POLICY PRIVACY

(ai sensi del Regolamento UE 2016/679 – GDPR e del D. Lgs. 196/2003 come modificato dal Decreto Legislativo 10 agosto 2018, n. 101)

Numero versione	Data approvazione Comitato ESG	Modifiche introdotte
V. 01/2021	16.04.2021	Prima versione

1. SCOPO

La presente policy privacy descrive il modello organizzativo adottato da questa struttura, sia quando tratta i dati in qualità di titolare, sia quando li tratta in qualità di responsabile del trattamento ai fini di un'adeguata gestione dell'acquisizione del consenso, della prevenzione e della protezione di tutti i dati personali.

Vengono perciò descritte le tipologie di interessati, il tipo di dati trattati, le azioni intraprese in qualità di Titolare e in qualità di responsabile del trattamento, la gestione delle persone autorizzate, la gestione dei responsabili del trattamento nominati e come vengono applicati tutti gli strumenti di prevenzione e protezione (vedi art. 32 del Reg. UE 2016/679-GDPR). Tutti i trattamenti effettuati (definiti nell'art.4 del GDPR) vengono eseguiti secondo i principi dettati dall'art. 5 (liceità, correttezza e trasparenza) e sono elencati nella rispettiva scheda del registro del trattamento (vedi plico generale).
Inoltre, gli stessi dati devono essere adeguati e pertinenti e il loro trattamento deve essere limitato al tempo strettamente necessario come riportato nelle finalità indicate nelle specifiche informative (es. informativa clienti o dipendenti, vedi relativi plichi operativi).
Questo documento spiega altresì l'importanza di censire ed individuare tutti gli archivi, sia cartacei (es. armadi, cassettiere) che elettronici (es. siti web, singoli pc, server locali, cloud, database gestiti nei server del software house, account di posta elettronica). Per entrambi gli archivi tutta la documentazione è stata suddivisa in 8 plichi di cui 1 generale e 7 operativi. Lo scopo di ogni singolo plico viene dettagliato alla fine del presente documento.

2. POLITICA DI PREVENZIONE E PROTEZIONE DEGLI ARCHIVI IN QUALITÀ SIA DI TITOLARE CHE DI RESPONSABILE DEL TRATTAMENTO

2.1. Prevenzione

La nostra politica di prevenzione e protezione prevede che l'ubicazione dei dati personali trattati ed archiviati sia monitorata almeno una volta l'anno, allo scopo di proteggerli in base all'ambiente che li circonda.

Le 3 misure di prevenzione adottate da questa struttura sono:
2.1.1. formazione - il primo passo della prevenzione è formare periodicamente tutte le figure coinvolte nel
trattamento dei dati.
2.1.2. minimizzazione - tutto lo staff del titolare del trattamento (es. persone autorizzate) viene formato ad archiviare solo i dati strettamente necessari per lo scopo per i quali sono trattati.

2.1.3. pseudonimizzazione (dove tecnicamente e legalmente possibile) - tutto lo staff del titolare del trattamento (es. persone autorizzate) viene formato a codificare i dati personali, sia cartacei che elettronici, in modo che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Vengono infatti creati due archivi: uno in cui ci sono i dati identificativi (es. nome e cognome) con il relativo codice assegnato e l'altro in cui ci sono i dati più delicati come quelli particolari (es. dati sulla salute) dove viene trascritto il solo codice creato nel primo archivio. Questi due archivi (quello contenente il codice e i dati identificativi e quello in cui ci sono i dati particolari associati al solo codice), sono conservati in ambienti separati ai quali può accedere un numero limitato di persone.

2.2. Protezione

Le 7 misure di protezione che la struttura sceglie di attuare in base al livello di rischio sono:
2.2.1. accesso controllato e limitato – viene ridotto il numero di persone autorizzate che accedono ai dati;
2.2.2. porte con chiave – viene isolato l'ambiente all'interno della struttura dove abbiamo i dati più delicati;
2.2.3. grate alle finestre (nei piani più bassi) – si riduce il rischio di furti da parte di persone malintenzionate;
2.2.4. sistema di allarme – viene ridotta l'intrusione da parte di malintenzionati fuori dall'orario di lavoro;
2.2.5. videosorveglianza – è possibile controllare chi ha avuto accesso agli archivi sia cartacei che elettronici;
2.2.6. dispositivi antincendio – viene ridotta la probabilità di danni agli archivi in caso di incendio;
2.2.7. armadi e cassettiere con chiave – in questo modo vengono protetti ulteriormente i dati più delicati; Per le specifiche misure di protezione relative i luoghi di lavoro, si rimanda al plico generale.

