo stesso considerato come avente natura istituzionale e quindi riservata.

Art. 4

Responsabilità personale dell'utente

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ente, nonché dei relativi dati trattati per finalità aziendali.
A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ente, è tenuto a tutelare (per quanto di propria competenza) il patrimonio da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse dell'Ente.
Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo ed alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica aziendale, riportando al proprio responsabile senza ritardo eventuali rischi di cui è a conoscenza, ovvero violazioni del presente disciplinare interno.
Sono vietati comportamenti che possano creare un danno, anche di immagine, all' Ente.

Art. 5

I controlli

I principi

L'Ente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa dell'Utente.
Ciononostante, non si esclude che, per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tali casi, infatti, sarà onere dell'Ente sottoporre tali forme di controllo (contenute in specifico allegato) all'accordo con le rappresentanze sindacali aziendali ovvero, in assenza di queste, con la commissione interna. In difetto di accordo, su istanza dell'Ente, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.
L'Ente, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa, nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 c.c.), agirà in base al **principio della "gradualità"**. Secondo questo principio:

a. i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
b. nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso

anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;

c. in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati

In ogni caso l'Ente non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

d. la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
e. la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
f. la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
g. l'analisi dei dispositivi per l'accesso alla rete internet.

CAPO II - MISURE ORGANIZZATIVE

Art. 6

Amministratori del sistema

L'Ente conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche aziendali. È compito dell'amministratore di sistema:

a. gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ente;
b. gestire la creazione, l'attivazione, la disattivazione e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
c. monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
d. creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
e. rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
f. provvedere alla sicurezza informatica dei sistemi informativi dell'Ente, nel rispetto di quanto prescritto dal GDPR 2016/679 (artt. 32) e D.lgs. 65/2018 (sicurezza dei sistemi Informativi).
g. utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, o impedimento dello stesso.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che sia in possesso di requisiti dimostrabili di professionalità, esperienza, onorabilità, competenza e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Art. 7

Assegnazione degli account e gestione delle password

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e, di conseguenza, ne disciplina l'accesso alle risorse informatiche aziendali, per singola postazione lavorativa.
Gli account utenti vengono creati dagli amministratori di sistema e sono personali, ovvero associati univocamente alla persona assegnataria:

a. l'accesso al proprio account avviene tramite l'utilizzo delle ''credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza (Es: busta chiusa e sigillata);
b. le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati dei quali non è consentito comunicarne gli estremi a terzi (seppur soggetti in posizione apicale all'interno dell'Ente);
c. se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Referente Privacy del Titolare del Trattamento di riferimento;
d. ogni Utente è responsabile dell'utilizzo del proprio account Utente.

Si ricorda che in caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza ed operatività delle risorse informatiche dell'Ente, lo stesso si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di sistema.
Si ricorda, infine, che i beni e la strumentazione informatica oggetto del presente disciplinare interno rimangono di esclusivo dominio dell'Ente, il quale, in virtù dei rapporti instaurati con gli utenti, ne disciplina l'affidamento.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo almeno ogni 6 mesi (nel caso di trattamento di dati ex sensibili (categorie particolari di dati ex art. 9 GDPR 2016/679) e di dati giudiziari (ex art. 10 Gdpr 2016/679) la parola chiave è modificata almeno ogni 3 mesi.
L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

e. utilizzare almeno 11 caratteri alfanumerici, inclusi i caratteri speciali (#,%, ecc.);

f. la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#§f:$%...";
g. evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili (es. date di nascita, nominativi di parenti, di animali domestici, codici fiscali, hobby, altri dati comunque riconducibili al soggetto);
h. deve risultare completamente differente dalle ultime tre utilizzate e non assomigliare loro anche solo in parte;
i. evitare l'utilizzo di password comuni e/o prevedibili;
j. proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che scrivere la password su post-it o altri supporti non è conforme alla normativa e costituisce violazione del presente disciplinare interno.

Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente.

