# REGOLAMENTO AZIENDALE INFORMATICO E DEL TRATTAMENTO DEI DATI PERSONALI

## 1. Scopo del presente Regolamento

Lo scopo del presente Regolamento è la descrizione, anche ai sensi della vigente normativa sulla privacy, delle modalità per il corretto utilizzo dei sistemi informatici e telematici aziendali e del trattamento dati anche in formato cartaceo da parte del *Titolare del trattamento dati* – Asec S.p.a. (in seguito indicata come: "**Asec**").

## 2. Campo di applicazione

Il presente Regolamento si applica a tutti i dirigenti, dipendenti, componenti del Consiglio di Amministrazione e, in generale, a tutti gli utenti che anche occasionalmente sono autorizzati ad utilizzare i servizi tecnologici e informatici di Asec (in seguito cumulativamente indicati come: "**Utenti**" e singolarmente come: "**Utente**"), in merito all'utilizzo dei Pc, notebook, tablet smartphone, cellulari aziendali, ecc.... (in seguito anche indicati cumulativamente come: "**Strumenti**" e singolarmente come: "**Strumento**") ed in merito al trattamento dei dati personali anche in formato cartaceo.

## 3. Responsabilità

Le tipologie e le caratteristiche degli Strumenti da assegnare agli Utenti sono stabilite dall'Ufficio Sistemi Informativi di concerto con la Direzione.
I profili e le tipologie di accesso degli Utenti alle procedure informatiche, nel rispetto delle regole di sicurezza del trattamento dati ai sensi della vigente normativa sulla tutela dei dati personali, sono sottoposti anche alla validazione dell'Ufficio Risorse Umane.

## 4. Assegnazione dello Strumento

La progressiva diffusione di nuove tecnologie informatiche ed il libero accesso alla rete Internet, espone Asec al rischio di responsabilità civili, penali ed amministrative oltre a problemi per la propria immagine e sicurezza.
Asec fornisce istruzioni ad ogni Utente anche in merito alle misure di sicurezza da adottare onde evitare comportamenti scorretti e non conformi alla disciplina in materia di trattamento dei dati personali, inclusi i provvedimenti generali adottati dal *Garante per la protezione dei dati personali* – oggi Autorità di Controllo.
Gli Strumenti sono assegnati in relazione alla posizione ricoperta e/o alle esigenze di lavoro. Qualora per qualsiasi motivo dovesse cessare il rapporto di lavoro, l'Utente è tenuto a restituire ad Asec gli Strumenti ricevuti in dotazione entro l'ultimo giorno lavorativo.

Gli Strumenti devono essere custoditi con diligenza ed in modo appropriato, possono essere utilizzati solo per fini lavorativi in relazione alle mansioni assegnate e, in caso di furto, danneggiamento o smarrimento, l'Utente deve immediatamente darne notizia alla Direzione di Asec.
L'Utente è responsabile della custodia degli Strumenti ricevuti in assegnazione da Asec sia all'interno che all'esterno del luogo di lavoro.

## 5. Modalità di utilizzo

Tutti gli Strumenti devono essere protetti tramite *PIN* o *password* (con esclusione di impostazioni di blocco biometriche o per segno) al fine di prevenire l'accesso non autorizzato agli stessi.
Nel malaugurato caso di pregiudizio per la sicurezza o per il normale svolgimento delle attività lavorative aziendali o in caso di notizia di azione illecita ivi compresa il simpatizzare con ideologie terroristiche e/o discriminatorie per sesso, razza e/o religione o in caso di notizia di concorrenza sleale o di lesione dell'immagine aziendale, Asec si riserva la facoltà di accedere ai dati trattati dal singolo Utente nel rispetto della normativa vigente.