2.3. Archivi cartacei

Per gli archivi cartacei in base al livello di rischio, il titolare del trattamento sceglie di applicare sotto la propria responsabilità parte o tutte le misure di prevenzione e protezione sopra elencate. Vengono comunque sempre applicate le 3 misure di prevenzione sopra descritte e le seguenti misure di protezione:
1) chiusura degli armadi e cassettiere;
2) chiusura delle porte in caso di dati più delicati;
3) dispositivi antincendio;
4) accesso controllato e limitato. Nei casi ritenuti a maggior rischio vengono implementate le rimanenti misure di sicurezza sopra descritte.

2.4. Archivi elettronici

La stessa politica di prevenzione e protezione attuata per gli archivi cartacei si applica per gli archivi elettronici ubicati nei dispositivi hardware (es. smartphone, pc, server locali). Di seguito, per ogni tipologia di archivio, viene illustrata la modalità di prevenzione e protezione attuate in aggiunta a quelle sopra descritte.
2.4.1. Siti web. Per gli archivi dei siti internet la prevenzione avviene attraverso la minimizzazione dei dati archiviando solo nome, telefono, mail e provincia, quando si danno informazioni, archiviando anche cognome, codice fiscale e indirizzo quando si effettuano la vendita e la spedizione dei prodotti al cliente (previo consenso). La protezione avviene attraverso l'utilizzo del protocollo HTTPS, l'analisi annuale del sito, la lettera di nomina a persona autorizzata o responsabile del trattamento nei confronti di chi gestisce il sito e il server dove risiede il sito con la

relativa dichiarazione di conformità al GDPR. Per ogni singola sezione del sito vengono caricate tutte le informative dove si possono trovare tutte le specifiche tecniche con i relativi flag specifici per ciascuna finalità lasciando sempre la possibilità all'interessato di prestare o negare il consenso (es. informativa cookie, informativa raccolta contatti). In particolare, per quanto riguarda la gestione dei cookie, sul sito è stata caricata e messa a disposizione dei visitatori l'informativa cookie, ed è stato implementato il banner dei cookie in modo che il visitatore possa, prima di iniziare la navigazione, scegliere a quale cookie prestare il proprio consenso. I consensi di tutte le informative vengono memorizzati e messi a disposizione dell'autorità di controllo (anche in formato cartaceo ove possibile). Ogniqualvolta l'interessato inserisce i propri dati sul sito web per chiedere informazioni, registrarsi o effettuare acquisti esso dovrà acconsentire alle finalità dell'informativa specifica, inoltre il sistema invierà in automatico una mail di verifica che l'interessato dovrà convalidare per poter accedere al servizio richiesto. Solo dopo la convalida il titolare del trattamento erogherà il servizio richiesto e contestualmente archivierà i dati personali dell'interessato. In questo modo il titolare del trattamento potrà trattare, e quindi archiviare i dati personali avendo una maggiore garanzia che sia stato proprio l'interessato a richiedere il servizio sul proprio sito. La politica da attuare è quella di delegare un unico fornitore sia alla gestione del sito web (database) che a quella del server su cui il sito si appoggia per cui il fornitore sarà nominato sia amm. di sistema che Responsabile del trattamento.
2.4.2. PC. Le misure di prevenzione sono improntate per lo più sulla formazione delle persone autorizzate che utilizzano tali dispositivi.
Le misure di protezione adottate sono invece:
1) analisi del PC effettuata almeno una volta all'anno;
2) account diverso per ogni utente e ben distinto dall'account amministratore;
3) utilizzo di Firewall;
4) utilizzo di antivirus;
5) password d'accesso, sostituita ogni 3 mesi, di almeno 8 caratteri alfanumerici e con caratteri speciali;
6) accesso tramite impronta digitale, riconoscimento iride e Smart card;
7) cifratura dell'hard disk attraverso il sistema operativo;
8) salvaschermo (screensaver) con richiesta della password alla riattivazione del PC;
9) disabilitazione delle porte USB per evitare virus e furti di dati;
10) aggiornamento del sistema operativo;
11) nomina dell'amministratore di sistema adeguatamente formato per la gestione e la tutela dei singoli pc;
12) backup (vedi documento di politica di backup aziendale).

