Policy per l'Uso degli Strumenti Informatici e dei Supporti Cartacei

1. Finalità

1.1 La policy ha lo scopo di conformare le attività lavorative concernenti l'uso di apparati elettronici o di supporti cartacei alle norme sulla riservatezza dei dati e sulla sicurezza delle informazioni
Il riferimento giuridico è dato dal:
REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO
E DEL CONSIGLIO del 27 aprile 2016
pubblicato dalla gazzetta ufficiale della comunità europea il 4 maggio 2016 e diventato contestualmente legge dello stato degli stati ad essa afferenti. I suoi effetti diventano operativi a partire dal 25 maggio 2018.

1.2 La presente policy include anche le politiche aziendali in riferimento all'uso dei mezzi di comunicazione di proprietà degli utenti al fine di salvaguardare la sicurezza sul lavoro e il rispetto delle norme etiche e di fedeltà e di diligenza nei confronti dell'azienda. Tali politiche non sono in contrasto con quanto previsto al punto 1.

1.3 La policy è inoltre conforme alle prescrizioni del garante e a quanto previsto dalla legislazione del lavoro D.Lgs 196/2003 e modifiche successive D.Lgs 185/2016.

2. Definizioni

2.1 Termini concernenti la riservatezza dei dati

2.1.1 **Dati personali**: 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;

2.1.2 **Categorie particolari di dati personali** - dati personali che rivelano **l'origine razziale o etnica**, **opinioni politiche**, **convinzioni religiose** o **filosofiche**, o **appartenenza sindacale** e il **trattamento di dati genetici**, **dati biometrici** al fine di identificare in modo univoco una persona fisica, dati riguardanti la **salute** o

dati riguardanti la **vita sessuale** o **l'orientamento sessuale** di una persona fisica.

2.1.3 **Interessato** - qualsiasi persona fisica vivente che è oggetto di dati personali detenuti da un'organizzazione.

2.1.4 **Trattamento** - qualsiasi operazione o insieme di operazioni eseguite su dati personali o su serie di dati personali, anche con strumenti automatizzati, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, reperimento, consultazione, uso, divulgazione mediante trasmissione, diffusione o altrimenti messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione.

2.1.5 **Titolare del trattamento**: FUTURAUTO LIKE S.r.l.

2.1.6 **Violazione dei dati personali** - una violazione della sicurezza che porta all'accidentale, o illecita distruzione, perdita, alterazione, divulgazione non autorizzata o accesso ai dati personali trasmessi, archiviati o altrimenti elaborati. Esiste l'obbligo per il responsabile del trattamento di segnalare violazioni dei dati personali all'autorità di vigilanza e laddove la violazione possa pregiudicare i dati personali o la riservatezza dell'interessato.

2.1.7 **Responsabile GDPR** – Persona incaricata dall'azienda di gestire monitorare e implementare i processi relativi alla riservatezza dei dati personali in ottemperanza al regolamento Europeo

2.2 Termini concernenti la riservatezza delle informazioni

Strumenti Elettronici – qualsiasi mezzo che consenta di accedere ad uno o più dati e/o di collegarsi ad una rete di dati o di fonia e/o di comunicare a distanza.
Personal Computer – solitamente abbreviato in **PC**, è un qualsiasi computer (elaboratore) di uso generico le cui dimensioni e prestazioni lo rendono adatto alle esigenze del singolo individuo nell'uso lavorativo quotidiano.
Stazione di Lavoro (si veda il punto precedente)
Computer Portatile – personal computer facilmente trasportabile di proprietà dell'azienda (sono assimilati i dispositivi quali tablet, palmari, smartphone e simili).
Wi-Fi - è una tecnologia per reti locali che consente l'accesso in Internet senza l'utilizzo di fili o cavi (WLAN)
Attrezzatura di Lavoro – qualsiasi mezzo, inclusi gli strumenti elettronici elencati ai punti precedenti.
Utente – colui che utilizza una attrezzatura di lavoro.
Azienda - FUTURAUTO LIKE S.r.l. con sede in Via Galileo Ferraris 5/A 56121Pisa
Server - componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate *clients*, cioè *clienti*) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer.
Client - indica genericamente un qualunque componente che accede ai servizi o alle risorse di un'altra componente detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware oppure al software.

