

PROPOSTA DI DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE N. 13 DEL 26/11/2024

Deliberazione n. 152 del 26/11/2024

OGGETTO: REGOLAMENTO PER L'USO AZIENDALE DELLE APPARECCHIATURE INFORMATICHE E LA SICUREZZA DI DATI.

ALLEGATI:

- All. 1) bozza regolamento per l'uso aziendale delle apparecchiature informatiche e la sicurezza di dati;
all. 2) mail del 16 novembre 2024 del DPO (prot. az. n. 18418)

Il Direttore Generale, di concerto con il Direttore Amministrativo f.f., con il capo unità organizzativa AA.GG. e con il capo unità organizzativa informatica, riferisce quanto segue:

PREMESSO:

- che si è reso necessario adottare il Regolamento aziendale per l'uso aziendale delle apparecchiature informatiche e la sicurezza dei dati;
- che il presente documento si inquadra nei principi contenuti nell'art.32 del GDPR recante "Sicurezza del Trattamento", ai sensi e per effetto del quale, il trattamento dei dati personali in Azienda deve essere assistito da adeguate misure di sicurezza al fine di attuare efficacemente i principi di protezione dei dati, secondo l'art. 5 del GDPR;
- che detto Regolamento è stato condiviso con l'unità organizzativa affari generali, la ripartizione informatica ed il DPO pro-tempore;

Visti:

- la Legge 20 maggio 1970, n. 300 recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (c.d. Statuto dei Lavoratori);
- il D.Lgs. 30 giugno 2003 n. 196 "codice in materia di protezione dei dati personali" come modificato e integrato dal D. Lgs. n. 101/2018;
- il Provvedimento del Garante per la Protezione dei dati personali "Linee guida per posta elettronica e Internet" del 1° marzo 2007, con particolare riferimento alla tematica trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori;
- la Direttiva 2/2009 della Presidenza del consiglio dei Ministri – Dipartimento della Funzione Pubblica relativa all'utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro che fornisce indicazioni relative al corretto utilizzo degli strumenti ICT da parte dei dipendenti e al proporzionato esercizio del potere datoriale di controllo da parte delle Amministrazioni pubbliche di cui all'art. 1, comma 2, del d.lgs n. 165/2001;

KYMA

MOBILITÀ

- il D. Lgs. n. 151/2015 (c.d. Jobs Act), art. 23 che modifica la fattispecie integrante il divieto dei controlli a distanza;
- il Regolamento Generale sulla Protezione dei Dati – Regolamento (UE) 2016/679 del 27.04.2016 (d'ora in poi GDPR; evidenziato che, con l'entrata in vigore delle Misure Minime per la Sicurezza Informatica della Pubblica Amministrazione (Circolare Agid n.2/17) e la definitiva applicazione del Regolamento Europeo per la Protezione dei Dati Personali (GDPR), l'Azienda ha la necessità di innalzare e rafforzare la tutela della protezione dei dati personali dei propri dipendenti e dei cittadini che usufruiscono dei servizi erogati dall'Azienda.

Rilevato:

- che l'elevato uso delle tecnologie informatiche (e in particolare l'accesso alla rete informatica e telematica, Internet e posta elettronica) e la messa a disposizione del personale aziendale di strumentazione informatica, nell'ottica di uno svolgimento più agevole delle attività, impongono la necessità di regolamentarne l'utilizzo attraverso specifiche disposizioni, onde evitare che comportamenti inconsapevoli possano generare problemi o minacce alla protezione dei dati personali, agli strumenti di lavoro e a tutti i documenti aziendali rilevanti;
- che in questo contesto tra i poteri del datore di lavoro rientra quello, solitamente riportato nell'ambito del potere direttivo, di controllare l'esatta esecuzione della prestazione lavorativa dovutagli, verificando se il proprio personale usi la prescritta diligenza e osservi le disposizioni impartitegli, prevenendo, ove possibile, o minimizzando utilizzi indebiti o non corretti che possano essere fonte di responsabilità;
- che proprio in considerazione della delicatezza dell'argomento risulta necessario porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche senza che ciò possa in alcun modo interferire nella sfera personale del lavoratore e nel diritto alla riservatezza e alla dignità, come sanciti dalla normativa vigente in materia di protezione dei dati personali e dallo "Statuto dei Lavoratori" (L. 20.05.1970, n. 300) ed, in particolare, dal nuovo articolo 4 come modificato dal D. Lgs. n. 151/2015 (c.d. Jobs Act), in tema di divieto dei controlli a distanza;

Dato atto:

- che, come da disposizioni dettate dal succitato D. Lgs. 151/2015, questa Azienda può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (Personal Computer, tablet, telefoni e smartphone) senza la necessità di accordi sindacali preventivi e fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo di detti strumenti e sulle modalità e i casi in cui potranno effettuarsi i controlli;
- che, con propria mail del 16 novembre scorso (**All. 2**) il D.P.O., Dott. Ernesto Barbone, esaminata l'ipotesi di Regolamento, lo ha condiviso nelle misure e nelle prescrizioni ivi

KYMA

MOBILITÀ

contenute.

Tanto premesso, si propone:

- a) di approvare la bozza del "Regolamento aziendale sulla Sicurezza Informatica", accluso alla presente per costituirne parte integrante e sostanziale;
- b) di fornire apposita informativa alle OO.SS., chiedendo di far pervenire eventuali rilievi entro il 31 dicembre 2024.

Il Capo unità organizzativa AA.GG.: dott.ssa Tiziana Tursi

Il Capo unità organizzativa informatica: p.i. sig. Enrico Picchi

Il Direttore Amministrativo f.f.: dott.ssa Maria Fabiola Menenti

Il Direttore Generale: dott. Pietro Carallo

IL CONSIGLIO DI AMMINISTRAZIONE

- udita la relazione che precede;
- Visto lo Statuto Sociale ed il Codice Civile ;
- Visti gli atti allegati;
- a voti.....

DELIBERA

- 1) di approvare la bozza del "Regolamento aziendale sulla Sicurezza Informatica", accluso alla presente per costituirne parte integrante e sostanziale;
- 2) di dare mandato agli uffici aziendali di fornire adeguata informativa alle OO.SS., chiedendo di far pervenire eventuali rilievi entro il 31 dicembre 2024.



Regolamento Utilizzo Sistemi ICT

KYMA MOBILITA' SPA

Ver. 1.0

Approvato con deliberazione del Cda n° XX in data XX XXXXXXXX XXXX

Sommario

1.	Premessa, scopo del regolamento e riferimenti normativi	2
2.	Campo di applicazione del Regolamento – Normativa e documenti di riferimento – Glossario.	3
3.	Informativa riguardante l'utilizzo degli strumenti elettronici Aziendali	9
4.	Principi generali e di riservatezza nelle comunicazioni	10
5.	Tutela del lavoratore	11
6.	Nuovi Dipendenti e/o Collaboratori	11
7.	Creazione nuove banche dati, gestione programmi	11
8.	Trattamento dei dati personali	12
9.	Comunicazione e diffusione dei dati	12
10.	Norme basilari di uso degli strumenti informatici	12
11.	Caratteristiche di base del software antivirus	13
12.	Utilizzo del Personal Computer	14
13.	Utilizzo della rete di KYMA MOBILITÀ	16
14.	Utilizzo della bacheca aziendale di KYMA MOBILITÀ	18
15.	Gestione delle password	18
16.	Utilizzo dei supporti magnetici	20
17.	Utilizzo di dispositivi portatili	20
18.	Utilizzo della posta elettronica	22
19.	Utilizzo della Posta Elettronica Certificata	26
20.	Utilizzo della rete Internet e dei relativi servizi	26
21.	Utilizzo degli impianti telefonici	28
22.	Utilizzo dei Social Media	29
23.	Utilizzo delle carte di pagamento	30
24.	Controlli	30
25.	Obbligo di fedeltà	33
26.	Osservanza delle disposizioni in materia di Privacy	34
27.	Violazione dei Dati – Data Breach	34
28.	Cessazione del rapporto di lavoro	35
29.	Dismissione degli strumenti aziendali.	36
30.	Sanzioni disciplinari per non osservanza della normativa aziendale	37
31.	Aggiornamento e revisione	37

1. Premessa, scopo del regolamento e riferimenti normativi

Con il presente Regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche e dei dispositivi fissi e mobili (personal computer, smartphone, tablet, modem/router, etc.), qualora utilizzati come strumenti informatici, che KYMA MOBILITÀ S.p.A. (in seguito anche "Azienda"), tramite la Ripartizione Informatica, Statistica ed Innovazione (in seguito anche "Ripartizione"), mette a disposizione del personale dipendente e degli, eventuali, collaboratori (di seguito "Utenti/Utilizzatori") per l'esecuzione delle funzioni istituzionali di competenza, non solo all'interno dei locali dell'Ente, ma anche in modalità remota o agile (smart working).