2.4.3. Smartphone/tablet. Le misure di prevenzione sono improntate per lo più sulla formazione delle persone autorizzate che utilizzano tali dispositivi. Le misure di protezione adottate sono invece:
1) password d'accesso, sostituita ogni 3 mesi e costituita da almeno 8 caratteri alfanumerici e caratteri speciali;
2) aggiornamento del sistema operativo;
3) utilizzo di antivirus;
4) cifratura dei dispositivi;
5) backup.

2.4.4. Singoli software gestionali (con database). A livello di prevenzione vengono attuate sia la

minimizzazione che la pseudonimizzazione ove tecnicamente e legalmente possibile. Le misure di protezione attuate sono:
1) utilizzo di una password di accesso robusta e diversa da quella del pc; 2) log che tracciano gli accessi al programma; 3) utilizzo del doppio fattore nel caso in cui si trattino dati particolarmente delicati.
Quando i gestionali sono utilizzati in qualità di titolare del trattamento la politica è quella di ottenere almeno una volta l'anno una dichiarazione di responsabilità sul mantenimento della conformità al GDPR da parte della software house.
Inoltre, essa viene nominata responsabile del trattamento in quanto archivia i dati per conto del titolare del trattamento. Qualora i dati vengano archiviati nel server locale le misure di protezione attuate sono quelle descritte per i singoli pc e server locali, qualora il server locale sia gestito da un fornitore esterno quest'ultimo viene nominato responsabile del trattamento.
Se i gestionali sono gestiti in virtù di un servizio offerto al titolare del trattamento questa struttura, in qualità di responsabile del trattamento (software house), attua tutte le misure di prevenzione protezione descritte nel paragrafo 2 e tutte le indicazioni che verranno eventualmente fornite dal Titolare del trattamento.

2.4.5. Server locali. Le misure di protezione, oltre tutte quelle attuate per i pc, sono:
1) utilizzo di firewall hardware;
2) log che tracciano gli accessi;
3) password d'accesso, sostituita ogni 3 mesi, di almeno 15 caratteri alfanumerici e con caratteri speciali;
4) utilizzo di un solo account da amministratore;
5) aggiornamento del sistema operativo;
6) nomina dell'amministratore di sistema adeguatamente formato per la gestione e la tutela dei server locali;
7) Cifratura dell'hard disk;
8) backup periodici.

2.4.6. Server in cloud. In questo caso la politica è quella di ottenere almeno una volta l'anno una dichiarazione di responsabilità sul mantenimento della conformità al GDPR da parte dell'azienda che gestisce il server, la quale viene anche nominata responsabile del trattamento in quanto archivia i dati per conto del titolare del trattamento.

2.4.7. Singoli account posta elettronica. A livello di prevenzione la struttura si avvale della formazione delle persone autorizzate, della minimizzazione e preferibilmente della pseudonimizzazione per file contenenti dati personali. A livello di protezione i file contenenti dati personali ricevuti ed inviati attraverso la posta elettronica possono essere protetti attraverso password o cifratura e vengono salvati su una cartella ubicata sul server (locale o in cloud), evitando salvataggi sul singolo pc.

3. PRINCIPALI COMPITI IN QUALITÀ DI TITOLARE DEL TRATTAMENTO
I Compiti principali del Titolare del trattamento sono:
1) capire con precisione quali sono le finalità dei propri trattamenti da comunicare all'interessato;
2) informare l'interessato e ottenere il consenso per le specifiche finalità attraverso le informative che devono contenere, oltre alle finalità, la tipologia dei dati trattati, i destinatari, i diritti degli interessati, i dati di contatto del titolare del trattamento e del DPO (ove nominato);

3) formare annualmente tutte le persone che trattano i dati per suo conto (es. persone autorizzate, resp. del trattamento) affinché i dati vengano protetti in maniera adeguata.
4) Redigere tutti i documenti necessari (es. Informative, DPIA, Registri del trattamento);
5) Verificare periodicamente la protezione dei dati personali (coadiuvato dal DPO ove nominato).

