REGOLAMENTO DI UTILIZZO DEGLI STRUMENTI INFORMATICI

REVISIONI	DATA	OGGETTO DELLA REVISIONE
1	10.06.2024	Autenticazione ai dispositivi informatici

ORDINE DEGLI INGEGNERI DELLA CITTÀ METROPOLITANA DI VENEZIA
Via Bruno Maderna, 7 Int. 29 - 30174 Venezia Mestre - Tel. 0415289114 – Fax 0415228902
e-mail: info@ordineingegneri.ve.it – pec: ordine.venezia@ingpec.eu
sito web: www.ordineingegneri.ve.it

1. Scopo del documento

Il presente documento definisce le modalità di comportamento per l'utilizzo delle risorse informatiche messe a disposizione del personale dell'Ordine degliIngegneri della città metropolitana di Venezia (d'ora in poi "Ordine").

2. Normativa di riferimento

L'utilizzo degli strumenti informatici all'interno dell'Ordine avviene nel rispetto della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghidi lavoro e norme sul collocamento"; in particolare l'art. 4, comma 1, della Legge 300/1970, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali. In particolarenel rispetto dell'articolo 23 del D.lgs. n. 151/2015 (c.d. Jobs Act) che modificae rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agliimpianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzatidal lavoratore per rendere la prestazione lavorativa»

L'Ordine regolamenta l'utilizzo degli strumenti informatici nel rispetto del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR); in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679.

Infine si recepiscono le "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

3. Misure generali da Regolamento Europeo 679/2016

La persona autorizzata al trattamento dei dati nello svolgimento delle proprie mansioni è tenuta a:

- essere istruita periodicamente sul trattamento dei dati personali nel rispetto del Regolamento Europeo n. 679/2016 (GDPR);

- accertare che l'informativa privacy, pertinente allo specifico trattamento effettuato, completa in tutte le sue parti, sia stata fornita agli interessati, ai sensi dell'art. 13 del GDPR;

- verificare che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di legge e regolamento, adempimento di un contratto, soddisfacimento della richiesta dell'interessato;

- collaborare, con le altre persone autorizzate al medesimo trattamento, esclusivamente per i fini dello stesso e nel rispetto delle indicazioni fornite;

- non trasmettere, a soggetti terzi, informazioni circa dati personali trattati. La comunicazione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati, previa autorizzazione del Titolare del trattamento o suo delegato;

- non creare nuove ed autonome banche dati senza il permesso del Titolare del trattamento;

- non trasmettere dati in qualsiasi forma all'esterno qualora non vi siano espressamente destinati e ciò, eventualmente, solo previa autorizzazione dal Titolare del trattamento;

- accertarsi dell'identità del diretto interessato, prima di fornire informazioni circa i dati personali o il trattamento effettuato;

- non fornire dati o informazioni per telefono o per e-mail, qualora non si abbia certezza assoluta sull'identità del destinatario e che tale destinatario sia autorizzato;

- riporre in un luogo ad accesso controllato, al termine del periodo di trattamento, i supporti o i documenti cartacei, ancorché non definitivi, contenenti i dati personali;

- conservare i dati trattati secondo quanto indicato (tempo/criterio) nel registro dei trattamenti e comunque per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati;

- segnalare qualsiasi anomalia e stranezza al Titolare del trattamento/ Referente Privacy/RPD;

- rispettare eventuali ulteriori istruzioni, oltre a quelle del presente documento,impartite dal Titolare, nonché le ulteriori istruzioni e direttive impartite da un delegato del Titolare del trattamento/Referente Privacy/RDP;

- accertare che la cancellazione dei dati contenuti nelle banche dati elettroniche avvenga secondo i tempi/criteri contenuti nel "Registro dei

Trattamenti" e previa autorizzazione del Titolare del trattamento o secondo leprocedure definite. Potrà essere richiesta la verbalizzazione di tale atto. Nel caso di difficoltà nel compiere tali azioni dovrà essere richiesta la collaborazione dell'Amministratore di Sistema;

- furto, il danneggiamento o la perdita, anche accidentale dei dati o l'accesso abusivo agli strumenti a disposizione contenenti dati aziendali deve essere comunicato immediatamente all'Ordine in modo che possa attivare le procedure di Data Breach.

4. Misure di sicurezza

Tutti gli strumenti informatici affidati al personale dell'Ordine, compreso il PC, sono strumenti di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ne consegue che tali strumenti informatici possono essere utilizzati **esclusivamente** per rendere la prestazione lavorativa e vanno rispettati i seguenti comportamenti:

- **non è consentito installare autonomamente programmi provenienti dall'esterno,** salvo previa autorizzazione esplicita dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare virus e di creare rischiseri per la sicurezza informatica;

- **non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Amministratore di Sistema**. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema perincompatibilità 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;

- **non è consentito all'utente modificare le caratteristiche impostate sul proprio PC,** salvo previa autorizzazione esplicita dell'Amministratore di Sistema. Il personal computer, inoltre, deve essere spento ogni sera prima dilasciare gli uffici o in caso di assenze prolungate dall'ufficio;

- **non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro** (come ad esempio chiavette USB, masterizzatori, modem, ecc…), se non con l'autorizzazione espressa dell'Amministratore di Sistema;

- **l'accesso agli strumenti informatici è protetto da password**; per l'accesso devono essere utilizzati username e password assegnate

dall'Amministratore di Sistema. A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza;

- nel caso in cui sia necessario **dismettere uno strumento elettronico** dato in utilizzo da parte dell'Ordine (pc, tablet, portatile, smartphone, ecc..) si dovrà provvedere alla cancellazione di tutti i dati ivi presenti ed alla distruzione fisica dello strumento e prima di consegnare il prodotto al centro di smaltimento.