Lo Scopo del Regolamento, attraverso la promozione di una corretta "cultura informatica" che consenta di evitare il verificarsi di qualsiasi abuso o uso non conforme degli strumenti aziendali, è la tutela dei beni di proprietà dell'Ente consegnati in uso ai propri dipendenti, al fine di evitare condotte inconsapevoli e/o scorrette, che possono esporre l'Azienda a rischi connessi con la sicurezza, ad eventuali danni patrimoniali a terzi, o a danni di immagine derivanti dal libero accesso alla rete Internet dai Personal Computer e dagli strumenti mobili.

Ribadendo che l'utilizzo delle risorse informatiche e telematiche dell'Azienda deve sempre ispirarsi ai principi di diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Azienda ha adottato il presente Regolamento interno.

Si specifica infine che:

- gli Strumenti, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico della Azienda;
- i dati personali e le altre informazioni dell'Utente/Utilizzatore registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Per tutela del patrimonio si intende, altresì, la sicurezza informatica e la tutela del sistema informatico. Tali informazioni sono, altresì, utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

Si specifica, inoltre, che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, ove confliggenti, devono intendersi abrogate e sostituite

dalle presenti.

Il Regolamento è presente e consultabile in formato elettronico nella bacheca internet aziendale, nonché disponibile, in formato cartaceo, presso la Ripartizione Informatica, Statistica ed Innovazione.

3

2. Campo di applicazione del Regolamento – Normativa e documenti di riferimento – Glossario.

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, tirocinio, ecc.), nonché agli amministratori, agli organismi di controllo, ai dirigenti.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente/utilizzatore" deve intendersi ogni persona fisica o organismo di controllo come sopra menzionata, in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata nel prosieguo quale "incaricato del trattamento".

Normativa di riferimento

- Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- Articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».
- Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR) ed in particolare si richiamano:

Articolo 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento.

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 32 - Sicurezza del trattamento

1. *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 la libertà delle persone fisiche, il titolare del trattamento ed il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*
 - a) *la pseudonimizzazione e la cifratura dei dati personali;*
 - b) *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
 - c) *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
 - d) *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.*
 2. *Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*
 3. *L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.*
 4. *Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*
- "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
 - Circolare AGID del 18/04/2017, disposizioni in materia di sicurezza informatica;
 - Direttiva della Presidenza Consiglio Ministri n. 02/09, disposizioni in materia di utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro;
 - Provvedimento dell'Autorità Garante per la protezione dei dati personali "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 e successive modifiche ed integrazioni;
 - ACN-GPDP Linee Guida Conservazione Password del 7 dicembre 2023; Regolamento ACN n. 21007/24 "Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione, ai sensi dell'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221";
 - Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati - Registro dei provvedimenti n. 364 del 6 giugno 2024

- L. del 28 giugno 2024 n. 90 – rafforzamento della cybersicurezza nazionale e reati informatici.

DOCUMENTI DI RIFERIMENTO

1. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.
2. Procedura per la gestione dei Data Breach – Violazione dei Dati.
3. Procedura sull'esercizio dei diritti dell'Interessato.
4. Registro dei Trattamenti ex art. 30 GDPR.
5. Linee guida del Garante per posta elettronica e internet (del. N. 13 pubblicata sulla G.U. n. 58 del 10 marzo 2007)

GLOSSARIO E ACRONIMI

Amministratore di sistema o di rete: soggetto designato dall'Azienda che si occupa di vigilare sul corretto utilizzo dei sistemi informatici aziendali.

Apparati Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro dell'Azienda quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale.

Apparati Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, notebook, ultrabook, tablet e smartphone utilizzati dagli incaricati del trattamento per uso professionale.

Aree Sensibili: sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo f11 GDPR.

Consenso dell'Interessato o Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento.

Backup: duplicazione di un file o di un insieme di file su un supporto esterno al computer, per avere una copia di riserva.

Cloud: sistema configurato su server remoto che consente di disporre di risorse software e hardware (come memorie di massa per l'archiviazione di dati, o applicazioni), il cui utilizzo è erogato come servizio.

Dati Biometrici: i Dati Personali ottenuti da un Trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati Comuni: sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari.

Dati Genetici: i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati Giudiziari: Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Dati Particolari: Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale.

Dati relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

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

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

Download, scaricamento: ricevere o prelevare tramite rete telematica (ad esempio da un sito web) uno o più file, trasferendolo sul disco rigido del computer o su altra periferica.

DPO o Data Protection Officer: è una persona fisica, nominata obbligatoriamente solo nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR.

File sharing: sistema per lo scambio di file tra utenti di Internet tramite un server comune.

GDPR o Regolamento: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, job-sharing, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.

Hard disk: principale unità di memorizzazione dei dati sul computer, in cui vengono memorizzati il sistema operativo, i programmi applicativi, i dati di configurazione del computer, ed eventualmente i documenti creati dall'utente.

Instant messaging: strumenti di comunicazione on-line, simultanea ed in tempo reale, tra due o più utenti.

Login: procedura di accesso a un sistema informatico, che prevede l'inserimento di un codice identificativo (UserID o nome utente) e di una parola d'ordine (Password) da parte dell'utente. Nei sistemi che richiedono particolari cautele di sicurezza può essere integrata con un codice (PIN), assegnato all'utente o rilasciato in tempo reale tramite telefono cellulare (OTP).

Logout: procedura di scollegamento da un sistema informatico a cui si era avuto accesso tramite un'operazione di login.

OTP: codice numerico di sicurezza per accesso ai sistemi informatici, abbinato a nome utente e password, come il PIN, ma rilasciato tramite app o SMS sul telefono cellulare dell'utente, ed utilizzabile una sola volta per un tempo limitato.

Password: parola d'ordine dell'utente.

Phishing: Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.

PIN: codice alfanumerico breve (di solito non più di 8 caratteri) abbinato a nome utente e password, che integra la sicurezza negli accessi ai sistemi informatici.

Pseudonimizzazione: il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano

conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile.

Responsabile del Trattamento o Responsabile: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Rete Aziendale: rappresenta il perimetro digitale dell'Azienda, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN).

Server: computer di elevate prestazioni, che in una rete distribuisce un servizio (un applicativo, o l'accesso a cartelle e file di dati) agli elaboratori degli utenti collegati, detti client.

Software: è l'insieme delle componenti immateriali di un sistema informatico, costituito principalmente dai programmi che vengono elaborati dal computer; è contrapposto all'hardware, cioè la parte materiale, tangibile, dello stesso sistema.

SPAM: messaggio pubblicitario non richiesto, inviato in modo massivo e ripetuto a un numero molto elevato di utenti di Internet, tramite posta elettronica.

Spyware: software scaricato, per lo più in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario.

Strumenti Aziendali: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dall'Azienda agli incaricati del trattamento al fine di svolgere le proprie mansioni.

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

Trattamento o Trattato/Trattati: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Violazione Dei Dati Personali ovvero Data Breach: è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.

Worm: sottoclasse di virus, software che crea diverse copie di se stesso in uno stesso computer.

9

3. Informativa riguardante l'utilizzo degli strumenti elettronici Aziendali

KYMA MOBILITÀ S.p.A. rende noto che il sistema informativo è gestito dalle seguenti figure:

- a) personale incaricato che opera presso la Ripartizione Informatica, Statistica ed Innovazione, tra cui l'analista di sistema, eventuali consulenti esterni che operano sotto la diretta supervisione del personale incaricato oltre che del dirigente del settore competente;
- b) responsabili del trattamento, di volta in volta individuati tra coloro i quali è stata affidata in outsourcing la gestione di uno specifico sistema, ad esempio il Cloud¹ Aziendale.

