REGOLAMENTO AZIENDALE IN MATERIA DI GESTIONE DELLE INFORMAZIONI E DELLA PRIVACY (POLICY)

IGSA S.r.l.
Via Sant'Egidio 91 – fraz. San Michele
48124 Ravenna (RA)
C.F. e P. IVA: 02760110391

Aggiornato al 01/07/2024.

Premessa.
IGSA S.r.l. è una realtà aziendale che si occupa di manutenzione di strade, autostrade, piazzali, aree di sosta e di servizio, di formazione e manutenzione del verde e arredo urbano, di sfalcio manuale e meccanizzato di aree verdi di qualsiasi tipo e natura (comprese strade, autostrade, canali, porti, aeroporti, ferrovie e relative pertinenze) e di attività edile in generale (costruzione, riparazione e manutenzione di opere edili civili ed industriali, ivi comprese le opere accessorie, annesse e connesse, quali recinzioni, opere in muratura, ecc.), oltre a quanto previsto dall'oggetto sociale.

La progressiva evoluzione e diffusione di nuove tecnologie informatiche ed elettroniche impone a IGSA S.r.l. di adeguarsi alle conseguenti necessità di aggiornamento, predisponendo strumenti e accorgimenti volti a tutelare sia il proprio patrimonio che i diritti/interessi dei propri dipendenti.
Una modalità efficace per raggiungere questo ambizioso adeguamento è certamente quella di definire preventivamente le procedure e le regole aziendali che IGSA S.r.l. intende adottare e che devono, inevitabilmente, essere conosciute da ciascun dipendente.
L'utilizzo delle risorse informatiche e telematiche infatti deve sempre maggiormente ispirarsi ai principi di diligenza, di correttezza e di conoscibilità.

Principi generali.
Il presente regolamento si pone come obiettivo quello di disciplinare, in maniera specifica ma semplice e comprensibile, ogni aspetto delle modalità di utilizzo degli strumenti messi a disposizione dei dipendenti di IGSA S.r.l., con indicazione della misura e delle modalità di svolgimento di eventuali controlli.
In particolare, saranno affrontate le tematiche dell'utilizzo della strumentazione informatica da parte dei dipendenti (posta elettronica, Internet, social network, ecc.), del Regolamento UE n 679/2016 (c.d. "GDPR") e dell'utilizzo, da parte del datore di lavoro, degli impianti di videosorveglianza e di geolocalizzazione dei veicoli.
Il luogo di lavoro è una formazione sociale nella quale deve essere assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.
Il controllo sull'uso degli strumenti informatici deve infatti garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione ed il proprio patrimonio aziendale, quanto il diritto del lavoratore alla propria riservatezza e dignità, così come stabilito in primis dalla Legge n. 300/1970 (c.d. Statuto dei Lavoratori), poi dal D. Lgs. n. 196/2003 (c.d. Codice della Privacy) ed infine dal Regolamento UE n. 679/2016 (c.d. GDPR).
Quest'ultimo Regolamento infatti, entrato in vigore il 25/05/2018, impone al datore di lavoro in generale di adottare comportamenti proattivi volti ad assicurare il rispetto dello stesso (c.d. principio di responsabilizzazione – "accountability").

IGSA S.r.l. tratterà i dati dei propri dipendenti nel rispetto dei principi di liceità, correttezza e trasparenza, nonché per gli scopi determinati, espliciti e legittimi individuati nella presente policy e nella normativa nazionale e comunitaria, nel rispetto dei diritti di integrità e di riservatezza.
La presenza della presente policy inoltre è volta ad escludere ogni tipo di aspettativa dei dipendenti o dei terzi circa la confidenzialità/personalità di alcune forme e/o strumenti di comunicazione: tutti gli strumenti, tutte le informazioni, tutte le comunicazioni, tutto ciò che riguarda l'aspetto e l'ambito lavorativo è di proprietà esclusiva di IGSA S.r.l.

Finalità.
Le finalità principali della presente policy sono:

- accrescere la consapevolezza e responsabilizzazione del personale relativamente al corretto utilizzo degli strumenti di proprietà aziendale in modo da evitare comportamenti lesivi, non consapevoli e/o scorretti;
- non disperdere tempo e/o risorse per attività estranee alla prestazione lavorativa;
- evitare e/o prevenire sottrazioni e/o illeciti utilizzi di dati aziendali e/o personali, accessi abusivi a sistemi informatici e utilizzo per fini personali degli strumenti informatici di proprietà di IGSA S.r.l.;
- contrastare comportamenti estranei e/o lesivi del rapporto di lavoro.