Art. 8

Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro device concesso in uso all'Utente da parte dell'Ente. L'assegnatario di tali beni e strumenti informatici aziendali, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.
Al fine di disciplinare un corretto utilizzo di tali beni, l'Ente ha adottato le regole tecniche, che di seguito si riportano:

a. ogni PC, notebook (accessori e periferiche incluse), e altro device, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ente, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e, comunque, per finalità strettamente attinenti all'attività svolta;
b. è dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente.
c. il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa richiesta scritta dell'utente indirizzata al proprio Responsabile privacy di riferimento che ne valuterà i requisiti tecnici e l'aderenza alle policy interne ed al ruolo ricoperto in azienda;
d. le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
e. quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password, o effettuare il log-out dalla sessione;

f. l'Utente deve segnalare con la massima tempestività all'amministratore del sistema, ovvero al proprio Responsabile di riferimento, eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
g. va' fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;
h. l'Ente si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata;
i. gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer o alle reti informatiche aziendali, salvo preventiva autorizzazione scritta dell'Ente.

CAPO III - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9

Personal computer e computer portatili

Gli utenti utilizzano per l'espletamento delle proprie mansioni dispositivi di proprietà dell'Ente; ne consegue che gli stessi sono tenuti al rispetto delle seguenti regole:

a. non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione dell'Ente che la esegue per mezzo dell'amministratore del sistema;
b. non è consentito rimuovere, danneggiare o asportare componenti hardware;
c. non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Ente;
d. è onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus, nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
e. è onere dell'Utente spegnere il proprio PC o computer portatile al termine del lavoro. Per quanto concerne la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali file elaborati prima della sua riconsegna.

Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

Art. 10 Software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'Ente per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").
L'Ente richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software in azienda:

a. l'Ente acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza;
b. non è consentito fare il download e l'upload tramite internet di software non autorizzato;
c. l'Ente, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;
d. l'Ente non tollererà la duplicazione illegale del software.

Art. 11

Dispositivi mobili di connessione (internet key)

Agli assegnatari di computer portatili può essere fornita in dotazione una chiavetta per la connessione alla rete aziendale volta a facilitare lo svolgimento delle mansioni lavorative anche da remoto.
I suddetti dispositivi devono essere utilizzati esclusivamente sui computer forniti in dotazione dall'Ente e non è consentito concederne l'utilizzo a soggetti terzi, né utilizzarli su computer privati.
Specifiche relative ai limiti entro cui l'Utente potrà utilizzare il servizio offerto tramite la chiavetta, sono riportate nella scheda tecnica consegnata all'Utente unitamente al dispositivo di cui sopra.
L'Utente dovrà attenersi ai suddetti limiti potendo l'Ente, in caso contrario, richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

Art. 12

Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, dischi rigidi esterni, ecc.
L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

a. non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'Ente (cfr. art. 23);
b. è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto. La custodia dei dati e dei documenti, nei modi detti, si uniforma a criteri di omogeneità rifuggendo

ogni promiscuità. (ad es. documenti contenenti dati sensibili non possono essere custoditi unitamente ad altri contenenti dati amministrativi o contabili);

c. si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'Ente, i dispositivi saranno soggetti (ove compatibili) al presente disciplinare interno.

Art. 13

Stampanti, fotocopiatrici e fax

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Ente.
È richiesta una particolare attenzione quando si inviano su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.
L'utilizzo dei fax (se ancora in uso) per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e chiedere la conferma telefonica di avvenuta ricezione.
Di tali strumenti è necessario gestire la coda di stampa, nel caso predisponendo psw personalizzate da digitare una volta raggiunta la stampante, per evitare di lasciare documenti in attesa.

Art. 14

Strumenti di fonia mobile e/o di connettività in mobilità

L'azienda può mettere a disposizione, in relazione al ruolo o alla funzione del singolo Utente, impianti di telefonia fissa e mobile, nonché dispositivi - quali Smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonia tramite rete cellulare.
Specifiche relative ai limiti entro cui l'Utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata all'Utente unitamente ai dispositivi di cui sopra.
L'Utente dovrà attenersi ai suddetti limiti potendo l'Ente, in caso contrario, richiedere il rimborso dei costi sostenuti per il superamento degli stessi.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale che è dato in uso per scopi esclusivamente lavorativi. È tuttavia concesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la c.d. "diligenza del buon padre di famiglia" e, comunque, tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro (Ente).
A tal fine si informano gli utilizzatori dei servizi di fonia aziendale, che l'Ente eserciterà i diritti di cui all'art. 124 d.lgs. 196/2003 (c.d. fatturazione dettagliata), richiedendo ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo.
I controlli saranno eseguiti secondo le modalità descritte all'art. 5 del presente disciplinare interno.
L'Ente si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate

dalla SIM in incarico all'Utente per il periodo interessato. L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano:

a. ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso e, conseguentemente, anche della sua diligente conservazione;
b. i dispositivi devono essere dotati di password di sicurezza (c.d. codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine si precisa che:
   - il CODICE PIN dovrà essere composto di n. 5 cifre numeriche;
   - il CODICE PIN dovrà essere modificato dall'assegnatario con cadenza al massimo semestrale;
   - ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'Ente;
c. in caso di furto, danneggiamento o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà darne immediato avviso all'Ente e, qualora necessario, produrre denuncia presso l'autorità di Pubblica Sicurezza; ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
d. in caso di furto o smarrimento l'Ente si riserva la facoltà di attuare la procedura di remotewipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili;
e. non è consentito all'Utente caricare o inserire all'interno del dispositivo o qualsiasi dato personale non attinente all'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione;
f. non è consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi;
g. l'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli Smatphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'Utente le spese che l'Ente dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata;
h. salvo diversi specifici accordi, al momento della consegna del tablet o Smatphone l'Utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli Smatphone e tablet, consapevole che, in caso contrario, l'Ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

CAPO IV - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 15

Gestione e utilizzo della rete internet

Ogni Utente potrà essere abilitato dall'ente alla navigazione Internet. Col presente disciplinare interno si richiamano gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'Ente stesso.

REGOLAMENTO CONCERNENTE L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA DELL'ENTE[1], DELLA RETE INTERNET LA POSTA ELETTRONICA E L'ADOZIONE DI ADEGUATE PROCEDURE COMPORTAMENTALI

Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

a. l'utilizzo è consentito esclusivamente per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
b. è richiesta la costante verifica della correttezza dell'indirizzo web cui si intende accedere, specie se tale accesso viene sollecitato o stimolato da mail, comunicazioni telefoniche, o altro;
c. non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'Ente;
d. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
e. non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nickname);
f. non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
g. è consentito l'utilizzo di soluzioni di Instant Messanger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'Ente;
h. non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
i. non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright;
j. non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente;
k. analogamente, non è consentito pubblicare immagini o notizie riferibili all'Ente e a suoi dipendenti che possano ledere diritti o agevolare l'azione intrusiva di ingegneri sociali.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere nocivo all'immagine dell'Ente.

Per facilitare il rispetto delle predette regole, l'Ente si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

Art. 16

Ransomware

È un programma informatico dannoso che infetta, attraverso cryptor o blocker, un dispositivo (PC, notebook, tablet, smartphone, smart TV) e ne blocca l'accesso ai contenuti (foto, video, file) per fini delittuosi.

L'Utente deve considerare costantemente tale pericolo e:

a. al verificarsi del sintomo di tale problematica, interrompere tempestivamente l'alimentazione al dispositivo, ove possibile rimuovendo l'alimentazione dalla rete;
b. prestare massima cautela verso messaggi pervenuti via email, sms, o altro, da soggetti che possono sembrare conosciuti e sicuri come corrieri espressi, gestori di servizi (acqua, luce e gas), operatori telefonici, soggetti istituzionali, ecc.;
c. in tali ultimi casi, non aprire allegati, o cliccare su link o banner che potrebbero essere collegati a software dannosi;
d. non aprire messaggi provenienti da soggetti sconosciuti o estranei a rapporti aziendali, nè cliccare su collegamenti a link o siti sospetti;
e. provvedere, preliminarmente all'avvio della sessione di lavoro quotidiana, all'aggiornamento antivirus e del sistema operativo;
f. provvedere, al termine della sessione di lavoro e ove non sia già automaticamente previsto, al back up dei dati custoditi;
g. non assecondare in alcun modo astenendosi da attività o comunicazioni nell'alveo di richieste estorsive collegate all'insorgenza di ransomware;
h. rappresentare al proprio referente privacy di riferimento ogni elemento informativo utile per la denuncia dell'evento criminoso alla Polizia Postale.