Ogni figura indicata è stata autorizzata a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi come ad esempio aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc..

Detti interventi potranno anche comportare l'accesso, in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet visitati dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o di impedimento dell'utente.

Il personale incaricato ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.

L'intervento viene effettuato esclusivamente su chiamata dell'utente (nel momento di attivazione della connessione con il suo esplicito consenso) o, in caso di oggettiva necessità, a seguito della

¹Ndr.: Per tutte le tipologie di servizi, di infrastrutture ed in caso di utilizzo di infrastrutture (anche cloud), il Fornitore dovrà attestare che gli stessi siano conformi alle previsioni della determinazione ACN n. 307/2022 e s.m.i. e che in particolare siano state implementate tutte le misure relative ai "livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità" previste ai sensi dell'allegato A della determinazione AgID nr. 628/2021, A2 e C della determinazione ACN n. 307/2022 e s.m.i., ed inoltre adeguarsi al Parere sullo schema di Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione - 9 maggio 2024 - Registro dei provvedimenti n. 289 del 9 maggio 2024 ed al Regolamento unico per le infrastrutture e i servizi cloud per la PA, adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024.

rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, direttamente o tramite il personale della Ripartizione Informatica, Statistica ed Innovazione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Si rammenta che l'utilizzo degli strumenti mobili come smartphone e/o tablet deve seguire le stesse regole indicate successivamente per gli strumenti informatici aziendali.

4. Principi generali e di riservatezza nelle comunicazioni

I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

- il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);
- il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa;
- i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.

Il dipendente si attiene alle seguenti regole di trattamento:

- è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno della Società. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/unità organizzativa.
- È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
- È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.
- Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori della Società è necessario utilizzare le eventuali /zone sale dedicate.

5. Tutela del lavoratore

Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, 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.

È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16.

6. Nuovi Dipendenti e/o Collaboratori

All'arrivo di un nuovo dipendente e/o collaboratore, l'Area Risorse Umane, in relazione alle mansioni affidate, si occuperà di coordinare con l'area/unità organizzativa di destinazione e la Ripartizione Informatica, Statistica ed Innovazione, la creazione e/o assegnazione degli strumenti aziendali (siano essi strumenti fisici e/o informatici), la consegna delle lettere di incarico al trattamento dei dati, l'attivazione delle specifiche login informatiche in base ai servizi aziendali che dovrà utilizzare, nonché ad una formazione adeguata all'utilizzo degli stessi.

7. Creazione nuove banche dati, gestione programmi

Senza preventiva autorizzazione dei Titolari del Trattamento dei Dati a KYMA MOBILITÀ S.p.A: non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

8. Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'Azienda e, pertanto, in conformità alle informazioni che KYMA MOBILITÀ S.p.A. ha comunicato agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati da KYMA MOBILITÀ S.p.A. . L'incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

9. Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai soggetti esterni indicati da KYMA MOBILITÀ S.p.A. per ognuna di esse.

Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dall'Azienda.

10. Norme basilari di uso degli strumenti informatici

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte da KYMA MOBILITÀ S.p.A., nonché quelle che in futuro verranno comunicate.

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

1. i supporti removibili (a titolo esemplificativo ma non esaustivo per supporto removibile si intende: CD, DVD, Schede di memoria SD, dispositivi esterni USB) non possono essere utilizzati sugli strumenti informatici se non previo controllo da parte del personale della Ripartizione Informatica, Statistica ed Innovazione.
2. è obbligatorio sottoporre a controllo tutti i supporti removibili di provenienza incerta prima di eseguire o caricare uno qualsiasi dei file in esso contenuti;
3. limitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .BAT) e di sistema (.SYS) tra computer in rete;
4. non aggiungere mai dati o file ai supporti removibili contenenti programmi originali.

Regole operative

1. Tutti i computer dell'Azienda devono essere dotati di programmi antivirus;
2. Il Responsabile deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus;
3. Il personale delle ditte addette alla manutenzione dei supporti informatici devono usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta;
4. Ogni P.C. deve essere costantemente sottoposto a controllo anti-virus;
5. I supporti di memorizzazione quali, a titolo di esempio non esaustivo CD, DVD, Floppy, USB Drive, Smartphone, provenienti dall'esterno devono essere sottoposti a verifica da attuare con un dispositivo non connesso alla rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell'Amministrazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus;
6. All'atto della individuazione di un'infezione il virus deve essere immediatamente rimosso;
7. Il personale deve essere a conoscenza che la diffusione dei virus è punita dagli artt. 615-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del Codice Penale.
8. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.

11. Caratteristiche di base del software antivirus

Le postazioni di lavoro sono protette da software antivirus aggiornato quotidianamente ed in particolare:

- a. gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite Internet;
- b. deve essere particolarmente efficace contro i virus della nostra area geografica
- c. deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma
- d. deve poter effettuare una scansione automatica del floppy disk e comunque dei supporti di memorizzazione esterni come gli USB drives.
- e. deve accorgersi del tentativo di modificare le aree di sistema
- f. deve essere in grado di effettuare scansioni a intervalli regolari e programmati
- g. deve essere in grado di effettuare la scansione all'interno dei file compressi
- h. deve mantenere il livello di protezione in tempo-reale
- i. deve eseguire la scansione in tempo reale
- j. deve poter eseguire la rimozione del codice virale in automatico
- k. in caso di impossibilità di rimozione i file non pulibili devono essere spostati in una sub



KYMA MOBILITÀ S.p.A.

Società per Azioni con Socio unico soggetta a direzione e coordinamento da parte del Comune di Taranto

Via Cesare Battisti, 657 – 74121 Taranto / 099 7356111 – Fax 099 7794247

www.kymamobilita.it – kymamobilita@kymamobilita.it – PEC: kymamobilita@pec.kymamobilita.it

C.F., P.IVA e N° iscrizione al Registro Imprese di Taranto 00146330733 – Capitale Sociale € 2.340.463,00 int. vers.

directory predefinita

- l. deve essere in grado di effettuare la rilevazione la pulizia dei virus da Macro sconosciute
- m. deve essere in condizione di rilevare e rimuovere i virus da macro senza file pattern con un grado di riconoscimento superiore al 97%
- n. deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo.

14

Considerato che in sistemi basati su reti locali o su reti geografiche, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:

- 1. distribuzione degli aggiornamenti sia dei motori di scansione che degli eventuali file "pattern"
- 2. controllo e monitoraggio degli eventi virali
- 3. automatico spostamento in directory di "quarantena" di virus informatici risultati non pulibili
- 4. avviso all'amministratore di sistema di rilevazione di virus e indicazione del file "infetto".

Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si auto-installano, all'insaputa dell'Utente, all'interno del Pc, infettandolo e diffondendosi nella rete informatica dell'ente.

Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al personale tecnico autorizzato dal Responsabile dei servizi informatici.

Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale tecnico autorizzato che provvederà ad effettuare le dovute operazioni di disinfezione.

Si considererà comportamento sanzionabile quello dei dipendenti che assoggetteranno il proprio PC alla aggressione di virus per avere RIPETUTAMENTE superato gli alert del sistema antivirus, aprendo comunque i files dei quali veniva rilevata la pericolosità.

12. Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente o collaboratore, che deve sempre ispirarsi ai principi di diligenza e correttezza, è uno strumento di lavoro: esso deve essere custodito con cura evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, pertanto esso va utilizzato esclusivamente per fini professionali (in relazione alle mansioni assegnate), evitando usi per fini personali al di fuori dei casi consentiti ed autorizzati in maniera scritta dalla Direzione.



KYMA MOBILITÀ S.p.A.

Società per Azioni con Socio unico soggetta a direzione e coordinamento da parte del Comune di Taranto

Via Cesare Battisti, 657 - 74121 Taranto / 099 7356111 - Fax 099 7794247

www.kymamobilita.it - kymamobilita@kymamobilita.it - PEC: kymamobilita@pec.kymamobilita.it

C.F., P.IVA e N° iscrizione al Registro Imprese di Taranto 00146330733 - Capitale Sociale € 2.340.463,00 int. vers.