Entrata in vigore e pubblicità notizia.
La presente policy entra in vigore il 01/07/2024.
Una copia del presente regolamento verrà consegnata a ciascun dipendente nelle forme e nei modi che IGSA S.r.l. riterrà più appropriate.
In ogni caso, una copia sarà costantemente disponibile nel cloud/server interno aziendale.
L'inosservanza dei contenuti del presente Regolamento può comportare sanzioni di natura civile e penale sia per il dipendente che per l'azienda: si invita pertanto ad una scrupolosa lettura e ad un suo massimo ed integrale rispetto.

Destinatari.
Il presente regolamento si applica a tutti coloro che operino, a qualsiasi titolo, all'interno e all'esterno della presente realtà aziendale nell'interesse o a favore della stessa.
In particolare, la presente policy si applica e disciplina:

- A tutti i lavoratori dipendenti e tutti i collaboratori di IGSA S.r.l. a prescindere dal rapporto contrattuale con la stessa intrattenuto;
- A tutte le attività connesse all'utilizzo degli strumenti informatici.

Definizioni.
Si evidenzia, che ai fini della presente policy (in ossequio a quanto previsto dal Regolamento UE n. 679/2016), si intende per:

- "**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;

- "**trattamento"**: 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;
- **"titolare del trattamento":** 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 del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- "**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- "**consenso dell'interessato**": 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;
- "**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 biometrici**": i dati personali ottenuti da un trattamento tecnico specifico relativi 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 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.

Si intende invece per "**sistema informatico**" il complesso organico di elementi fisici (hardware) ed astratti (software) che compongono un apparato di elaborazione dati.

Utilizzo della Rete aziendale.

L'unità di rete è un'area di condivisione di informazioni strettamente professionali che non possono essere utilizzate per fini diversi e/o personali e/o estranei al rapporto di lavoro.

La rete aziendale è di proprietà esclusiva di IGSA S.r.l.

Qualunque file che non sia legato all'attività lavorativa non può essere dislocato e/o salvato in queste unità, neppure per brevi periodi.

Su queste unità vengono svolte regolari attività di amministrazione, controllo e backup.

L'accesso alla rete avviene esclusivamente tramite digitazione di apposita password segreta (per quanto riguarda la gestione delle stesse si rimanda al capitolo "Password") assegnata a ciascun utente appositamente designato.

La password è associata direttamente alla persona fisica (il PC pertanto, con l'inserimento della password, riconosce la persona e permette di accedere alle cartelle e ai files che la stessa ha diritto di consultare e per le quali è stata previamente autorizzata dal datore di lavoro).
Il Titolare del trattamento, individuato nella persona giuridica IGSA S.r.l., può in qualunque momento effettuare controlli e procedere alla rimozione di files e/o applicazioni che riterrà pericolosi per la sicurezza della rete o in contrasto con l'attività lavorativa.
È espressamente vietata l'introduzione e/o la permanenza nel sistema in relazione ad aree e dati altrui, non strettamente connesse alla propria prestazione lavorativa.
Il personale dipendente può procedere in qualunque momento alla rimozione di ogni file e/o applicazione ritenuta pericolosa per la sicurezza della rete, degli strumenti informatici e dei dati contenuti.
Il personale tecnico/informatico incaricato ha facoltà di collegarsi e visualizzare in remoto (ad es. tramite Teamviewer) il desktop delle singole postazioni PC per garantire assistenza tecnica. L'intervento viene effettuato solamente su segnalazione dell'utente e previo parere positivo dei legali rappresentanti o del responsabile IT.
Il personale tecnico informatico, su indicazione del Titolare del trattamento, potrà infine compiere interventi per garantire la sicurezza e la salvaguardia degli strumenti informatici aziendali.
Questi interventi potranno comportare l'accesso ai dati trattati da ciascun dipendente, ivi compresi la posta elettronica, i siti internet visitati, ecc.