Art. 17

Gestione e utilizzo della posta elettronica aziendale

Principi guida

Ad ogni Utente titolare di un account l'Ente provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale. Si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà dell'Ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate

esclusivamente per la ricezione dei messaggi, mentre per le risposte o gli invii, si deve sempre utilizzare la casella di posta individuale assegnata.
L'Ente valuterà caso per caso e previa richiesta dell'Utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato.
Attraverso l'e-mail aziendale gli utenti rappresentano pubblicamente la società e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine aziendale.
Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale e sono tenuti ad utilizzarle in modo conforme alle presenti regole. Gli stessi, pertanto, devono:

a. conservare la password nella massima riservatezza e con la massima diligenza;
b. mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
c. utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario (ove possibile a seconda dei sistemi);
d. prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura, nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto potrebbero essere utilizzati come veicolo per introdurre programmi dannosi (es. virus);
e. inviare preferibilmente file in formato PDF;
f. accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;
g. rispondere ad e-mail pervenute solo da emittenti conosciuti, verificandone l'esatta coincidenza dell'indirizzo[1], e cancellare preventivamente le altre soprattutto se: trattano questioni non di interesse aziendale, violazioni di sicurezza, pubblicità di vario genere, riguardano mittenti che avrebbero dovuto utilizzare PEC, tendono ad alimentare catene di Sant'Antonio invitando a reindirizzare messaggi ricevuti, provengono da banche, assicurazioni, riguardano codici di accesso, avvisi relativi ad errori di inoltro di mail, soluzioni antivirus gratuite;
h. tenere in debito conto che mail insidiose potrebbero pervenire anche da indirizzi conosciuti già vittima di intrusione informatica. Pertanto, è necessario interrompere immediatamente ogni attività e cestinare mail che non si attendono, non risultano opportune, presentano errori di ortografia, anomalie di ogni genere, comprese eventuali richieste o proposte come cliccare dei link, inserire credenziali e password personali, o scaricare dei software. Tali probabili attività fraudolente, confezionate con stimoli motivazionali idonei a elicitare risposte immediate (autorità del mittente, situazioni di pericolo, ecc.), si presentano generalmente sotto forma di contenuti allarmistici all'interno di false pagine: di consulenti, fornitori, clienti, Poste Italiane, Agenzia Dell'Entrate, INPS, Guardia di Finanza, indagini istat, altri siti istituzionali, ebay, paypal, ecc.. In tali casi è probabile l'intento di sottrarre notizie riservate o installare malware;
i. astenersi dal variare la regola della casella di posta che impedisce l'apertura automatica degli allegati, compreso quelli in formato Html;
j. in nessun caso, per i documenti in formato word, abilitare le macro che costituiscono un potenziale veicolo di infiltrazione di virus;

[1] Specie: commercialista, consulente del lavoro, fornitori in genere, e similari

k. collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

Non è consentito agli utenti, al contrario:

l. diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet;
m. utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (quali ad es. presentazioni o materiali video aziendali).

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".

Occorre, inoltre, che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente. Le presenti disposizioni, ove compatibili, si applicano all'utilizzo di posta elettronica certificata dell'Ente.

Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun Utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi web mail), l'Ente, perdurando l'assenza oltre un determinato limite temporale pari a 3 giorni, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento (risposta automatica o re indirizzamento), avvertendo l'assente.

Nel caso, invece, l'Ente necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

n. la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato (per iscritto) dall'Utente assente;
o. di tale attività sarà redatto apposito verbale e informato l'Utente interessato alla prima occasione utile.

Cessazione dell'indirizzo di posta elettronica aziendale

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; entro 3 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

CAPO V – CLEAN POLICY DESK

Premessa

Tale procedura integra modalità comportamentali vincolanti per l'Utente anche nel caso di prestazione lavorativa espletata al di fuori dell'ambito aziendale.

Art. 18

Gestione della postazione di lavoro

La clean policy desk costituisce procedura obbligatoria per l'Utente da attuarsi scrupolosamente al variare di ogni incombenza d'ufficio e si conclude con l'assoluta pulizia della scrivania al termine della giornata lavorativa. Sulla scrivania trovano posto solo gli oggetti e i documenti necessari ad assolvere il compito in via di risoluzione. Ogni documento non più necessario viene riposto nel luogo prescritto salvaguardando le relative procedure di sicurezza (ad es. armadio chiuso a chiave).

I supporti cartacei o di altra natura contenenti dati – come CD-ROM, DVD, chiavette USB, hard disk, o altri già indicati - non più utili o utilizzabili vanno immediatamente distrutti o custoditi a tal fine. La distruzione di tali materiali, ove necessario e in accordo con le politiche aziendali, va documentata al fine di poterla dimostrare successivamente.