L'accesso all'elaboratore (accesso alla rete e screen saver), al sistema gestionale e a tutti gli altri applicativi aziendali sono protetti da binomio nome utente/password; quest'ultima deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (Bios) degli strumenti informatici che ne abbiano la funzione, senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

L'Amministratore di Sistema, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno. Lo stesso potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa Azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa Azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

In caso di interventi da parte di personale tecnico, l'utente è invitato a digitare personalmente la password ed a presenziare durante le operazioni di assistenza e/o installazione.

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 informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Amministratore di Sistema di KYMA MOBILITÀ; l'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore ed altri diritti connessi al suo esercizio aggiornato, da ultimo, con le modifiche apportate dal D.L. 16 ottobre 2017, n. 148, convertito, con modificazioni, dalla L. 4 dicembre 2017, n. 172.) che impone la presenza, nel sistema, di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore (art. 615-ter e 615-quater c.p. richiamati dall'articolo 24-bis del decreto 231/2001).

Nel caso fosse necessario sviluppare dei nuovi programmi o database personalizzati (ad esempio in Microsoft Access, HTML, ecc.) ad accesso condiviso da più utenti, è necessario discuterne preventivamente con la Ripartizione Informatica, Statistica ed Innovazione per valutarne la fattibilità, le possibili alternative e la protezione dei dati.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer,

salvo previa autorizzazione esplicita dell'Amministratore di Sistema.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Ove l'Azienda dovesse opzionare lo Smart Working o la possibilità di lavorare da remoto, oltre a censire gli utenti a ciò abilitati, gli stessi dovranno attivare le operazioni di sblocco di seguito descritte. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Si raccomanda comunque di attivare manualmente il blocco del proprio PC quando ci si allontana dallo stesso. Lo si può fare premendo contemporaneamente la combinazione di tasti "CTRL + ALT + CANC" e, nella videata che appare, premere il pulsante "Blocca computer".

Non è consentita l'installazione sul proprio personal computer di nessun dispositivo di memorizzazione, comunicazione o altro (come, ad esempio, masterizzatori, modem, "chiavette" USB), se non con l'autorizzazione espressa dell'Amministratore di Sistema.

Non è consentito l'utilizzo di sistemi di archiviazione esterna basati su "cloud" (a titolo esemplificativo ma non esaustivo sistemi come Dropbox, Wetransfer, OneDrive, etc) né l'utilizzo di sistemi di posta elettronica non aziendali se non per casi di assoluta necessità, in ogni caso evitando di utilizzarli per qualsiasi documento e/o file che contenga dati personali in carico al Titolare del Trattamento KYMA MOBILITÀ.

L'utilizzo di tutte le reti WiFi presenti in Azienda è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile in Azienda e dalla stessa configurata è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dalla Ripartizione Informatica, Statistica ed Innovazione.

I log relativi all'utilizzo di Strumenti, 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. I controlli possono avvenire secondo le disposizioni previste al successivo punto 20 del presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

13. Utilizzo della rete di KYMA MOBILITÀ

L'accesso alla rete aziendale ed ai sistemi aziendali è protetto da password individuale, che ha il compito di prevenire accessi da parte di soggetti non autorizzati ai sistemi.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia

legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup. Ciascun utente ha a disposizione un'unità di rete condivisa (es. Z:\, Y:\, K:\, ecc) sui server o sui NAS (dispositivi di archiviazione di rete) aziendali.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

L'Amministratore di sistema può in qualunque momento procedere alla rimozione di ogni cartella, file o applicazione che riterrà non essere attinenti alle finalità lavorative e/o essere pericolosi per la sicurezza, sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni tre mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È, infatti, assolutamente da evitare una doppia archiviazione di dati.

Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, sui dispositivi di rete aziendali.

E' fatto divieto assoluto di salvare qualsiasi tipologia di file contenente dati personali sulle cartelle di rete accessibili indistintamente a tutti gli utenti.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola stampare documenti o file molto lunghi sui dispositivi multifunzione. Su tali dispositivi è inoltre possibile effettuare scansioni di documenti, indirizzandole direttamente alla propria email aziendale. In caso di necessità le stampe o le scansioni in corso possono essere eliminate.

È vietato scansionare digitalmente documenti contenenti dati particolari, se non per casi strettamente necessari e alle seguenti condizioni congiunte:

- immediata asportazione del documento cartaceo dalla stampante;
- solo su file con destinazione cartelle di rete protette da password e/o ad accesso riservato esclusivamente all'utente che effettua la scansione o con invio via mail alla casella di posta di chi effettua la scansione.

È, altresì, vietato monitorare ciò che transita in rete.

Controlli su base individuale saranno attivati solo in caso di reiterati comportamenti illeciti e non conformi e comunque dopo un avviso generalizzato relativo al rilevato utilizzo anomalo degli strumenti dell'ente.

Non è consentito collegare alle prese di rete apparecchiature non autorizzate da parte del Responsabile dei servizi informatici, quali: hub, switch, access point o similari. Non è inoltre consentito installare o utilizzare qualsiasi altra

apparecchiatura atta a gestire comunicazioni, salvo specifica autorizzazione rilasciata dal Responsabile dei servizi informatici, quali, a titolo esemplificativo: modem, router, Internet key, Non è inoltre consentito effettuare spostamenti o modifiche di risorse collegate alla rete dell'ente (es. pc, Stampanti, fotocopiatori e altro) senza una preventiva autorizzazione.

I log relativi all'uso del File System e della intranet, nonché i file salvati o trattati su Server o Strumenti, 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. I controlli possono avvenire secondo le disposizioni previste al successivo punto 20 del presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

14. Utilizzo della bacheca aziendale di KYMA MOBILITÀ

È presente una Bacheca aziendale basata su piattaforma web. Ad essa possono avere accesso tutti gli utenti abilitati e profilati in relazione al ruolo aziendale.

Nella bacheca vengono caricati tutti i documenti di interesse aziendale (modulistica, regolamenti, comunicati, ordini di servizio, cedolini paga, cedolini turni, ecc).

Le password d'ingresso alla bacheca sono segrete e vanno gestite secondo le procedure impartite. È assolutamente proibito divulgarle.

15. Gestione delle password²

La sicurezza dei servizi e delle procedure informatiche è basata sull'uso di password e, ove richiesto, di codici di sicurezza (PIN oppure OTP).

Pertanto, è necessario che ciascun Utente scelga una password "robusta" e che tale password sia mantenuta rigorosamente segreta. A questo scopo è necessario scegliere la propria password seguendo i seguenti requisiti minimi, comuni a tutti i sistemi. Infatti, la password deve essere composta da almeno dodici caratteri e deve essere "robusta". Una password si dice robusta quando è difficile ricostruirla e cioè quando risponde ad alcuni principi quali:

- a) la password deve includere, di regola, le seguenti caratteristiche: lettera maiuscola, lettera minuscola, cifre, caratteri speciali da selezionare fra quelli messi a disposizione dal sistema di autenticazione;

² Ndr: Registro dei provvedimenti n. 362 del 31 agosto 2023 – Autorità Garante Privacy; Registro dei provvedimenti n. 594 del 7 dicembre 2023 – Autorità Garante Privacy; ACN-GPDP Linee Guida Conservazione Password del 7 dicembre 2023.

- b) la password non deve far riferimento ad informazioni personali o al servizio al quale si accede, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa;
- c) all'aumentare della sua lunghezza, aumenta la difficoltà a carpirla;
- d) non contiene parole che si trovano nei dizionari di qualsiasi lingua, anche se digitate al contrario, in quanto esistono software in grado di individuarle;
- e) non sono composte da semplici sequenze di tasti, come ad esempio "qwerty", o da ripetizioni del proprio nome utente (ad es. se il proprio utente è rossi; la password "rossi rossi" sarebbe inopportuna).

È necessario cambiare la password con regolarità. Ad ulteriore garanzia di sicurezza, oltre che in adempimento a specifiche disposizioni legislative, le password di accesso ai sistemi sono soggette a rinnovo obbligatorio, con cadenza predefinita, con segnalazione all'utente dell'approssimarsi della scadenza.