Password.
La credenziale di autenticazione di accesso al sistema di rete, di accesso ai programmi e dell'eventuale screen saver è assegnata dal responsabile IT.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user-id) associato ad una parola chiave riservata (password) che dovrà essere custodita dall'utente con la massima diligenza e non divulgata. La persona a cui vengono confidate le password è personalmente responsabile del loro utilizzo e della loro eventuale dispersione e/o comunicazione indebita e/o illecito utilizzo.
Le passwords devono essere di almeno 8 caratteri alfanumerici (di cui almeno una lettera maiuscola, una minuscola, un numero e un simbolo) e non devono essere facilmente riconducibili al dipendente (es. nome dipendente 1234, data di nascita, nome del proprio animale domestico, ecc.).
La finalità della password non risiede nel proteggere la segretezza dei dati personali contenuti negli strumenti messi a disposizione del singolo dipendente, ma solo quella di impedire che possano accedere ai predetti strumenti persone estranee alla società e/o non autorizzate.
È vietato annotarsi le passwords su post-it, fogli e/o altri documenti e apporli direttamente sul PC e/o lasciarli nei pressi della propria postazione, rendendo così facile il loro ritrovamento da parte di terzi non autorizzati.
Nel caso in cui si verifichi un furto di password e/o questa venga riferita per qualunque motivo ad altro dipendente, il custode della password dovrà darne comunicazione immediata al responsabile IT, il quale fornirà le dovute direttive e imporrà la sostituzione di una nuova password (diversa dalla precedente).

Utilizzo del Personal Computer.

Il PC affidato al dipendente (sia fisso che portatile) è uno strumento di lavoro ed è di proprietà di IGSA S.r.l.
Ogni utilizzo non inerente all'attività lavorativa e/o per fini personali è vietato. È espressamente vietato un utilizzo promiscuo.
Il PC deve essere custodito ed utilizzato con cura, evitando ogni forma di danneggiamento.
Non sono consentiti la memorizzazione e/o divulgazione di documenti informatici di natura oltraggiosa e/o discriminatoria per lingua, opinione religiosa e/o politica e/o sindacale e/o filosofica, origine razziale e/o etnica, vita e/o orientamento sessuale.
L'accesso al PC è protetto da password che deve essere custodita con la massima diligenza e non divulgata a terzi.
In caso di emergenza e/o assenza dell'utente, il responsabile IT avrà diritto di accedere al computer ed ai suoi contenuti per esigenze di carattere lavorativo, utilizzando la password comunicata e/o in caso di irreperibilità effettuando un reset della stessa.
È espressamente vietata l'introduzione e/o la permanenza nel sistema in relazione ad aree e dati altrui, non strettamente connesse alla propria prestazione lavorativa e unicamente per la stessa autorizzate.
È vietato utilizzare e/o scaricare programmi diversi da quelli ufficialmente installati dal personale tecnico per conto di IGSA S.r.l. L'inosservanza della presente disposizione espone la Società a gravi responsabilità civili. La violazione della normativa sul diritto d'autore, in particolare, è sanzionata anche penalmente.
Il datore di lavoro si riserva ogni diritto di rivalsa nei confronti del dipendente.
Gli strumenti informatici devono inoltre essere spenti in caso di inutilizzo, in caso di assenze prolungate e ogni sera prima di lasciare gli uffici.

Supporti rimovibili.
Per supporti rimovibili si intendono CD, DVD, supporti USB, ecc., forniti e di proprietà dell'azienda e contenenti dati e/o informazioni della stessa.
Tali strumenti devono essere utilizzati con particolari cautele in modo da evitare la loro perdita e/o danneggiamento e soprattutto che il loro contenuto possa essere trafugato e/o alterato e/o distrutto e/o recuperato e utilizzato da persone non autorizzate o senza titolo.
Occorre in ogni caso accertarsi che i dispositivi non contengano virus che possano danneggiare e/o creare problemi ai supporti informatici utilizzati dall'azienda.
È vietato inoltre scaricare e/o salvare files non attinenti alla prestazione lavorativa e/o per fini personali.
Tutti i files di provenienza incerta, anche se potenzialmente riferibili alla prestazione lavorativa, non devono essere aperti e/o utilizzati e/o installati e/o scaricati.
È vietato utilizzare sui dispositivi aziendali USB, CD, DVD, ecc. personali.
Il dipendente è personalmente responsabile della custodia e/o danneggiamento e/o perdita di questi dispositivi.