- nel caso vengano messi a disposizione del personale **dispositivi mobili**, il dispositivo dovrà essere utilizzato solo per l'attività lavorativa, protetto da password/PIN e protetto da furto o smarrimento,

- non è consentito l'utilizzo di **dispositivi informatici personali** (smartphone, tablet o laptop) per svolgere l'attività lavorativa, al fine di proteggere i dati dell'Ordine

I **log relativi all'utilizzo di strumenti informatici**, reperibili nella memoria degli strumenti stessi ovvero sui server o sui router, nonché i file con essi trattati **sono registrati e possono essere oggetto di controllo** da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

5. Utilizzo della posta elettronica

L'Ordine non ha assegnato al suo personale caselle di posta elettronica nominative, ma dispone di un unico indirizzo e-mail consultabile da tutto il personale e dal Consiglio dell'Ordine.

La casella di posta è uno strumento di lavoro. Le persone che accedono alla casella di posta elettronica sono responsabili del corretto utilizzo della stessa. L'utilizzo dell'e-mail deve essere limitato esclusivamente per scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. È buona norma evitare messaggi completamente estranei al rapporto di lavoro. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Nei messaggi inviati tramite posta elettronica aziendale verrà accluso il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza delmittente secondo le modalità previste dal regolamento adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne*

informazione all'indirizzo mittente".

È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.

L'iscrizione a mailing-list o newsletter esterne con l'indirizzo dell'Ordine deve essere autorizzata.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari è obbligatorio che questi allegati vengano preventivamente resi illeggibili attraverso la crittografia con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o dati particolari di competenza possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.

Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato del personale (attivando per esempio un "inoltro" automatico delle e-mail entranti),anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.).

Ai sensi del Codice civile e della normativa in materia fiscale, l'azienda è tenuta **a conservare per dieci anni sui propri server di posta elettronica tutti i messaggi e-mail a contenuto e rilevanza giuridica e commerciale** provenienti da e diretti a domini della stessa.

6. Autenticazione ai dispositivi informatici

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato;

- realizzazione e gestione di un sistema di autorizzazione che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere ed i trattamenti che si possono effettuare a quelli strettamente necessari

per lo svolgimento delle proprie mansioni lavorative.

Per realizzare le credenziali di autenticazione si associa un codice per l'identificazione dell'autorizzato al trattamento (username), attribuito dall'Amministratore di Sistema, ad una parola chiave riservata (password), conosciuta solamente dall'autorizzato che ha l'obbligo di elaborarla in modo appropriato, mantenerla riservata senza comunicarla ad altri con ogni modalitàe modificarla trimestralmente.

Le password devono essere composte da almeno otto caratteri ricordando che più la password è lunga più è difficile decifrarla. Nell'elaborazione delle password è bene utilizzare caratteri alfanumerici e speciali (simboli graficidella tastiera come % - $ - / - ecc.) e non utilizzare riferimenti agevolmente riconducibili all'interessato.

Il personale ha l'obbligo di non lasciare incustodito e accessibile lo strumento informatico, durante una sessione di trattamento, neppure in ipotesi di breve assenza.

Nei casi di prolungata assenza o impedimento dell'utente autorizzato al trattamento, unico abilitato ad accedere a determinati dati, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e/o di sicurezza del sistema, potrebbe rendersi necessario disporre dellapassword dell'autorizzato al trattamento, per accedere agli strumenti e ai dati. A tale fine ogni dipendente ha scritto la propria password in un foglio, ogni foglio è stato inserito in una busta chiusa, datata e vidimata sul punto di apertura. Tutte le buste vengono conservate sottochiave. In caso di necessità il Responsabile dell'Ufficio o soggetto da lui delegato potrà aprire la busta con la password del dipendente dal computer del quale si ha necessità di fare accesso agli strumenti aziendali. Avvisato il dipendente quest'ultimo provvederà a sostituire la password che verrà inserita nuovamente in busta chiusa secondo la procedura precedentemente illustrata.

In caso di estrema e giustificata urgenza l'Amministratore di Sistema potrà forzare un cambio password sulle credenziali del dipendente indisponibile, creare una nuova password, accedere con questa agli strumenti aziendali necessari.

7. Prevenzione degli attacchi informatici

Le postazioni di lavoro sono dotate di software antivirus.

Allo scopo di ridurre i rischi, non è consentito:
- disattivare il sistema antivirus presente sulla postazione di lavoro;

- l'uso di prodotti antivirus differenti da quelli forniti;
- qualora ci si trovi in presenza di comportamenti anomali nella propria postazione deve essere effettuata tempestiva comunicazione al personale tecnico;
- particolare attenzione si deve riporre nella apertura di documenti allegati alle e-mail nei seguenti casi:

1 il mittente è sconosciuto;

2 il mittente è conosciuto, ma utilizza un dominio di posta elettronica non usuale;

3 il contenuto della e-mail appare verosimile ma presenta errori ortografici evidenti, oppure contengono informazioni allarmanti o riferimenti generici al destinatario (es. Gentile cliente);

4 l'argomento della e-mail non è consono alla attività lavorativa;

Inoltre:

- non utilizzare i link presenti nei messaggi di posta indesiderata: potrebbero portare all'installazione di virus malevoli;
- non rispondere mai a messaggi che richiedono informazioni finanziarie, esempio password o dettagli dei conti correnti bancari o che comprendono link per effettuare operazioni bancarie/finanziarie. Le banche e le società di e-commerce di solito non spediscono messaggi di questo tipo;
- non rispondere a messaggi di spam per non confermare l'indirizzo e-mail dell'Ordine che potrebbe diventare oggetto di truffe