3.1. PRINCIPALI TIPOLOGIE DI INTERESSATI

Di seguito vengono contrassegnate le tipologie di interessati che il Titolare del trattamento gestisce:

1) potenziale cliente SI ☒ NO ☐;
2) cliente SI ☒ NO ☐;
3) potenziale dipendente (curriculum) SI ☒ NO ☐;
4) dipendente SI ☒ NO ☐;
5) fornitore (solo se ditte individuali) SI ☒ NO ☐;

3.2. TIPOLOGIA DI DATI IDENTIFICATIVI TRATTATI

Sono i dati più comunemente richiesti e anche quelli che possono arrecare meno danno dal punto di vista della privacy. Per questo tipo di dati il titolare del trattamento utilizza un livello medio alto di protezione che si basa sulle misure di prevenzione (es. pseudonimizzazione se ritenuta necessaria) e protezione (es. chiusura cassetti, cifratura hard disk) meglio specificate al punto 2 della presente policy e descritte nelle relative DPIA (ove redatte) e nel registro del trattamento.
I dati identificativi che vengono trattati in qualità di titolare del trattamento previo consenso sono:

1)nome SI ☒ NO ☐;
2) cognome SI ☒ NO ☐;
3)data di nascita SI ☒ NO; ☐;
4) luogo di nascita SI ☒ NO ☐;
5) codice fiscale SI ☒ NO ☐;
6) indirizzo SI ☒ NO ☐;
7) IBAN SI ☒ NO ☐;
8) credenziali SI ☒ NO ☐;
9) recapito telefonico SI ☒ NO ☐;
10) indirizzo mail SI ☒ NO ☐;
11) dati economici SI ☒ NO ☐;
12) dati finanziari SI ☒ NO ☐;
13) immagini SI ☒ NO ☐;
14) indirizzo IP SI ☒ NO ☐.

3.3. TIPOLOGIA DI DATI PARTICOLARI TRATTATI (EX DATI SENSIBILI)

La loro tutela è di massima importanza perché la loro violazione potrebbe avere forti impatti verso la persona. Per questo motivo il livello di protezione di questi dati è alto e si basa su misure più restrittive di prevenzione e protezione ove la pseudonimizzazione è la misura più attuata e necessaria (vedere punto 2 del presente documento, le relative DPIA e il registro del trattamento).
I dati particolari che vengono trattati in qualità di titolare del trattamento previo consenso sono:

1) origine razziale o etnica SI ☐ NO ☒;
2) opinioni politiche SI ☐ NO ☒;
3) convinzioni religiose SI ☐ NO☒;
4) appartenenza sindacale SI ☒ NO ☐;

5) dati genetici (es. DNA) SI ☐ NO ☒;
6) dati biometrici (es. impronte dentali) SI ☐ NO ☒;
7) dati relativi alla salute SI ☒ NO ☐;
8) orientamento sessuale SI ☐ NO ☒.

3.4. TIPOLOGIA DI DATI GIUDIZIARI TRATTATI

Si tratta di dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Questa struttura non tratta in alcun modo i dati giudiziari a meno che essi non siano funzionali all'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalla normativa sugli appalti; in questo caso le basi giuridiche delle operazioni di trattamento sono riconducibili agli artt. 10 Reg. UE n. 2016/679, e 2-octies, co. 1 e 3, lett. i), D.Lgs. 196/03, come modificato dal D.Lgs. 101/2018. In questi casi, i dati vengono trattati solo a livello cartaceo e, poiché la tutela di tali dati è di massima importanza in quanto la loro violazione potrebbe avere forti impatti verso la persona, vengono attuate misure più restrittive di prevenzione e protezione come cassetti e armadi chiusi a chiave e accesso limitato al personale debitamente formato (vedere punto 2 del presente documento, le relative DPIA e il registro del trattamento). Nei casi sopra descritti i dati giudiziari trattati in qualità di titolare del trattamento previo consenso sono:

1) condanne penali SI ☐ NO ☒;
2) reati SI ☐ NO ☒;
3) casellario giudiziale SI ☒ NO ☐;
4) carichi pendenti SI ☐ NO ☒

3.5. TIPOLOGIA DI PROFILAZIONE EFFETTUATA

La profilazione è una qualsiasi forma di trattamento **automatizzato** di dati personali che utilizza tali dati per valutare, analizzare o prevedere determinati aspetti relativi a una persona fisica. Gli aspetti valutati previo consenso (profilazione) dal titolare del trattamento sono di seguito elencati e contrassegnati con il "SI":