Protezione antivirus.
Il sistema informatico di IGSA S.r.l. è protetto da un software antivirus aggiornato quotidianamente.
Ogni dipendente deve in ogni caso tenere comportamenti tali da ridurre il rischio di attacchi al sistema informatico aziendale da parte di virus o altri software aggressivi.

Utilizzo della posta elettronica.
La casella di posta elettronica assegnata al dipendente è uno strumento di lavoro ed è di proprietà di IGSA S.r.l., compresi i suoi contenuti.
Essa rappresenta uno spazio di memoria di un sistema informatico destinato a contenere messaggi o altri file (immagini, video, documenti, ecc.) di un soggetto identificato tramite un account registrato presso un provider del servizio.
La casella di posta elettronica deve essere protetta da password di almeno 8 caratteri alfanumerici (di cui almeno una lettera maiuscola, una minuscola, un numero e un simbolo) e non facilmente riconducibili al dipendente (es. nome dipendente 1234, data di nascita, nome del proprio animale domestico, ecc.).
La finalità della password non risiede nel proteggere la segretezza dei dati personali contenuti negli strumenti messi a disposizione del singolo dipendente, ma solo quella di impedire che possano accedere ai predetti strumenti persone estranee alla società e/o non autorizzate.
La corrispondenza contenuta nelle email non ha natura privata e/o personale, ma è di proprietà della Società. È espressamente vietato quindi un utilizzo promiscuo.
Tale esplicitazione consente di escludere in assoluto ipotesi di legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.
Il dipendente infatti deve tenere in debita considerazione che i soggetti esterni possano attribuire carattere istituzionale alla corrispondenza ricevuta dagli stessi.
Il datore di lavoro mette a disposizione indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, segreteriaDT3@igsasrl.it, amministrazione@igsasrl.it, bandi@igsasrl.it).
L'indirizzo di posta elettronica assegnato non può essere utilizzato per fini personali e/o diversi e/o estranei all'ambito lavorativo.
A mero titolo esemplificativo, è vietato (anche a titolo di prevenzione da eventuali virus):

- l'invio e/o la ricezione di messaggi personali;
- aprire messaggi confluiti nella casella spam;
- l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, concorsi, forum, mailing list, catene telematiche, ecc.
- l'invio e/o la ricezione di allegati contenenti filmati e/o brani musicali non legati all'attività lavorativa.

Ogni indirizzo di posta elettronica deve essere protetto da password: la finalità della password non risiede nel proteggere la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo dipendente, ma solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società e/o non autorizzate.
Ogni comunicazione inviata e/o ricevuta che abbia contenuti di rilevante importanza e/o contenga accordi contrattuali e/o preliminari oppure contenga documenti riservati, deve essere comunicata al datore di lavoro, visionata ed autorizzata dallo stesso.
Il datore di lavoro può effettuare controlli saltuari e/o mirati (sono invece vietati i controlli massivi) e accedere alle email aziendali affidate ai singoli dipendenti per finalità esclusivamente lavorative per verificare l'effettivo e corretto adempimento della prestazione lavorativa contrattualmente convenuta e/o il corretto utilizzo degli strumenti di lavoro e/o in caso di sospetto indiziario circa l'utilizzo improprio dello strumento aziendale.

I controlli sono ammissibili soltanto nella misura in cui siano quindi strettamente proporzionati e non eccedenti lo scopo di verifica dell'adempimento contrattuale. Essi saranno inoltre limitati nel tempo e nell'oggetto.
Il datore di lavoro mette a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di altro soggetto o altre utili modalità di contatto della struttura. In questi casi, ogni dipendente è obbligato ad avvalersi delle presenti prescrizioni.
In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche tramite servizi webmail, in ogni caso entro 24 ore), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre lecitamente, in caso di necessità e mediante l'ausilio del responsabile IT, l'attivazione di un analogo accorgimento, avvertendo gli interessati.
Qualora, in caso di assenza improvvisa e/o prolungata e/o per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il dipendente può delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Il superiore gerarchico, in questi casi, potrà accedere alla casella di posta elettronica intestata al lavoratore (ma di proprietà dell'azienda) con l'ausilio di altra persona di sua fiducia, senza incorrere in sanzioni.
Per rimarcare la natura esclusivamente aziendale della casella di posta elettronica, i messaggi di posta elettronica contengono un avvertimento ai destinatari nel quale è dichiarata la natura non personale dei messaggi stessi, con la precisazione che le risposte e gli invii potranno essere visionati dal Titolare del trattamento secondo le regole fissate nella presente policy.
Il controllo, in ogni caso, non supererà mai i limiti imposti dalla finalità del trattamento di cui sopra.