Browser - è un'applicazione per il recupero, la presentazione e la navigazione di risorse sul web. Tali risorse (come pagine web, immagini o video) sono messe a disposizione sul World Wide Web (la rete globale che si appoggia su Internet), su una rete locale o sullo stesso computer dove il browser è in esecuzione.

Rete Aziendale – Sistema integrato di trasmissione delle informazioni in formato digitale costituito da linee di comunicazione e da nodi, ognuno dei quali può configurare una unità di elaborazione e trasmissione dei dati (punti 2.2.2, 2.2.3,2.27).

Log – sistema di registrazione ufficiale di eventi.

Password – Parola chiave di accesso utilizzata dall'utente per accedere e utilizzare una attrezzatura di lavoro.

Estensione – insieme di tre caratteri che aggiunta al nome di un file ne caratterizza la tipologia.

E-Mail – sistema di posta elettronica e messaggio da esso gestito

Spamming l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati (generalmente commerciali o offensivi) ed è noto anche come **posta spazzatura**.

Peer-to-Peer – sistema di computer (o di strumento elettronici) collegati senza l'intermediazione di server allo scopo di scambiare informazioni (file audio, video ecc.)

Chat – sistema di conversazione molti a molti basato su internet

Messaggistica istantanea - categoria di sistemi di comunicazione in tempo reale in rete, tipicamente Internet o una rete locale, che permette ai suoi utilizzatori lo scambio di brevi messaggi.

Phishing - truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale

Malware - abbreviazione per malicious software (che significa letteralmente *software malintenzionato*, ma di solito tradotto come *software dannoso*), indica un qualsiasi programma

informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, dati personali o informazioni aziendali riservate, accedere a sistemi, informatici privati, o mostrare pubblicità indesiderata

3. Norme di Comportamento Generali

3.1 Personal Computer e Portatili

Salvo autorizzazione scritta da parte dell'azienda è vietato:

- Cambiare la configurazione HW del PC affidato all'utente aggiungendo, togliendo o modificando componenti (lettore o masterizzatore DVD, supporti esterni di memorizzazione, modem, ecc.)
- Connettere alla rete aziendale apparati di proprietà dell'utente (smartphone, tablet, ecc.)
- Modificare la configurazione SW impostata dall'azienda installando programmi non autorizzati (come programmi peer-to-peer, applicazioni ricevute via email o altri mezzi, oppure scaricate via internet o da qualunque altra fonte e con qualunque altro metodo) oppure disinstallando programmi installati (come anti-malware ecc.)
- Sviluppare applicazioni in modo autonomo e non controllato.

Le azioni effettuate in violazione di quanto specificato costituiscono una grave infrazione ai doveri di diligenza nei confronti delle norme di sicurezza aziendale e di quanto qui stabilito.

Verrà quindi ripristinata senza preavviso la situazione precedente alla violazione e verrà fatta segnalazione al Manager di linea al responsabile della sicurezza e al Responsabile del GDPR

3.2 Spazi di memoria permanente riservati agli utenti

Sui server centrali vendono creati spazi di memoria (cartelle) riservati agli utenti per le loro necessità lavorative. Tali spazi non devono essere utilizzati per conservare informazioni personali ma soltanto quanto necessario allo svolgimento della propria attività. In caso si contravvenga a tale disposizione l'azienda non risponderà della perdita o dell'integrità di tali dati. È inoltre vietata, sia sui sistemi aziendali di uso personale che sui server, la conservazione di dati o immagini che costituiscano in qualunque forma reato, e ad es. ledono la dignità della persona, che rivestano carattere pedopornografico, incitino all'odio raziale o verso una qualunque discriminazione o costituiscano apologia di reato o istigazione a delinquere.