1) Rendimento professionale SI ☒ NO ☐;
2) Situazione economica SI ☐ NO ☒;
3) Salute SI ☐ NO ☒;
4) Interessi SI ☐ NO ☒;
5) Preferenze personali SI ☐ NO ☒;
6) Affidabilità finanziaria SI ☐ NO ☒;
7) Comportamento SI ☒ NO ☐;
8) Ubicazione/Spostamenti SI ☐ NO ☒;

La loro tutela è di massima importanza perché la loro violazione potrebbe avere forti impatti verso la persona fisica.
A livello di prevenzione la pseudonimizzazione è la misura più attuata e necessaria (ove legalmente e tecnicamente possibile). Il livello di protezione in questo caso è molto alto con misure ancor più restrittive (vedere punto 2 del presente documento, le relative DPIA e il registro del trattamento).

4. PRINCIPALI COMPITI IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO

Per tutti quei trattamenti in cui la struttura tratta e archivia i dati per conto del Titolare del trattamento essa si configura come Responsabile del trattamento i cui obblighi sono disciplinati attraverso il documento di nomina descritto al punto 5.2. Poiché viene attuata la stessa politica di prevenzione e protezione sia in qualità di Titolare che in qualità di Responsabile del trattamento, il trattamento è realizzato con le stesse misure di prevenzione e protezione (vedere punto 2) e i contenuti dei documenti redatti (DPIA, Registro del trattamento, Nomine e gestione del data breach) sono gli stessi, cambiando solamente la natura degli interessati (clienti e i dipendenti nel caso di titolare, utenti nel caso di responsabile del trattamento).
Il Responsabile del trattamento può nominare il Responsabile del trattamento di 2° livello previa autorizzazione del Titolare del trattamento.

4.1. TIPOLOGIA DI INTERESSATI (utenti)
Di seguito vengono contrassegnate le principali tipologie di interessati gestiti in qualità di responsabile del trattamento:
1) pot. cliente del cliente SI ☐ NO ☒;
2) cliente del cliente SI ☒ NO ☐;
3) pot. dip. del cliente SI ☐ NO ☒;
4) dip. del cliente SI ☒ NO ☐;
5) dip. del fornitore SI ☐ NO ☒;
6) fornitore del cliente SI ☒ NO ☐

4.2. TIPOLOGIA DI DATI IDENTIFICATIVI TRATTATI:
I dati trattati in qualità di Responsabile sono:
1) nome SI ☒ NO ☐;
2) cognome SI ☒ NO ☐;
3) data di nascita SI ☒ NO ☐;
4) luogo di nascita SI ☒ NO; ☐;
5) codice fiscale SI ☒ NO ☐;
6) indirizzo SI ☒ NO ☐;
7) IBAN SI ☐ NO ☒;
8) credenziali SI ☒ NO ☐;
9) recapito telefonico SI ☒ NO ☐;
10) indirizzo mail SI ☒ NO ☐;
11) dati economici SI ☒ NO ☐;
12) dati finanziari SI ☐ NO ☒;
13) immagini SI ☒ NO ☐; 14) indirizzo IP SI ☐ NO ☒

4.3. TIPOLOGIA DI DATI PARTICOLARI TRATTATI: (ex dati sensibili):
I dati trattati in qualità di Responsabile sono:
1) origine razziale o etnica SI ☐ NO ☒;
2) opinioni politiche SI ☐ NO ☒;
3) convinzioni religiose SI ☐ NO ☒;
4) appartenenza sindacale SI ☐ NO ☒;
5) dati genetici (es. DNA) SI ☐ NO ☒;
6) dati biometrici (es. impronte dentali) SI☐ NO☒;

7) dati relativi alla salute SI☐ NO☒;
8) orientamento sessuale SI ☐ NO ☒.