Utilizzo della Posta elettronica certificata.
L'utilizzo della posta elettronica certificata aziendale (P.e.c.) soggiace alle medesime regole della posta elettronica ordinaria.
Al pari della posta elettronica ordinaria, rappresenta uno strumento di lavoro di proprietà esclusiva aziendale.
L'ordinamento italiano attribuisce ai messaggi inviati tramite P.e.c. un importante valore giuridico, che richiede pertanto le dovute cautele.
La P.e.c. infatti prevede un sistema di attestazioni aventi ad oggetto l'invio e la consegna di messaggi ad opera di soggetti terzi (gestori del servizio) e assicura la non alterabilità dei messaggi e dei documenti trasmessi.
Gli effetti giuridici connessi alla notifica di atti tramite P.e.c. si producono nel momento in cui il gestore del servizio P.e.c. rende disponibile il documento nella casella di posta del destinatario. Pertanto, nel caso ad esempio di notifica di sanzioni amministrative e/o altri atti giudiziari, la notifica a mezzo P.e.c. è idonea a rendere efficace il provvedimento nei confronti del destinatario. Il messaggio si intende ricevuto, ai fini legali, non appena risulti pervenuto nella casella P.e.c. del destinatario, indipendentemente dalla sua effettiva lettura. L'avvenuta consegna (con relativa ricevuta di consegna) equivale quindi a conoscenza del messaggio.

Il dipendente abilitato alla gestione di questa specifica casella (e a cui vengono confidate le relative credenziali di accesso) è tenuto quindi a prestare le dovute cautele e a verificare quotidianamente la presenza di nuovi messaggi.
L'invio di messaggi P.e.c., per l'efficacia legale attribuita, potrà quindi avvenire esclusivamente previa autorizzazione scritta del datore di lavoro.

Navigazione in Internet.
Gli strumenti informatici abilitati alla navigazione in Internet sono strumenti aziendali, di proprietà di IGSA S.r.l., necessari e collegati allo svolgimento dell'attività lavorativa.
È vietata pertanto la navigazione in Internet per motivi diversi e/o estranei a quelli strettamente correlati all'attività lavorativa (quale ad esempio la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività).
È vietata la partecipazione a forum, l'utilizzo di chat line (ad eccezione degli strumenti autorizzati quali Wildix, Whatsapp – limitatamente al gruppo aziendale), l'accesso tramite internet a caselle di posta elettronica personale, ecc.

Social Networks (Facebook, Instagram, Twitter, LinkedIn, ecc.).
I Social Networks sono piattaforme di comunicazione online tra utenti che condividono determinati interessi e attività oppure che intendono esplorare gli interessi e le attività di altri soggetti (Gruppo di lavoro Articolo 29 per la protezione dei dati, Parere 5/2009).
Le pagine social aziendali, quali Facebook e Linkedin, sono utilizzate con scopo promozionale ed al fine di pubblicare annunci di ricerche di personale e l'esclusivo autorizzato al trattamento è il datore di lavoro.
Durante l'attività lavorativa il dipendente non può utilizzare alcun social network.
Il tempo così impiegato, all'interno degli orari di lavoro, integra un grave inadempimento contrattuale facendo venire meno la prestazione contrattualmente dovuta.

Utilizzo dei telefoni, smartphone, tablet e fax aziendali.
Sono strumenti di lavoro, di proprietà di IGSA S.r.l., devono essere utilizzati solo per l'attività professionale.
Ogni utilizzo non inerente all'attività lavorativa e/o per fini personali è vietato.
La ricezione o l'effettuazione di chiamate personali è consentita solo nei casi di necessità ed urgenza.
Il dipendente è personalmente responsabile degli strumenti che gli vengono assegnati, sia per quanto riguarda il loro utilizzo, che per quanto la perdita, distruzione, danneggiamento, furto, ecc.
L'eventuale uso promiscuo (ossia l'utilizzo anche a fini personali) necessita della preventiva autorizzazione scritta del datore di lavoro.
Non sono autorizzate divulgazioni telefoniche di alcun genere riguardanti l'attività aziendale così come non sono ammesse risposte in merito a questionari di settore, statistiche, dati finanziari, dati sul personale assunto e/o quant'altro venisse richiesto telefonicamente. Ogni richiesta può essere inoltrata per iscritto, via fax, mail o posta: sarà l'ufficio competente a decidere come comportarsi.