3.3 Procedure di Accesso ai Sistemi informatici

L'accesso ai sistemi informatici aziendali è regolato dall'utilizzo di credenziali assegnate ad ogni singolo utente. (si vedano le procedure GDPR-C DOC 9.1.1i e GDPR-C DOC 9.1.2i della documentazione GDPR)
Tali credenziali sono costituite dal *nome utente* e dalla *password,* esse sono personali ed uniche. La password deve contenere almeno 8 caratteri alfanumerici e speciali e deve essere cambiata all'atto del primo accesso (login) e in seguito ogni mese (documenti citati).

3.4 Gestione della sessione di lavoro

La stazione di lavoro deve essere configurata in modo in automatico affinché dopo *10 minuti* in stand-by venga attivato il salvaschermo e sia necessario reimmettere utente e password per accedere nuovamente al suo utilizzo.

A fine lavoro o pere un'assenza prolungata (*ore?*) l'utente deve chiudere la sessione, spegnere la stazione di lavoro ed eventuali altri apparati connessi che non richiedano una disponibilità continua.

I dati di utilizzo dei sistemi (inizio e fine sessione di lavoro e il dispositivo utilizzato) e i dati di navigazione in internet, vengono conservati nei termini consentiti dalle normative vigenti (per un massimo di 24 ore)

3.5 Utilizzo di INTERNET

La navigazione in internet, utilizzando strumenti elettronici di proprietà dell'azienda, è funzione esclusiva del perseguimento degli obiettivi e degli incarichi lavorativi.
I dati di navigazione in internet vengono conservati nei sistemi aziendali per non più di 24 ore. Tuttavia nel browser utilizzato possono rimanere tracce della navigazione nella cronologia, conservate sul sistema utilizzato, è cura dell'utente conservare le informazioni ritenute utili e funzionali al proprio lavoro. Tali informazioni potranno essere accedute dall'azienda solo in casi eccezionali connessi con la sicurezza e l'integrità dei processi aziendali o dietro richiesta dell'autorità giudiziaria.

3.6 Utilizzo della Posta Elettronica

- Gli utenti del sistema di posta elettronica di FUTURAUTO LIKE S.r.l.,siano dipendenti o a qualunque altro titolo, avranno a disposizione un indirizzo di posta elettronica che indicherà chiaramente la struttura e la funzione svolta all'interno dell'azienda nella forma: nomereparto@citroen-futurauto.it, tale indirizzo è a tutti gli effetti un bene aziendale e uno strumento di lavoro.
- Potranno essere assegnati anche indirizzi nominali contrassegnati da nome.cognome@citroen-futurauto.it,

anche tali indirizzi sono un bene aziendale oltre che uno strumento di lavoro.
In tutti e due i casi gli utenti devono apporre all'interno di ogni messaggio la propria firma e la funzione svolta

- Inoltre ogni utente si impegna ad un uso corretto ed in linea con le politiche aziendali in termini di protezione della riservatezza dei dati personali.
- In caso di assenza prolungata ogni utente dovrà provvedere ad attivare la risposta automatica ai messaggi in ingresso, specificando il periodo di assenza e un indirizzo alternativo a cui far pervenire le comunicazioni.
- In caso di assenza imprevista e nell'impossibilità per l'utente di provvedere all'attivazione di tale procedura, l'azienda potrà informare il Responsabile del GDPR che potrà richiedere eccezionalmente al responsabile dei sistemi informativi per tutelare la continuità dei processi aziendali di attivare la procedura in vece dell'utente impossibilitato.
- In caso di cessazione del rapporto l'azienda provvederà immediatamente a chiudere "*l'account* "di **posta nominale** e a provvedere a istituire un messaggio automatico con l'informazione ed un indirizzo alternativo a cui reindirizzare i messaggi.
  La posta verrà in tal caso cancellata a meno di necessità legate a ragioni legali e/o connesse all'interesse aziendale, in tal caso la casella di posta verrà criptata per evitare violazioni della privacy dell'interessato.
- L'utente dovrà adottare tutte le cautele necessarie in caso di ricezione di messaggi contenenti allegati. Allegati con estensione .exe,.bt,.xml,vbs,.vb,.zip,.doc,.pdf, possono contenere programmi pericolosi per la sicurezza aziendale, (Malware), oppure la richiesta di "cliccare" su un indirizzo internet particolare; in caso di dubbio chiedere assistenza al responsabile del sistema informativo, uno scorretto uso della mail aziendale può causare gravi danni all'azienda.
- L'uso di sistema di posta elettronica personale (webmail) attraverso i sistemi aziendali è fortemente sconsigliato in

quanto molto più vulnerabile ad attacchi di malware e di phishing del sistema aziendale.