4.4. TIPOLOGIA DI DATI GIUDIZIARI TRATTATI:
l dati trattati in qualità di Responsabile sono:
1) condanne penali SI ☐ NO ☒;
2) reati SI ☐ NO ☒;
3) casellario giudiziale SI ☐ NO ☒;
4) carichi pendenti SI ☐ NO ☒

4.5. TIPOLOGIA DI PROFILAZIONE EFFETTUATA
Gli aspetti di valutati (profilazione - previo consenso) in qualità di Responsabile del trattamento sono di seguito elencati e contrassegnati con il "SI":
1) rendimento professionale SI ☐ NO ☒;
2) situazione economica SI ☐ NO ☒;
3) salute SI ☐ NO ☒;
4) interessi SI ☐ NO ☒;
5) preferenze personali SI ☐ NO ☒;
6) affidabilità finanziaria SI ☐ NO ☒;
7) comportamento SI ☒ NO ☐;
8) ubicazione/spostamenti SI ☐ NO ☒;

5. ADEMPIMENTI
5.1. NOMINA DELLE PERSONE AUTORIZZATE
Le persone autorizzate sono le persone interne alla struttura, adeguatamente istruite a trattare i dati personali, sulla base di un incarico specifico dato dal titolare del trattamento (es. dipendenti o collaboratori a P.IVA).
Ciascuna persona viene formata e sensibilizzata alla tutela del dato e riceve e sottoscrive il documento di nomina in cui vengono descritte in modo dettagliato le istruzioni che il titolare del trattamento impartisce al fine di proteggere i dati che essa tratta per conto del titolare.

5.2. NOMINE DEI RESPONSABILI DEL TRATTAMENTO
Questa struttura, quando tratta i dati in qualità di Titolare del trattamento, nomina tutti i responsabili del trattamento, che trattano ed archiviano i dati personali per suo conto (es. commercialista) e li istruisce sulle modalità di trattamento dei dati personali. Qualora un responsabile del trattamento avesse necessità di nominare ulteriori sub responsabili (2° livello) questa struttura ne valuterà la fattibilità caso per caso.
Qualora questa struttura dovesse trattare i dati per conto di un titolare del trattamento essa stessa verrà nominata Responsabile del trattamento. In qualità di responsabile del trattamento, se autorizzata dal titolare, potrà nominare responsabili del trattamento di 2° livello, che a loro volta potranno nominare responsabili di 3° livello (se ulteriormente autorizzati).
Questa struttura, poiché responsabile di 1° livello, conserva comunque nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dei sub responsabili. Il documento di nomina del responsabile del trattamento (sia quando sottoposto in qualità di titolare sia quando ricevuto in qualità di responsabile) è sempre in forma scritta e vi sono descritte

le categorie di dati personali trattati, la natura, le finalità e la durata del trattamento nonché le istruzioni al responsabile del trattamento da parte del titolare del trattamento.

5.3. NOMINA DEL RESPONSABILE DELLA PROZIONE DEI DATI (DPO/RPD)

Il DPO è una figura che deve essere designata dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, nonché consultive, formative e informative, relativamente all'applicazione del GDPR. La struttura, in virtù dei trattamenti effettuati e in ossequio al principio di accountability ha ritenuto opportuno nominare con apposito contratto scritto il proprio responsabile per la protezione dei dati i cui dati di contatto sono indicati nella relativa casella in calce al presente documento.

5.4. DPIA (Data Protection Impact Assessment - Valutazione di impatto sulla protezione dei dati)

La DPIA è un documento redatto dal Titolare del trattamento o dal Responsabile del trattamento che ha lo scopo di valutare il rischio (danno), indicare le misure di prevenzione e protezione, descrivere il flusso dei dati con i relativi destinatari.
La politica, sia in qualità di Titolare che di Responsabile del trattamento, è quella di redigere tutte le DPIA previste dall'allegato 1 del provvedimento n. 467 del 11 ottobre 2018 del Garante (di seguito allegato 1) e di redigere anche quelle non indicate espressamente nell'allegato 1 ma ritenute necessarie ai fini di una maggior tutela dell'interessato (vedere plico generale). Le DPIA redatte sono perciò le seguenti:

1) gestione delle buste paga SI ☒ NO ☐;
2) gestione selezione del personale SI ☒ NO ☐;
3) gestione videosorveglianza SI ☐ NO ☒;
4) gestione geolocalizzazione SI ☐ NO ☒;
5) gestione delle cartelle cliniche SI ☐ NO ☒;
6) gestione dei questionari delle attitudini professionali SI ☒ NO ☐;
7) gestione dati giudiziari SI ☐ NO ☒;