È vietato abbandonare documenti in sale riunioni o in altri luoghi estranei alla propria postazione di lavoro; l'utilizzo di lavagne, o altri supporti analoghi, impone la rimozione di ogni traccia al termine dell'attività. Eventuali bacheche presenti in ambito lavorativo vanno gestite adeguatamente al fine di prevenire inopportuna pubblicità di dati conseguente alla pubblicazione di avvisi.

Inoltre:

a. i contenitori di documenti trasparenti devono trovare allocazione permanente all'interno di altri contenitori oscurati;
b. non è consentito introdurre nell'ambiente lavorativo documenti personali o comunque estranei ai compiti aziendali;
c. l'utilizzo dei post-it viene disciplinato attraverso il divieto di annotazione di dati riservati di qualsiasi natura;
d. è tassativamente vietato annotare password, oltre che su post it, su supporti cartacei o file non adeguatamente protetti;
e. la corrispondenza, comprese le relative buste, viene gestita alla stregua dei rimanenti documenti aziendali;
f. le fotografie ritraenti dipendenti, clienti, fornitori, locali aziendali, o altre informazioni riconducibili al contesto lavorativo, vanno gestite con cautela rispettando gli altrui diritti;
g. è vietato esporre in azienda immagini di minori;

h. è vietata l'introduzione negli stessi locali di I.O.T. (smart toys e similari), salvo preventiva autorizzazione scritta;
i. l'allontanamento dell'Utente dal raggio di sorveglianza della propria postazione lavorativa è preceduto dall'attuazione della clean policy desk estesa al monitor del proprio computer, da proteggere con l'attivazione dello screen saver, nonché dalla rimozione e custodia di memorie esterne. I notebook, I Pad e altri device vengono riposti in luoghi sicuri quali cassetti chiusi a chiave o armadi. Nessun dato da proteggere può essere lasciato incustodito in tale frangente;
j. è vietato memorizzare sullo schermo del PC link a file o directory;
k. calendari da tavolo e da parete non devono rivelare dati da proteggere;
l. viene comunque previsto il blocco temporizzato dello schermo del PC a mezzo password in caso di inattività;
m. la dislocazione e organizzazione delle postazioni di lavoro risponde alle caratteristiche fisiche dei locali, alla loro insonorizzazione, alla presenza di finestre o specchi idonei a consentire o agevolare captazioni di dati. Pertanto, non è consentito all'Utente modificare tale condizione;
n. l'Utente è tenuto a disattivare ogni eventuale comando o messaggio vocale, adeguando il volume dei telefoni e delle comunicazioni verbali affinché non risultino percettibili ad astanti non autorizzati;
o. in presenza di estranei o di altro personale non autorizzato, i documenti vanno riposti sulla scrivania in modo da non consentirne la lettura e, a fattor comune, con la parte leggibile orientata verso il basso;
p. la corretta attuazione della clean policy desk va salvaguardata anche in caso di abbandono repentino della postazione lavorativa per prove di evacuazione, o eventi sopravvenuti di qualsiasi natura. Ciò al fine di prevenire eventi cagionati surrettiziamente con l'intento di carpire dati.

CAPO VI – GESTIONE DEI RIFIUTI CARTACEI O DI ALTRA NATURA CONTENENTI DATI

Art. 19

Gestione dei rifiuti contenenti dati

I rifiuti cartacei prodotti in ambito lavorativo vanno smaltiti esclusivamente in contenitori dislocati all'interno del perimetro aziendale ove vengono prelevati da addetti incaricati. Tali materiali devono essere considerati dall'Utente alla stregua di fonte informativa utile per attività intrusive. Ogni supporto cartaceo o di altra natura tipo CD-ROM, DVD, hard disk, chiavette USB, ecc., utilizzato per scopi aziendali e divenuto non più necessario, deve essere smaltito alla stregua di materiale riservato. Pertanto, la sua custodia e le modalità di distruzione sono soggette a particolari cautele da parte dell'Utente:

a. per la distruzione della carta è obbligatorio l'utilizzo degli appositi macchinari ad elevata efficienza distruttiva o, in accordo con politiche aziendali, può essere disposta la custodia per il successivo affidamento a ditte specializzate;