Trattamento dei dati personali.

Il 25/05/2018 è entrato in vigore il Regolamento UE n. 679/2016 (c.d. "GDPR") che ha introdotto importanti novità (e imposto necessari adeguamenti) in materia di trattamento dei dati personali.
Prima che abbia inizio il rapporto contrattuale, il Titolare del trattamento informa il dipendente tramite un apposito documento ("informazioni") delle finalità, dei modi, delle categorie di dati e dei diritti che il Regolamento gli riserva in materia di dati personali.
In particolare, vengono comunicati:

- l'identità e i dati di contatto del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati (RPD);
- le finalità del trattamento e la base giuridica dello stesso;
- gli eventuali destinatari o le eventuali categorie di destinatari;
- la possibilità di trasferire dati personali a un Paese terzo o ad un'organizzazione internazionale;
- il periodo di conservazione dei dati (tutta la durata del rapporto di lavoro e, una volta cessato, per il tempo necessario al rispetto degli obblighi contabili previsti in capo alla Società) ed i criteri utilizzati per determinarlo (i dati sono conservati per il periodo necessario al raggiungimento delle finalità per le quali sono stati raccolti);
- il diritto di chiedere al titolare del trattamento l'accesso ai propri dati personali, ossia il diritto di conoscere e ottenere (ad intervalli ragionevoli) comunicazione in relazione alla finalità e alle modalità del trattamento;
- il diritto di rettifica dei dati, ossia il diritto di ottenere (senza ingiustificato ritardo) la correzione dei dati personali non esatti;
- il diritto alla cancellazione dei dati (c.d. diritto all'oblio), senza ingiustificato ritardo, qualora i dati non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; oppure nel caso in cui il dipendente revochi il proprio consenso su cui si basa il trattamento e non sussista altro motivo legittimo per trattarli; oppure in caso di opposizione al trattamento dei dati e non sussista alcun motivo legittimo prevalente per procedere al trattamento; in caso di trattamento illecito; in caso di adempimento di un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento; infine nel caso in cui i dati siano raccolti relativamente all'offerta di servizi della società dell'informazione a minori di età. Il dipendente non può esercitare il diritto all'oblio per fatti che lo riguardano se il trattamento dei dati personali è effettuato per l'esercizio del diritto alla libertà di espressione e di formazione; se il trattamento sia effettuato per l'adempimento di un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; per motivi di interesse pubblico nel settore della sanità pubblica; per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici se il diritto all'oblio rischi di rendere impossibile o pregiudicare gravemente il conseguimento degli obiettivi del trattamento; infine per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- il diritto alla limitazione dei trattamenti che lo riguardano, quando il dipendente contesta l'esattezza dei dati personali e per il tempo necessario alla loro verifica; nel caso di trattamento illecito e il dipendente si sia opposto alla cancellazione dei dati e ne abbia chiesto la semplice limitazione di utilizzo; nel caso in cui il titolare del trattamento non ne abbia più bisogno per il trattamento stesso, ma i dati personali sono necessari al dipendente per l'accertamento,

l'esercizio o la difesa di un diritto in sede giudiziaria; in caso di opposizione del dipendente e in attesa della verifica circa l'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli del dipendente stesso;