La password individuale deve essere riservata. L'Utente, al riguardo, deve mantenere i seguenti accorgimenti:

- a) non trascrivere la password su pezzi di carta o post-it lasciati in vista sulla scrivania, o attaccati al monitor;
- b) non comunicare a nessuno la propria password;
- c) non condividere con nessuno la propria password;
- d) assicurarsi che nessuno guardi la tastiera con l'intenzione di memorizzare la password, mentre la si digita;
- e) non inviare la password tramite e-mail e, se proprio è necessario comunicarla, farlo a voce, per telefono o a mano in una busta chiusa;
- f) non utilizzare la stessa password per più scopi o procedure informatiche.

Qualsiasi password deve essere immediatamente sostituita, dandone comunicazione all'Amministratore di Sistema, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore di Sistema.

La password di ingresso alla rete, se prevista, e degli eventuali gestionali non devono essere comunicate all'Amministratore di Sistema. Le altre password devono essere comunicate, solo nei casi in cui la mancata comunicazione pregiudicherebbe lo svolgimento dell'attività lavorativa in caso di prolungata assenza dell'incaricato (ad es. Programma per la gestione delle paghe, Home

Banking, fogli Word o Excel protetti da password, ecc.). Tale comunicazione deve avvenire tramite la consegna alla Ripartizione Informatica, Statistica ed Innovazione di un foglio in busta chiusa, o altro sistema equivalente, indicante:

- il proprio nome e cognome;
- l'eventuale nome di account dell'utente;
- la password;
- il nome dell'applicazione o del file o dell'apparato protetto.

20

Resta inteso che l'adozione di misure tecniche per la protezione delle password, la conservazione delle stesse per un arco di tempo superiore a consentire la verifica dell'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online o, se del caso, a garantirne la sicurezza (es. memorizzazione delle ultime password impostate per impedirne il riuso da parte dell'utente, c.d. password history, o di copie di sicurezza per assicurare il ripristino del sistema di autenticazione informatica in caso di incidente) presenta rischi per i diritti e le libertà delle persone fisiche anche in considerazione del progresso tecnologico che, con il passare del tempo, può rendere obsolete le misure tecniche adottate o comprometterne l'efficacia.

Dunque, al fine di assicurare la protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25 del Regolamento), è necessario che l'Ente rispetti, oltre al principio di integrità e riservatezza, anche quello della limitazione della conservazione di cui all'art. 5, par. 1, lett. e), del Regolamento, affinché le password siano tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per verificare l'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online o per garantirne la sicurezza e, comunque, in caso di cessazione dei sistemi informatici o servizi online cui consentono l'accesso oppure di disattivazione delle relative credenziali di autenticazione.

Laddove vengano invece adottate misure tecniche diverse da quelle individuate nelle citate linee guida, l'Ente in ossequio al principio di responsabilizzazione (artt. 5, par. 2, e 24 del Regolamento), deve essere in grado di comprovare che tali misure garantiscono comunque un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche.

16. Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, cd-rom e/o cd-rw, DVD e/o DVD-RW, schede di memorizzazione SD o similari, "chiavette" USB, ecc.) contenenti dati particolari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato e/o ve ne sia l'accesso da parte di persone non autorizzate. Qualora i supporti magnetici contenenti dati particolari non debbano più essere utilizzati per gli scopi per i quali erano stati destinati, essi devono essere consegnati all'Amministratore di Sistema, il quale provvederà a cancellarne il contenuto, annullando e rendendo non intelligibili e tecnicamente in alcun modo non ricostruibili le informazioni in essi contenute. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione.

17. Utilizzo di dispositivi portatili

L'assegnazione e l'uso dei dispositivi di telefonia e connettività mobile (cellulari, smartphone, tablet, modem/router, etc.), come quelle dei personal computer, devono rispondere all'interesse ed alle esigenze dell'Azienda, al fine di migliorare la qualità del lavoro e della produttività, in un quadro di economia, efficacia ed efficienza.

I dispositivi possono essere utilizzati come strumento informatico, sia per la gestione della comunicazione, ad esempio a mezzo e-mail, che per la navigazione online, oppure per la connettività Internet.

È fondamentale, dunque:

- a) individuare le figure aziendali che necessitano di un dispositivo mobile per l'esercizio della propria mansione;
- b) razionalizzare e controllare le spese riguardanti i servizi di telefonia e connettività mobile dell'Azienda;
- c) rispettare regole precise riguardo all'uso appropriato dei dispositivi mobili e delle relative utenze intestate all'Azienda.

Inoltre, in aggiunta a quanto indicato al capitolo "Utilizzo del personal computer", si definiscono ulteriori regole per gli utilizzatori di personal computer portatili e/o tablet e/o smartphone aziendali. L'utente è responsabile del o degli apparati portatili assegnati dall'Azienda e deve custodirli con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.

Ai dispositivi portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna e/o in caso di riparazione, in quanto potrebbero essere accessibili informazioni personali come, a titolo esemplificativo, foto, documenti, cronologia navigazione, email.

I dispositivi portatili utilizzati all'esterno (convegni, visite in aziende, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Al termine della giornata lavorativa, i dispositivi portatili devono essere lasciati negli uffici oppure si possono portare nella propria abitazione sotto diretta custodia.

Altri obblighi:

1. Tenere il dispositivo portatile con sé quando è possibile. Non condividere il proprio dispositivo portatile con altri per scopo privato.
2. Se si viaggia in aereo e/o treno, non mettere il dispositivo portatile nel bagaglio che viene imbarcato e/o riposto nelle cappelliere, e prestare attenzione a possibili furti nell'area di check-in degli aeroporti.
3. Il dispositivo portatile non dovrebbe essere lasciato in un veicolo incustodito.

4. Se è necessario lasciare il dispositivo portatile nell'albergo, chiuderlo in cassaforte, se disponibile.
5. Assicurarsi di collegare il personal computer portatile alla rete aziendale almeno una volta al mese, per scaricare gli aggiornamenti di sistema e dell'antivirus.

Il furto o smarrimento di qualsiasi dispositivo (telefono cellulare o smartphone, dispositivo di connessione remota o scheda SIM) deve essere immediatamente denunciato alle competenti Autorità di Pubblica Sicurezza, e tempestivamente comunicato - oltre che all'analista di sistema per quanto di propria competenza.

22

18. Utilizzo della posta elettronica³

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. I criteri che dovranno governare lo sfruttamento di questa risorsa sono la correttezza ed il buon senso. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse, tutti i messaggi inviati tramite l'indirizzo aziendale saranno considerati nella disponibilità dell'Azienda.

Il sistema aziendale per la posta elettronica è fornito dal programma Thunderbird, Outlook o similari oppure tramite accesso all'interfaccia web del sistema. All'interno della rete aziendale è vietato utilizzare qualsiasi altro sistema di messaggistica non autorizzato dagli Amministratori di sistema (ad esempio, il comando Net Send di Windows, etc.).

È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione e salvo casi di effettiva necessità e/o urgenza.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti (in termini di centinaia di MB e, ancor più di GB). Ogni incaricato è tenuto a rispettare le dimensioni massime, stabilite dall'Amministratore di Sistema, per la propria casella di posta elettronica aziendale e per i singoli messaggi.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per KYMA MOBILITÀ deve essere visionata od autorizzata dalla

³ Ndr.: Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati - *Registro dei provvedimenti n. 364 del 6 giugno 2024*; Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 - *Registro dei provvedimenti n. 393 del 2 luglio 2015*.

Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria. La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Per la trasmissione di file, che non contengano dati particolari, all'interno di KYMA MOBILITÀ è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). E' assolutamente necessario verificare la correttezza e provenienza delle mail contenenti link nei corpi delle email; prima di procedere a cliccare sul link è necessario verificarne la provenienza nei casi particolari anche con l'ausilio della Ripartizione Informatica, Statistica ed Innovazione.

Tutti i messaggi contenenti dati particolari nel corpo del testo e/o negli allegati vanno creati solo se strettamente necessario, in base alle mansioni svolte e quindi in base all'incarico ricevuto, vanno inviati solo a destinatari autorizzati.

È vietato inviare catene telematiche (o "di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore di Sistema. Non si devono in alcun caso attivare gli allegati di tali messaggi. Ciò vale anche per i messaggi di provenienza non identificabile.