## 6. Personal computer

Le credenziali di accesso ai sistemi informativi aziendali (nome utente e *password*), devono essere custodite con particolare cura, in modo che nessuno possa appropriarsene o venirne a conoscenza ad esclusione del custode di tutte le credenziali, individuato nella figura dell'Amministratore di Sistema dott. Fabrizio Gemelli. È escluso a tal fine l'uso della posta elettronica o di forme di *short message*, per le quali eventuali credenziali fornite hanno esclusivamente carattere provvisorio e possono essere cambiate autonomamente secondo le indicazioni fornite dall'Amministratore di Sistema.
Le *password* non devono essere associabili allo stesso Utente, né di regola devono essere annotate per iscritto. Ove tale annotazione si rivelasse necessaria, la stessa deve essere custodita in luogo protetto separato dallo Strumento e priva di alcuna possibilità di collegamento allo Strumento stesso.
La *password* deve essere composta da almeno 8 caratteri e non deve contenere riferimenti facilmente riconducibili all'Utente. Quando autonomamente possibile, come nel caso di accesso al proprio Personal Computer attraverso il dominio aziendale, deve essere modificata almeno ogni 6 mesi. Ove l'Utente tratti *dati personali particolari,* ai sensi del *Regolamento Europeo 2016 / 679,* alias i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale o dati che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza a sindacato, particolari condizioni economiche svantaggiate, la *password* deve essere modificata almeno ogni 3 mesi.
Il *personal computer* deve essere configurato con blocco schermo protetto da *password* e deve essere spento ogni sera prima di lasciare l'ufficio o, in caso di assenza prolungata, a fine utilizzo.
Onde evitare il grave pericolo di contaminazione con *virus* informatici di qualsiasi specie nonché di alterazione della stabilità delle applicazioni aziendali, è vietato installare programmi non provenienti da Asec né è consentita la connessione, anche occasionale, a *cloud* ai quali l'Utente abbia accesso con credenziali non aziendali.

## 7. Utilizzo della rete aziendale; posta elettronica; navigazione

La rete aziendale deve essere utilizzata con la massima attenzione per evitare disservizi, inclusa la perdita di dati. Qualunque *file* o applicazione non connessa all'attività lavorativa non può essere dislocata, nemmeno per brevi periodi, sulla rete.
Asec si riserva il potere di rimuovere ogni *file* o applicazione installati in violazione del presente Regolamento, che riterrà illeciti o pericolosi per la sicurezza e la stabilità della rete aziendale.
Non è consentito utilizzare la posta elettronica aziendale per fini personali né è permessa la navigazione sul *Web* per fini non attinenti a quelli lavorativi.
L'eventuale attività lavorativa su *notebook* e/o *tablet* effettuata fuori dalla sede aziendale deve avvenire in luogo adeguatamente riservato. È rigorosamente vietata la connessione a reti *Wifi* esterne alla sede aziendale, quand'anche protette.

## 8. Protezione *antivirus*

Ogni Utente deve sempre tenere comportamenti adeguati a minimizzare il rischio di attacchi al sistema informatico aziendale. È tenuto a controllare il regolare funzionamento e lo stato di aggiornamento di tutto il *software*, ivi compreso *l'antivirus* installato sul proprio *PC*.
Qualora dovesse sospettare o rilevare la presenza di un virus, o comunque di un'intrusione informatica, dovrà:

- sospendere l'attività in corso;
- se in rete, scollegarsi immediatamente dalla rete aziendale mediante la disconnessione fisica del cavo di rete dal proprio pc;
- avvisare immediatamente l'Amministratore di Sistema dott. Fabrizio Gemelli onde adottare le misure tecniche più adeguate.

## 9. Utilizzo Cellulare / *Smartphone* aziendale

L'Utente dotato di Smartphone non deve scaricare alcuna applicazione non attinente all'attività lavorativa. L'eventuale attività lavorativa fuori dalla sede aziendale deve avvenire in luogo adeguatamente riservato. È rigorosamente vietata la connessione a reti *Wifi* esterne alla sede aziendale, quand'anche protette.