- il diritto di opporsi al trattamento dei dati per scopi di pubblico interesse o per legittimo interesse, oppure per trattamenti di marketing o, infine, per trattamenti storici, scientifici e statistici;
- il diritto alla portabilità dei dati, ossia la possibilità per il dipendente di chiedere la restituzione dei propri dati personali al termine del rapporto di lavoro o di chiedere al titolare del trattamento la loro diretta trasmissione al nuovo titolare del trattamento, se tecnicamente fattibile. La portabilità inoltre è riservata ai casi in cui il trattamento si basi sul consenso ai sensi dell'art. 6, paragrafo 1, lett. a), oppure dell'art. 9, paragrafo 2, lett. a), o su un contratto ai sensi dell'art. 6, paragrafo 1, lett. b), e il trattamento sia effettuato con mezzi automatizzati;
- il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca nel caso in cui il trattamento sia basato sull'art. 6, paragrafo 1, lett. a), oppure sull'art. 9, paragrafo 2, lett. a) del GDPR;
- il diritto di proporre reclamo al Garante della Privacy;
- la circostanza che la comunicazione di dati personali è obbligo contrattuale/requisito necessario per la conclusione del contratto di lavoro;
- l'obbligo di fornire i dati personali e delle possibili conseguenze della loro mancata comunicazione (mancata instaurazione del rapporto di lavoro);
- l'assenza di un processo decisionale automatizzato.

Una volta consegnate le presenti informazioni tramite apposito documento il titolare del trattamento chiederà al dipendente la sottoscrizione al trattamento dei dati personali, anche sensibili. Il consenso è condizione necessaria per l'instaurazione del rapporto di lavoro.
I dati saranno trattati esclusivamente dal personale incaricato e saranno custoditi in modo da evitare dispersioni, danneggiamenti, consultazioni ad opera di terzi non autorizzati e furti.

Violazione dei dati personali (c.d. data breach).
Il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza riguardo al rischio inerente alla violazione dei dati personali.
In particolare, tiene conto dei rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati trasmessi, trattati o comunque conservati.
Per evitare che i dipendenti possano venire indirettamente/direttamente a conoscenza di dati e/o informazioni dell'ufficio amministrazione, si prescrive che **la consegna delle buste paga avvenga mensilmente mediante l'accesso all'area riservata sul portale dei lavoratori, messo a disposizione su Cedolini.Online**. Ogni dipendente ha accesso esclusivo alla propria area riservata mediante accesso con CF e PIN.
In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante della Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la valutazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Aggiornato al 01/07/2024.

Qualora la notifica al Garante della Privacy non sia effettuata entro 72 ore saranno indicati i motivi del ritardo.
Il titolare del trattamento documenta qualsiasi violazione dei dati personali, il cui contenuto è riportato nel c.d. registro data breach.
Quando la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà del dipendente, il titolare del trattamento comunica a quest'ultimo la violazione senza ingiustificato ritardo.
La comunicazione contiene la descrizione della natura della violazione di dati, gli eventuali interessati e le eventuali categorie e il numero approssimativo di registrazioni di dati personali in questione; il nome e i dati di contatto del responsabile della protezione dei dati; la descrizione delle probabili conseguenze e delle misure adottate o do cui si propone l'adozione per porvi rimedio.
Qualora la violazione, il danneggiamento, l'accesso non autorizzato, la modifica e/o la divulgazione non autorizzata dei dati sia compiuta da un dipendente, quest'ultimo sarà ritenuto personalmente responsabile.

Videosorveglianza.
La raccolta, la registrazione, la conservazione e, in generale l'utilizzo di immagini configura un trattamento di dati personali.
Nel corso degli anni il Garante ha emesso tre provvedimenti generali in tema di videosorveglianza:

- Provv. 29 novembre 2000 "Il decalogo delle regole per non violare la privacy" - [doc. web n. 31019];
- Provv. Generale 29 aprile 2004 - [doc. web n. 1003482];
- Provv. Generale 8 aprile 2010 - [doc. web n. 1712680].

Il quadro normativo concernente la videosorveglianza si è arricchito recentemente con l'entrata in vigore del Regolamento UE 670/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pienamente esecutivo a partire dal 25 maggio 2018.
I sistemi di videosorveglianza in azienda, autorizzati dall'Ispettorato Territoriale del Lavoro di Ravenna (non sussistendo rappresentanze sindacali), sono installati esclusivamente per soddisfare esigenze organizzative, di tutela della proprietà e del patrimonio aziendale, di protezione dei dipendenti e di eventuali terzi, per l'acquisizione di prove nell'ambito dei c.d. controlli difensivi e per garantire la sicurezza dei dipendenti.
Gli impianti di videosorveglianza sono attivati in quanto tutte le altre misure sono state ponderatamente ritenute insufficienti o inattuabili.
I dipendenti sono informati della presenza delle telecamere all'interno e all'esterno dei locali tramite cartelloni (compilati) apposti prima di accedere all'area videosorvegliata.
Al momento della consegna delle informazioni di cui all'art. 13 del Reg. UE n. 679/2016 inoltre viene raccolto anche il consenso al trattamento dei dati personali tramite gli strumenti di videosorveglianza per le finalità sopra richiamate.
Non sono installati sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi).
Il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare l'effettivo e il corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro nel rispetto della libertà e dignità dei lavoratori, nonché,