Qualora si ricevano messaggi che nulla hanno a che vedere con l'attività lavorativa e che si ritiene abbiano fini pubblicitari (SPAM) si invita l'utilizzatore a:

- non rispondere a messaggi di dubbia provenienza e che nulla hanno a che vedere con l'attività dell'Azienda;
- non fornire dati finanziari e password di un utente, con il rischio di essere vittima di phishing;
- non cliccare su link che si trovano all'interno di mail pubblicitarie;
- non rispondere mai alle mail degli spammer, nemmeno per rimuovere il proprio nominativo dalla loro lista;
- spostare i messaggi nella cartella SPAM del sistema di posta, in modo che il sistema stesso possa acquisire informazioni utili a ridurre o debellare l'intrusione.

Non è consentito utilizzare la posta elettronica per pubblicizzare o divulgare messaggi personali

non riguardanti l'attività lavorativa all'interno della rete aziendale.

Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Per evitare perdite di dati, è possibile eseguire periodicamente l'archiviazione della posta elettronica. Tale archiviazione deve essere eseguita su supporti di archiviazione esterni.

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel caso di assenza programmata, nel rispetto del principio di necessità e di proporzionalità, l'utente deve attivare la risposta automatica ai messaggi di posta elettronica ricevuti, che informi i mittenti della durata della sua assenza e delle coordinate aziendali che dovranno utilizzare in tale periodo.

Per garantire la continuità dell'attività, nei soli casi di assenza improvvisa o prolungata, l'azienda incarica gli amministratori di rete di accedere alla casetta postale dell'utente, per inoltrare al titolare del trattamento le comunicazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. In tal caso sarà premura del responsabile del trattamento redigere di tale attività un apposito verbale che informi il lavoratore interessato alla prima occasione utile.

Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, si invita tutto il personale ad inserire nei messaggi un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel proprio regolamento aziendale.

18.1 Trattamento dei metadati nel contesto lavorativo ⁴

I metadati cui fa riferimento la presente procedura corrispondono tecnicamente alle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni nell'interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client.

Tali informazioni relative alle operazioni di invio e ricezione e smistamento dei messaggi possono comprendere gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, in

⁴ Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati

relazione al sistema di gestione del servizio di posta elettronica utilizzato, anche l'oggetto del messaggio spedito o ricevuto.

I metadati cui ci si riferisce la presente procedura presentano la caratteristica di essere registrati automaticamente dai sistemi di posta elettronica, indipendentemente dalla percezione e dalla volontà dell'utilizzatore.

Gli stessi metadati come qui intesi non vanno in alcun modo confusi con le informazioni contenute nei messaggi di posta elettronica nella loro "body-part" (corpo del messaggio), che rimane nella piena disponibilità dell'utente/lavoratore, all'interno della casella di posta elettronica attribuitagli.

I tempi di conservazione dei metadati devono in ogni caso essere proporzionati rispetto alle legittime finalità perseguite (sicurezza informatica, tutela del patrimonio informatico, mitigazione di eventuali incidenti di sicurezza, adozione tempestivamente le opportune contromisure). Ove i tempi di conservazione non siano definiti in maniera proporzionata alle finalità del trattamento, il titolare del trattamento può incorrere nella violazione del principio di "limitazione della conservazione" (art. 5, par. 1, lett. e), del Regolamento).

L'attività di raccolta e conservazione dei soli metadati/log necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione, si ritiene che possa essere effettuata, di norma, per un periodo limitato a pochi giorni; a titolo orientativo, tale conservazione non dovrebbe comunque superare i 21 giorni.

Sempre nell'ambito della predetta finalità (assicurare il funzionamento delle infrastrutture del sistema della posta elettronica), a cui risulta applicabile il comma 2 dell'art. 4 della L. n. 300/1970, l'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability previsto dall'art. 5, par. 2, del Regolamento, le specificità della realtà tecnica e organizzativa del titolare.

Spetta in ogni caso al titolare adottare tutte le misure tecniche ed organizzative per assicurare il rispetto del principio di limitazione della finalità, l'accessibilità selettiva da parte dei soli soggetti autorizzati e adeguatamente istruiti e la tracciatura degli accessi effettuati

Le predette garanzie non trovano invece applicazione "agli strumenti di registrazione degli accessi e delle presenze", così come "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (art. 4, comma 2, l. n. 300/1970), in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire, la presenza in servizio e l'esecuzione della prestazione lavorativa.

19. Utilizzo della Posta Elettronica Certificata

La posta elettronica certificata (PEC) è stata introdotta con il DPR 11 febbraio 2005, n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3" in cui vengono emanate le regole per l'utilizzo della PEC e viene stabilito, tramite l'Art. 4 comma 1, che la PEC consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge. Il suo utilizzo è regolamentato anche dal CAD (Codice dell'Amministrazione digitale) all'art. 6 e smi.

La PEC ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale.

Il personale che ha in uso tale tipo di posta elettronica sia che si tratti di un indirizzo individuale o legato ad un determinato settore/ufficio/funzione, deve rispettare le medesime regole soprariportate, riguardante l'uso della posta elettronica standard in dotazione.

Si raccomanda, infine, in tutti i casi e per ogni tipologia di posta elettronica, di segnalare all'Analista di sistema qualunque abuso del servizio di posta elettronica di cui l'utente sia venuto a conoscenza.

Si informa che, ai sensi dell'articolo 2214 del Codice civile e dell'articolo 22 del Dpr 600/73, la Società deve conservare per dieci anni sui propri Server di Posta Elettronica tutti i messaggi di posta elettronica a contenuto e rilevanza giuridica e commerciale provenienti da e diretti a domini della stessa. Si informa altresì che la Società, per il tramite dell'Amministratore di Sistema, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio le ovvero per motivi di sicurezza del sistema informatico, la Società per il tramite dell'Amministratore di Sistema può accedere all'account di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file. Si informa che, in caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà sospesa per un periodo di 3 mesi e successivamente disattivata. Nel periodo di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dalla Società solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio le, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a reinviare il messaggio ad altro indirizzo mail.

Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

20. Utilizzo della rete Internet e dei relativi servizi

Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Pertanto, è consentita la navigazione solamente nei siti legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e a pagamento (shareware) prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

È vietata la navigazione su siti a pagamento, se non si è espressamente autorizzati dalla Direzione.

È da evitare ogni forma di registrazione a siti i cui contenuti non sono legati all'attività lavorativa.

È vietata la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche, le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) e l'iscrizione a social forum.

È vietato ascoltare musica tramite Internet, scaricare file musicali e altri file di natura multimediale non riconducibili all'attività lavorativa (es. files mp3, mp4, m4v, mov, mpg o mpeg, wmv eccetera).

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, KYMA MOBILITÀ rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

I filtri sopracitati limitano l'accesso ai siti Internet che presentano i seguenti contenuti:

- illegali o non etici, stupefacenti, razzismo e odio, estremismo, violenza, occultismo, plagio; materiale per adulti, nudità, pornografia; giochi, scommesse, intermediazione e trading, download software freeware; social network, radio e tv via Internet (salvo i casi espressamente autorizzati dal Titolare); peer to peer; malware, spyware, hacking, proxy anonimi, bypass proxy, phishing.

Tali limitazioni sono purtroppo talvolta aggirabili con artifici informatici; di conseguenza, la responsabilità sul rispetto del divieto di accesso a tali contenuti è in ogni caso in capo all'utente. Si rende noto che i moderni sistemi di controllo e sicurezza della navigazione (web proxy), come quello adottato in KYMA MOBILITÀ, per soddisfare i requisiti di protezione, devono effettuare, con opportune tecniche, il controllo della navigazione effettuata tramite protocollo HTTPS (ormai diffuso nella maggior parte dei siti web), questa modalità permette al sistema di tracciare anche eventuali immissioni di informazioni all'interno di pagine crittografate, come ad esempio login e password.

I controlli, compiuti dal personale incaricato, avverranno mediante il sistema di controllo dei contenuti Sophos Web Protection e su base statistica.

Il controllo sui file di log non è continuativo ed i file stessi vengono conservati per un tempo congruo e bilanciato e comunque mai superiore ai 6 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

Il prolungamento dei tempi di conservazione dei log potrà aver luogo solo nei seguenti casi:

- Esigenze tecniche o di sicurezza del tutto particolari;
- Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- Su specifica richiesta dell'autorità giudiziaria.

28

Si informa che la Società, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso. Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, la Società registra per 180 giorni i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni. Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, la Società potrà trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme precedentemente indicate nel presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection Regulation".