## 10. Trattamento dei dati personali

Il trattamento di dati personali da parte di ogni Utente deve avvenire, sia se operato con modalità informatiche ed elettroniche che in formato cartaceo, nel rispetto dei principi fissati dall'articolo 5 del *Regolamento Europeo* 2016/679:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'*Interessato* - colui i cui dati vengono trattati;
- limitazione della finalità del trattamento a quanto previsto dalla legge, con l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;

- esattezza e aggiornamento dei dati, con tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello strettamente necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: ogni Utente deve garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Asec ricorda ad ogni Utente che il *Regolamento Europeo,* come già il D.lgs. 196/2003 *Codice in materia di protezione dei dati personali*, prevede che ogni trattamento deve trovare fondamento in un'idonea base giuridica.

I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 di detto *Regolamento Europeo* e in particolare: consenso dell'*Interessato*, adempimento di obblighi contrattuali, obblighi di legge cui è soggetto Asec, interesse legittimo prevalente di Asec.

Per quanto riguarda le **"categorie particolari di dati personali"** (articolo 9 del *Regolamento Europeo*), il loro trattamento è ammesso solo:

- se l'Interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici di Asec o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; per finalità di medicina del lavoro quale la valutazione della capacità lavorativa del dipendente.

## 11. Misure di sicurezza

Asec ha adottato misure tecniche idonee a garantire un livello di sicurezza adeguato al rischio del trattamento con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato.

Fra tali misure, Asec:

- ha adottato un sistema informatico con funzioni di controller di Dominio, Dns, Dhcp, firewall, content filter, statistiche connessioni, monitoraggio, log traffico di rete, intrusion detection system, proxy, ecc... realizzato dalla Società Itesys S.r.l.;
- ha adottato, in fase di avvio del nuovo sistema Net@Dis, un sistema firewall realizzato a cura della Società Engineering;
- ha richiesto alla società Engineering la definizione del Progetto per fornitura, installazione e attivazione delle nuove funzionalità circa la pseudonimizzazione e cifratura dei seguenti dei dati presenti sul database di procedura ERP di Engineering, al fine di proteggere i dati personali e particolari di persone fisiche e giuridiche, garantendo loro piena e totale riservatezza, in conformità al Regolamento UE 2016/679 (GDPR);
- sta valutando di implementare una infrastruttura di sistema cloud, a vantaggio della possibilità di scalare gradualmente a seconda delle necessità, assicurando nel contempo misure atte a garantire il tempestivo ripristino della disponibilità dei dati;

### *12. Data breach*

Ogni Utente è tenuto a contattare immediatamente il *Referente Privacy*, identificato nel Dirigente Amministrazione Finanza e Controllo, dott. Salvatore Li Calzi all'indirizzo email privacy@asec.ct.it ed il *Data Protection Officer*, avv. Linka Zangara all'indirizzo dpo@asec.ct.it in caso di violazione di un dato personale trattato da Asec indicando:

- la natura della violazione, ove possibile, le categorie ed il numero approssimativo degli *Interessati* nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- descrivere le probabili conseguenze della violazione dei dati personali;
- le misure di sicurezza adottate per porre rimedio a detta violazione.

Nel malaugurato caso in cui detta violazione presenti un rischio per i diritti e le libertà delle persone fisiche, Asec tramite il proprio *Referente Privacy*, dott. Salvatore Li Calzi e il *Data Protection Officer*, avv. Linka Zangara, dovrà, entro 72 ore dal momento in cui ne è venuto a conoscenza l'Utente, notificare detto evento all'*Autorità di controllo – Garante per la protezione*.

Il *Referente Privacy*, dott. Salvatore Li Calzi tiene un apposito registro che documenta qualsiasi violazione dei dati personali.

### 13. Trattamento dei dati personali in formato cartaceo

Il trattamento dei dati personali in formato cartaceo è ammesso solo se essenziale ai sensi di legge e la documentazione può essere conservata solo per il tempo prescritto dalla normativa in materia civilistica, del diritto del lavoro, contabile e fiscale.

Se detti documenti hanno per oggetto *dati personali particolari,* devono essere sempre custoditi negli appositi armadi muniti di chiusura in dotazione a ciascun Ufficio e non devono mai essere lasciati incustoditi sui tavoli di lavoro o in prossimità di stampanti o fotocopiatrici.

Catania, 19/02/2019

Il Titolare del Trattamento