con specifico riferimento alla disciplina in materia di protezione dei dati personali, ai principi di correttezza (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o dati di carattere sensibile.
Il trattamento dei dati è eseguito attraverso procedure informatiche e la eventuale visualizzazione avviene solo ad opera del titolare del trattamento. I dati sono conservati su apposito registratore doverosamente custodito per la durata massima di 7 giorni, con successiva cancellazione automatica.
I dati non saranno diffusi, venduti o scambiati con soggetti terzi, salvo l'utilizzo in caso di reati e/o illeciti perpetrati ai danni della Società: in tal caso le immagini saranno messe a disposizione dell'autorità competente.
L'incaricato preposto a gestire le immagini è il datore di lavoro.

Auto aziendali e Geolocalizzazione.
I veicoli aziendali sono di proprietà di IGSA S.r.l., e il loro uso è finalizzato unicamente all'esecuzione del rapporto di lavoro. È vietato ogni utilizzo per fini personali.
Un eventuale utilizzo promiscuo deve essere appositamente autorizzato dal datore di lavoro.
Tutti i veicoli aziendali sono muniti di strumenti di geolocalizzazione (GPS) che consentono al titolare e al responsabile del trattamento di essere sempre a conoscenza del posizionamento dei propri veicoli.
L'installazione di rilevatori satellitari è stata autorizzata dall'Ispettorato Territoriale del Lavoro di Ravenna per finalità di tutela del patrimonio aziendale.
Tutti i dipendenti sono avvisati della presenza dei rilevatori satellitari all'interno dei veicoli tramite vetrofanie apposte sui veicoli stessi.
Al momento della consegna delle informazioni di cui all'art. 13 del Reg. UE n. 679/2916 inoltre viene raccolto anche il consenso al trattamento dei dati personali tramite gli strumenti di geolocalizzazione per le finalità sopra richiamate
Il dipendente a cui venga affidato un veicolo aziendale ne è interamente responsabile.
Nel caso in cui si verifichi un qualsiasi danno, venga contestata una qualsiasi sanzione (sia penale, che civile, che amministrativa) il dipendente che aveva il possesso momentaneo del veicolo, sarà ritenuto responsabile e il datore di lavoro avrà diritto di rivalersi integralmente nei suoi confronti.
Il datore di lavoro può effettuare dei controlli mirati (direttamente o attraverso la propria struttura) al fine di verificare l'effettivo e il corretto adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro nel rispetto della libertà e dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, ai principi di correttezza (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza, tenuto conto che tali controlli possono determinare il trattamento di informazioni personali, anche non pertinenti, o dati di carattere sensibile.
Il trattamento dei dati è eseguito attraverso procedure informatiche e la eventuale visualizzazione avviene solo ad opera del titolare del trattamento. I dati sono conservati su apposito registratore doverosamente custodito per la durata massima di 90 giorni, con successiva cancellazione automatica.
I dati non saranno diffusi, venduti o scambiati con soggetti terzi, salvo l'utilizzo in caso di reati e/o illeciti perpetrati ai danni della Società: in tal caso le immagini saranno messe a disposizione dell'autorità competente.

Aggiornato al 01/07/2024.

Sono lecitamente utilizzabili in via meramente esemplificativa e non esaustiva i dati relativi all'ubicazione del veicolo, la distanza percorsa, i tempi di percorrenza, il carburante consumato nonché la velocità media del veicolo.
L'incaricato preposto a gestire i dati è il datore di lavoro.

Mancato rispetto della normativa aziendale.
Il mancato rispetto o la violazione delle regole contenute nella presente policy aziendale sono perseguibili con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.

Aggiornamento e revisione.
Il presente regolamento è soggetto ad aggiornamento e ad eventuale revisione periodica.
Varranno le medesime modalità informative.
Ravenna (RA), 01/07/2024

IGSA S.r.l.