20.1 Utilizzo di infrastrutture e servizi cloud

La Società, in caso di utilizzo di infrastrutture e servizi cloud, predispone e aggiorna un elenco dei propri dati e dei propri servizi digitali, comprensivo di tutti gli elementi necessari alla loro caratterizzazione ai fini della relativa classificazione, così come previsto dal Regolamento ACN n. 21007/24.

21. Utilizzo degli impianti telefonici

Per "impianti telefonici aziendali" si intendono tutte le infrastrutture tecniche e le apparecchiature, sia fisse che mobili, atte alla comunicazione vocale ed in uso all'interno e all'esterno (ad es. i cellulari assegnati) dell'Azienda.

Gli impianti telefonici aziendali rientrano nella categoria dei "beni aziendali" e per questo il loro uso deve essere improntato alla tutela del patrimonio aziendale. Questo significa che chi è autorizzato all'utilizzo degli stessi lo dovrà fare nel rispetto del principio indicato.

Chiunque usi gli impianti telefonici per scopi estranei all'attività professionale a cui è addetto lo dovrà fare limitando al minimo i costi derivanti dalla telefonata. Da questo discende che l'uso degli impianti in questione per scopi privati è consentito in caso di necessità ma limitato secondo le regole della correttezza e del buon senso.

Nessun tipo di controllo personale verrà effettuato sulla natura e sulla durata delle telefonate eventualmente compiute. Il contenuto di esse ed il numero chiamato sono obbligatoriamente

segreti ed ogni controllo in merito violerebbe diritti costituzionalmente garantiti. Verranno effettuate esclusivamente rilevazioni di carattere impersonale ed anonimo sull'eventuale aumento del traffico generale telefonico e sull'eventuale aumento dell'importo delle bollette. In caso di riscontro positivo qualunque ulteriore indagine in merito sarà autorizzata con provvedimento dell'Autorità Giudiziaria. Solo successivamente a questa verifica potranno essere presi provvedimenti disciplinari.

L'Azienda assume l'impegno di non accedere ai dati inerenti al traffico telefonico per finalità diverse da quella della tutela del patrimonio aziendale. E' altresì esclusa la riferibilità del numero telefonico composto alla persona del chiamante. Per qualunque indagine di questo tipo verrà preventivamente richiesta l'autorizzazione all'Autorità giudiziaria competente.

In caso di furto si richiamano le disposizioni di cui al punto 16.

22. Utilizzo dei Social Media

La condivisione dei contenuti nei social media – quali, a titolo esemplificativo ma non esaustivo, Facebook™, Twitter™, LinkedIn™, Google™, dei blog e dei forum, anche professionali – deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Azienda riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sugli utenti, sui fornitori ed altri partners dell'Azienda stessa. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Azienda.

L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso della Direzione Aziendale, oppure solo per quanto riguarda la piattaforma Facebook sulle pagine di KYMA MOBILITÀ, nel rispetto di quanto definitivo nelle specifiche direttive aziendali di utilizzo di tale strumento. L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Azienda, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo ma non esaustivo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un

comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale. Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con la Società, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili alla Società.

30

23. Utilizzo delle carte di pagamento

Ai dipendenti possono essere assegnate una o più carte di pagamento:

a) Carta aziendale di credito/debito: la Direzione si riserva il diritto di valutare le figure professionali eleggibili di tale strumento. In caso di furto o smarrimento, oltre a quanto previsto dal regolamento del gestore della carta consegnato contestualmente alla carta stessa, il dipendente è tenuto a darne tempestiva comunicazione all'Area Contabilità.

KYMA MOBILITÀ S.p.A. utilizzerà le informazioni sulla data, luogo, importo e modalità di pagamento esclusivamente ai fini di sicurezza, controllo di gestione e corrispondenza ai limiti previsti nonché per la prevenzione frodi.

24. Controlli

24.1 Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, la Società verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

I controlli devono essere effettuati nel rispetto del presente Regolamento e dei seguenti principi:

- Proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- Trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- Pertinenza e non eccedenza: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'uso degli Strumenti Informatici della Società può lasciare traccia delle informazioni sul relativo utilizzo. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte della Società, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi e possono permettere alla Società di prendere indirettamente cognizione dell'attività svolta con gli Strumenti Informatici utilizzati.

24.2 Controlli per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/ sostituzione/implementazione di programmi, manutenzione hardware, ecc.).

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni, il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

- avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
- successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, la Società potrà autorizzare il personale addetto al controllo ad accedere alle informazioni disponibili con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo dell'indirizzo IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

- Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedurali descritti ai punti precedenti, il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

24.3 Controlli per esigenze produttive e di organizzazione.

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

- i. Redazione di un atto da parte del Direttore e/o Responsabile Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
- ii. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
- iii. Redazione di un verbale che riassume i passaggi precedenti.
- iv. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
- v. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività. In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche). Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

25. Obbligo di fedeltà

KYMA MOBILITÀ ricorda in via formale che i dipendenti e collaboratori tutti sono tenuti alla rigorosa osservanza dell'obbligo di fedeltà secondo quanto espressamente previsto, in via generale, dall'art. 2105 Cod. Civ. che, fra l'altro, fa espresso divieto a ciascun prestatore di lavoro di "divulgare notizie attinenti all'organizzazione" e "ai metodi di produzione dell'impresa", o farne uso in modo da poter "recare ad essa pregiudizio".

Ciascun dipendente e collaboratore deve quindi astenersi non solo dai comportamenti espressamente vietati dall'art. 2105 Cod. Civ. ma anche da tutti quei comportamenti che, per la loro natura e le loro conseguenze, possano creare situazioni di conflitto ovvero di pregiudizio per le finalità e gli interessi dell'Azienda stessa o siano idonei, comunque, a ledere il presupposto fiduciario del rapporto di lavoro.

A mero titolo esemplificativo si ricorda che a ciascun dipendente e collaboratore è fatto espresso divieto di sottrarre documenti aziendali, di utilizzarne il contenuto, a vantaggio proprio ovvero di terzi, di rivelare dati e notizie riservate della Azienda, non solo tecniche, acquisite in occasione del rapporto di lavoro, potendo derivare da simili condotte una responsabilità anche di rilievo penale, integrando esse i reati sanzionati dall'art. 624 Cod. Pen. in tema di "Furto" dall'art. 623 Cod. Pen. in tema di "Rivelazione di segreti scientifici o industriali".

Ciascun dipendente e collaboratore è tenuto al rispetto delle norme in materia di protezione del diritto d'autore di cui alla Legge 22 aprile 1941, n. 633, la cui violazione potrebbe integrare, ad esempio, le fattispecie penali di cui all'art. 171 (Divulgazione di opere dell'ingegno attraverso rete telematica) e all'art. 171-bis (Reati in materia di software e banche dati) della medesima Legge n. 633/1941. È espressamente vietato l'impiego per finalità aziendali di beni tutelati da diritti d'autore acquisiti in elusione dei relativi obblighi o comunque con modalità difformi da quelle previste dal titolare. È inoltre espressamente vietato l'impiego di beni aziendali (come fotocopiatrici, sito web o altro) al fine di porre in essere condotte che violino la tutela dei diritti d'autore, quale che sia il vantaggio perseguito.

Si ricorda che chi fosse o venisse a conoscenza di comportamenti equivoci e/o potenzialmente dannosi per l'Azienda da parte di collaboratori, di ex-collaboratori, fornitori, concorrenti ovvero di terzi in generale è tenuto ad informare prontamente la Direzione Generale e tanto sia per evitare qualsiasi danno a carico della Società, sia per evitare di essere incautamente coinvolto in atti di favoreggiamento a favore ed in concorso con quanti cerchino di danneggiare la KYMA MOBILITÀ in violazione dei diritti delle Aziende stesse.

KYMA MOBILITÀ S.p.A. espressamente si riserva e fa salva ogni iniziativa ed azione a tutela delle proprie ragioni e posizioni ove vengano accertati comportamenti da parte dei propri dipendenti e collaboratori contrari agli obblighi di fedeltà, di lealtà, di - correttezza e di riservatezza sopra richiamati, potendo tra l'altro detti comportamenti integrare gli estremi della giusta causa ovvero del giustificato motivo di licenziamento nei confronti dei dipendenti responsabili e comunque giustificare la irrogazione di sanzioni disciplinari.

26. Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di Incaricato del trattamento dei dati.

Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al precedente capitolo 19), fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 679/2016).

Viene, ancora una volta, ribadito che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, KYMA MOBILITÀ provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970.

27. Violazione dei Dati – Data Breach

Con il termine data breach si intende un incidente di sicurezza in cui dati personali, protetti o

riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto nonautorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezza (ad esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- **perdita accidentale:** ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati o confidenziali;
- **furto:** ad esempio, data breach causato da furto di un notebook contenente dati riservati o confidenziali;
- **infedeltà aziendale:** ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico;
- **accesso abusivo:** ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite.

Ogni collaboratore e/o dipendente e/o Amministratore è tenuto a comunicare immediatamente al Direttore Generale qualsiasi evento, anche solo sospetto, di una violazione di dati. L'Azienda adotta delle apposite procedure di gestione e di risposta in ottemperanza al Regolamento UE 679/2016.

28. Cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro, per il corretto trattamento dei dati personali effettuato con gli strumenti elettronici aziendali e, come indicato nel presente Regolamento, premettendo che:

- a) la posta elettronica, sia interna che esterna, è un mezzo di comunicazione messo a disposizione del dipendente o collaboratore esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, avendo raccomandato di evitare l'utilizzo di tali strumenti per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali di comprovata urgenza;
- b) salvo casi eccezionali di comprovata necessità, le unità di rete sono aree destinate alla condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Avendo raccomandato di non collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa.

L'utente, con anticipo di almeno sette giorni rispetto alla data di cessazione del rapporto di lavoro, è tenuto a:

- a) eliminare, dalla propria casella di posta elettronica, solo gli eventuali messaggi personali;

- b) eliminare dalle unità di rete utilizzate solo gli eventuali file personali;
 - c) copiare i dati aziendali accessibili nel disco locale del proprio pc in una posizione accessibile al proprio responsabile per successive consultazioni.
 - d) Eliminare i dati personali da eventuali dispositivi portatili aziendali dati in uso esclusivo.
- L'amministratore di sistema, al termine dell'ultimo giorno di lavoro del dipendente o collaboratore, o al massimo entro il giorno lavorativo successivo, provvederà a:

- a) disattivare l'utenza di rete (login di Windows) assegnata precedentemente al dipendente/collaboratore, provvedendo ad eliminarla definitivamente entro 30 giorni;
- b) solo nel caso fosse assegnato un indirizzo email aziendale di tipo **nome.cognome@kymamobilita.it**, inserire nel sistema di posta elettronica un autorisponditore che segnalerà al mittente la disattivazione della casella di posta elettronica ed i dettagli sulle future comunicazioni verso l'Azienda. La casella di posta elettronica, comunque non più accessibile da nessuno, verrà definitivamente eliminata dal sistema entro 30 giorni (salvo diversi accordi).
- c) Cancellare tutti i dati personali, se presenti, dai dispositivi aziendali, fermo restando che è onere del responsabile del dipendente/collaboratore verificare che lo stesso abbia correttamente consegnato i dati aziendali oppure richiedere per tempo all'amministratore di sistema di effettuare tale operazione per conto del dipendente/collaboratore.
- d) Solo in casi eccezionali e documentati KYMA MOBILITÀ potrà inoltrare le mail indirizzate al dipendente dimissionario ad altra casella di servizio. L'inoltro ad altra casella verrà attivato esclusivamente nei casi in cui l'indirizzo email sia associato a particolari servizi esterni e verrà lasciato attivo per il tempo necessario alla comunicazione del cambio di associazione che dovrà essere comunicato da KYMA MOBILITÀ ai fornitori dei servizi esterni.
- e) E' sempre prevista l'attivazione della risposta automatica al mittente con indicazione specifica riguardo alla nuova casella email a cui ci si deve rivolgere.

L'utente dovrà consegnare tutti i beni aziendali ricevuti in dotazione.

29. Dismissione degli strumenti aziendali.

Gli Strumenti Aziendali devono essere considerati in tutto il loro ciclo di vita e, dunque, regole di comportamento devono essere seguite anche quando diventano inservibili o, per qualsiasi causa, devono essere dismessi.

Nel seguito, come prescritto nel Provvedimento del Garante per la Protezione dei Dati Personali "Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali" del 13 ottobre 2008, si elencano le regole da rispettare per rottamare Strumenti

Aziendali, quando non sono più utilizzabili poiché non funzionanti o, per qualsiasi motivo, non si intende più utilizzarli, nonché quando gli Strumenti Aziendali vengono smarriti o illecitamente sottratti.

Una volta effettuata la ricognizione dei dati contenuti nello Strumento Aziendale (che per definizione possono essere utilizzati solo per scopi lavorativi) da parte dell'assegnatario, l'Amministratore di Sistema e/o il personale della Ripartizione Informatica, Statistica ed Innovazione autorizzato e/o l'Azienda Esterna e/o il Consulente esterno incaricati delle attività di gestione sistemistica, provvedono ad applicare misure tecniche per la cancellazione sicura dei dati tramite programmi (es. wiping program) che provvedono a distruggere i dati ivi contenuti in modo crittograficamente sicuro o comunque a renderli totalmente irrecuperabili. L'effettiva cancellazione dei Dati Personali dai supporti contenuti negli strumenti elettronici può anche risultare dai seguenti metodi, anche secondo il tipo di Strumento Aziendale da dismettere:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica;
- demagnetizzazione ad alta intensità.

Le tecniche usate dovranno essere in ogni caso adeguate agli standard internazionali. La stessa procedura si applica ai supporti cartacei - contenenti Dati Personali e/o informazioni aziendali - per i quali viene utilizzato, se del caso, un distruggi-documenti. Qualora i dati non siano stati cancellati prima della consegna dello Strumento Aziendale a un rottamatore, l'Azienda richiederà al rottamatore una dichiarazione scritta di garanzia di avere distrutto lo Strumento Aziendale consegnato e di non avere acceduto ai dati in esso contenuti o ceduti a terzi, né di averne tratto copie, né cartacee né informatiche, né totali né parziali.

30. Sanzioni disciplinari per non osservanza della normativa aziendale

È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

Eventuali violazioni del presente Regolamento da parte dei dipendenti nonché di altre norme previste dal CCNL applicato, a seconda della gravità della infrazione, comportano l'adozione dei relativi provvedimenti disciplinari.

Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno dell'Azienda.

31. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenute necessarie, integrazioni al presente

Regolamento. Le proposte verranno esaminate dalla Direzione aziendale.

Il presente Regolamento è soggetto a revisione.



Al 2)

Oggetto: Regolamento Strumenti Aziendali**Mittente:** "dott. Ernesto Barbone" <ernesto@studioconsulenzabarbone.it>**Data:** 15/11/2024, 17:28**A:** "Dott.ssa Maria Fabiola Menenti" <mariafabiola.menenti@kymamobilita.it>**CC:** Tiziana Tursi <tiziana.tursi@kymamobilita.it>, Enrico Picchi <enrico.picchi@kymamobilita.it>

Buon pomeriggio,

Dopo aver visionato il regolamento, come meglio specificato in oggetto, lo si approva nelle misure implementate e nelle prescrizioni descritte.

Si potrà pertanto approvarlo e renderlo operativo

A disposizione,

Dott. Ernesto Barbone

mobile 338.444.11.41

La Privacy è un bene di tutti

La sicurezza e crittografia end-to-end allo stato dell'arte: Le informazioni contenute nella presente comunicazione e i relativi allegati sono protetti da livelli di sicurezza elevati e viaggiano su protocolli di crittografia end-to-end, pertanto è garantito il rispetto della privacy e la sicurezza contro attacchi informatici dall'invio sino alla ricezione della presente.

La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita ai sensi dell'art. 616 c.p. I dati forniti verranno trattati ai sensi dell'art. 13 del Regolamento UE 2016/679 (normativa sulla privacy). Se ha ricevuto questo messaggio per errore Ti preghiamo di distruggerlo e di informarci immediatamente contattandoci mandando una mail a dpo@studioconsulenzabarbone.it. Copia integrale dell'informativa potrà essere visionata presso le nostre sedi.