b. è vietato introdurre documenti contenenti dati riferiti all'ambito lavorativo[2] all'interno di cestini della carta ancora integri, parzialmente leggibili, o personalmente valutati illeggibili. Il principio è tassativo e prescinde da valutazioni individuali di opportunità in ordine alla sensibilità dei dati;
c. la distruzione dei documenti non più necessari deve avvenire tempestivamente e riguardare ogni supporto cartaceo anche se apparentemente divenuto illeggibile, ad esempio perché sporco di inchiostro o sovrascritto;
d. la carta, benché resa illeggibile dalla triturazione, non deve essere asportata dagli appositi cestini per essere smaltita in contenitori posizionati al di fuori dell'azienda;
e. fogli di carta contenenti dati non vengono mai riciclati per il successivo utilizzo della facciata o parti non scritte;
f. le buste e gli involucri della corrispondenza vengono trattati alla stregua di documenti;
g. documenti e materiale informatico danneggiato a seguito di allagamento vengono custoditi nelle more del successivo corretto smaltimento;
h. appunti, documenti e altri supporti cartacei contenenti dati aziendali prodotti all'esterno dell'azienda, sono assoggettati alle medesime procedure di quelli interni con il preciso divieto di smaltirli in modo difforme.

CAPO VIII - MODALITA' COMPORTAMENTALI NELL'EMERGENZA O IN CONTESTI DUBBI

Art. 20

Modalità comportamentali

Si tratta di misure che fondano sulle conoscenze fornite agli Utenti in occasione di formazione. Di seguito si elencano, in modo non esaustivo, linee guida vincolanti che potrebbero essere variate e/o implementate da ulteriori misure eventualmente necessitate da casi concreti, evoluzione tecnologica, o altro.
In generale gli Utenti:

a. si riferiscono costantemente alle conoscenze apprese in materia di tendenze psicologiche e attività intrusive, per strutturare adeguate modalità operative rispetto a problematiche insorgenti;
b. osservano scrupolosamente rigide regole di autenticazione degli interlocutori;
c. adottano una corretta e razionale procedura di verifica della situazione concreta ritenuta sospetta per il sintomo di aggressioni intrusive;
d. in tale caso, focalizzano la propria attenzione sull'opportunità del comportamento che intenderebbero istintivamente adottare, valutandone uno alternativo;
e. pongono attenzione ad ogni traccia o elemento che possa ingenerare il dubbio che possa essersi verificata l'effrazione di porte, armadi o cassetti, rappresentandola tempestivamente al proprio referente privacy;
f. rappresentano tempestivamente a quest'ultimo sospetti in ordine a possibili tentativi di manipolazione o intrusione riferibili al proprio compito aziendale, anche se verificatisi in ambito privato;

[2] Prodotti in tale ambito o provenienti dall'esterno.

g. in caso di emergenza, adottano nell'immediatezza contromisure idonee, concertate con il proprio referente privacy, per preservare l'accesso illecito ai dati o, comunque, infrenare e non agevolare l'azione dell'intrusore;
h. accertano, di concerto con il responsabile ICT, la perfetta funzionalità del proprio PC e mobile device, nonché l'assenza di virus, malware, key logger, keyghost, o altro. Quindi modificano credenziali e password in uso;
i. collaborano all'attenta disamina dell'azione subita e contribuiscono, fin da subito e in occasione di successivi briefing/audit, ad orientare l'introduzione di misure necessarie per azzerare o contenere le eventuali acquisizioni informative illecite di terzi e adottare misure in ambiti che, sebbene estranei all'attacco, possano aver evidenziato o lascino presagire criticità.

Art. 21

Sanzioni

L'eventuale violazione di quanto previsto dal presente disciplinare interno - rilevante anche ai sensi degli artt. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.
L'Ente avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti nel caso venga commesso un reato, o ne sia ritenuta probabile o solo sospettata la commissione, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.
Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, l'Ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

Art. 22

Informativa agli utenti ex art. 13 Regolamento UE n. 2016/679

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici dell'Ente, e relativamente ai trattamenti di dati personali svolti dall'Ente e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento UE n. 2016/679.

Art. 23

Comunicazioni

Il presente disciplinare interno è messo a disposizione degli Utenti per la consultazione, al momento dell'assegnazione di un account Utente, sulla intranet comunale (qualora implementata); ovvero è pubblicata presso la bacheca aziendale la versione più aggiornata dello stesso, allo scopo di facilitarne la conoscibilità a tutti gli interessati.

Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulle bacheche aziendali e tramite l'invio di apposito messaggio e-mail. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare.
Le autorizzazioni e/o concessioni richieste dal presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate all'Ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es.: e-mail).

Art. 24

Approvazione del disciplinare

Il presente Regolamento è stato approvato con deliberazione del Consiglio di Amministrazione n. 18 del 29.06.2022.