5.5. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'art. 30 del GDPR prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento (es. aziende con più di 250 dipendenti, trattamento di dati particolari).
Il registro è stato redatto sia in qualità di Titolare che in qualità di Responsabile del trattamento e attraverso la redazione e la revisione periodica di tale documento viene fornito un quadro aggiornato dei trattamenti in essere all'interno di questa organizzazione. Per ciascun tipo di trattamento è stata redatta una scheda nella quale sono descritti i dati di contatto del DPO e del Titolare del trattamento, dei responsabili del trattamento (in qualità di titolare) dei sub-responsabili (in qualità di responsabile), dei destinatari e degli eventuali contitolari.
Inoltre, vengono riportati i tempi di conservazione dei dati, le misure di sicurezza e la descrizione degli archivi elettronici e cartacei. Le attività svolte ed elencate nel registro sono:

1) gestione raccolta contatti SI ☒ NO ☐;
2) gestione centralino SI ☒ NO ☐;
3) gestione selez. personale SI ☒ NO ☐;
4) gestione questionari valut. dell'attitudine professionale SI ☒ NO ☐;
5) gestione buste paga SI ☒ NO ☐;
6) gestione visite mediche dip. SI ☒ NO ☐;

7) gestione formazione dip. SI ☒ NO ☐;
8) gestione preventivi/contratti SI ☒ NO ☐;
9) gestione fatturazione SI ☒ NO ☐;
10) gestione cartelle cliniche SI ☐ NO☒
11) gestione recupero crediti SI ☒ NO ☐;
12) gestione sistemi aziendali e account aziendali SI ☒ NO ☐;
13) gestione videosorveglianza SI ☐ NO ☒; 14) gestione geolocalizzazione SI ☐ NO ☒; 15) gestione dispositivi di misura SI ☐ NO ☒;

5.6. GESTIONE DEI DIRITTI DELL'INTERESSATO

Questa struttura, quando si configura titolare del trattamento, adotta precise procedure per fornire all'interessato tutte le comunicazioni di cui agli articoli da 15 a 22 relative ai diritti dell'interessato espressamente indicate nelle informative redatte e consegnate all'interessato.
In particolare, per quanto riguarda il diritto all'oblio (art.17 GDPR) in caso di ricezione della richiesta da parte di un interessato la procedura prevede le seguenti fasi:
1) controllo dell'effettiva presenza presso gli archivi propri o dei propri responsabili dei dati della persona che ha fatto richiesta;
2) invio modello di cancellazione all'interessato con verifica identità dello stesso (come indicato dal considerando 64 del GDPR);
3) cancellazione dei dati dell'interessato dai propri archivi con codifica della richiesta di cancellazione (anonimizzazione) e richiesta di cancellazione a tutti i responsabili che hanno in archivio i dati;
4) verifica dell'effettiva cancellazione dei dati dei propri responsabili del trattamento e comunicazione dell'avvenuta cancellazione all'interessato con consegna del codice di richiesta cancellazione. 5) a questo punto non esisteranno più dati personali dell'interessato se non un codice di cancellazione anonimo.

5.7. DATA BREACH

Con il termine "data breach" si intende una 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 sia in qualità di titolare che di responsabile del trattamento. Al fine di evitare eventi di data breach vengono attuate tutte le strategie di prevenzione e protezione descritte nei paragrafi precedenti del presente documento sia per i trattamenti eseguiti in qualità di titolare che di responsabile del trattamento.
Quando la struttura tratta i dati in qualità di responsabile del trattamento in caso di Data breach per dati particolarmente delicati si hanno 72 ore per fare la comunicazione al Garante e all'interessato.
Per la gestione di un eventuale data breach i documenti redatti sono:
1) procedura di allerta;
2) registro interno delle violazioni;
3) modello di comunicazione di data breach all'interessato;
4) modello di comunicazione di data breach al Garante per la Privacy.
Quando la struttura tratta i dati in qualità di responsabile del trattamento, in caso di data breach, essa informa senza ingiustificato ritardo il titolare del trattamento per cui tratta i dati e collabora con esso per quanto di sua competenza.

Dati del Titolare del Trattamento
EdiliziAcrobatica S.P.A.
S. legale: Via Turati 29 - 20121 Milano
S. op.: Viale Brigate Partigiane 18 -16129 Genova
P.IVA 01438360990 - N. Verde 800.300.833
E-mail: info@ediliziacrobatica.com

Dati del DPO
DPO Srls
Via Cantalupo 1/A 02100 Rieti
Tel- 0746/484287
PEC: dpo@arubapec.it
Referente: Sig. Giuseppe Langellotti