3.7 Telefonia

Il telefono fisso e il telefono cellulare (smartphone) assegnati agli utenti dell'azienda sono a tutti gli effetti strumenti di lavoro di proprietà dell'azienda. Essi devono essere utilizzati esclusivamente per compiere mansioni lavorative, salvo casi particolari quali quelli legati alla sicurezza dell'utente o in generale a situazioni di necessità o di pericolo da esso conosciute.
Durante l'orario di lavoro, l'utente limiterà la ricezione di chiamate personali al minimo indispensabile.
Sono vietati l'uso di servizi a pagamento e l'orinazione di beni e/o servizi che comportano l'addebito dei costi direttamente sulla fattura telefonica, salvo autorizzazione dell'azienda.

3.8 Strumenti Mobili

Quanto descritto e prescritto in questo documento si applica a tutti gli strumenti mobili quali telefoni cellulari, computer portatili, tablet, ecc. che consentano l'accesso ad una rete di dati.
L'utente dovrà rigorosamente evitare di scaricare applicazioni che possono essere potenzialmente pericolose per la sicurezza dell'azienda, in caso di necessità si dovrà richiedere l'autorizzazione al Responsabile del GDPR e al responsabile del sistema informativo
L'utente dovrà avere la massima cura nel trasmettere informazioni (via email) attraverso la connessione ad una rete **Wi-Fi pubblica** poiché tali connessioni non sono sicure e possono comportare la perdita di dati personali, sensibili o riservati di interesse aziendale.

4. Norme di comportamento riguardanti i dati personali e sensibili

Particolari attenzioni dovranno essere messe in atto nei confronti della gestione di informazioni riguardanti dati personali e sensibili

4.1 Non è consentito ai dipendenti detenere o salvare localmente sulle loro stazioni di lavoro fisse o mobili elenchi di dati personali o sensibili.
Non è consentito estrarre liste di dati personali da database aziendali e salvarli sui propri dispositivi fissi o mobili.
In caso di esigenze particolari si deve richiedere l'autorizzazione formale del Responsabile del GDPR.

4.2 Non è consentito ai dipendenti l'invio di comunicazioni di marketing se non contemplato esplicitamente all'interno dei trattamenti legittimi effettuati dall'azienda e su base giuridica approvata.
In caso di dubbio è obbligatorio contattare il Responsabile del GDPR.

4.3 I dati personali e sensibili devono essere trattati esclusivamente per gli scopi per cui sono stati raccolti e nelle modalità autorizzate. La lista dei trattamenti è elencata nel registro dei trattamenti ed è consultabile in:
Per ogni dubbio si dovrà consultare il Responsabile del GDPR.

4.4 Sarà responsabilità dei singoli responsabili dei trattamenti dei dati osservare le precedenti prescrizioni.

5. Norme di comportamento riguardanti i documenti di tipo convenzionale (Cartacei).

5.1 I documenti cartacei contenenti dati personali dovranno essere trattati can la stessa attenzione se autorizzati, dovranno essere conservati in contenitori chiusi dotati di chiave di sicurezza e i documenti sensibili dovranno essere conservati in armadi di sicurezza.

5.2 Distruzione dei documenti. I documenti cartacei non più necessari dovranno essere distrutti in modo irrecuperabile.
Per i tempi e le modalità consultare il Responsabile del GDPR

5.3 Politica scrivanie pulite (clean-desk policy). Le scrivanie a fine lavoro o per assenze prolungate dovranno essere lasciate "pulite", cioè senza documenti e in particolare documenti contenenti informazioni riguardanti dati personali o sensibili ed anche documenti riservati riguardanti proprietà intellettuali aziendali o comunque informazioni rilevanti per lo sviluppo delle sue attività