|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ***Valutazione dei rischi e misure di sicurezza tecniche e organizzative adeguate sulla protezione dei dati oggetto del trattamento*** | | | |
| Documento N.: | Data emissione: | Stato: | | Revisione: |
| GW\_IT.001 | 16/05/2019 |  | | Rev\_001 |
| Proprietario del Documento: | Redatto da: | | Approvato da: | |
| Gowen s.r.l. | Gowen s.r.l. | |  | |

**Valutazione dei rischi e misure di sicurezza tecniche e organizzative adeguate sulla protezione dei dati oggetto del trattamento**

[Art. 32 e ss. Reg. EU 679/2016]

* *adeguamento Regolamento EU 2016/679 -*

Sommario

[MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADEGUATE 3](#_Toc8913676)

[*1.* *designazioni e organigramma privacy* 3](#_Toc8913677)

[*2.* *trattamento con strumenti informatici o telematici* 4](#_Toc8913678)

[*2.1) Autenticazione informatica* 4](#_Toc8913679)

[*2.2) Aggiornamento periodico dell’ambito consentito, manutenzione e verifica periodica efficacia misure;* 4](#_Toc8913680)

[*2.3) Protezione degli strumenti elettronici e dei dati da trattamenti illeciti, da accessi non consentiti e da determinati programmi informatici* 5](#_Toc8913681)

[*2.5) Procedura di custodia e procedura di valutazione dell’efficacia delle misure di sicurezza* 9](#_Toc8913682)

[*2.6) Sicurezza degli impianti e dei luoghi ove avviene il trattamento dei dati* 10](#_Toc8913683)

[*2.7) Eventuali richieste dell’autorità giudiziaria di documentazione informatica* 11](#_Toc8913684)

[*3.* *trattamento senza strumenti elettronici* 11](#_Toc8913685)

[*3.1) Aggiornamento periodico dell’ambito consentito e verifica periodica efficacia misure* 12](#_Toc8913686)

[*3.2) Procedure di custodia e conservazione di atti e documenti e manutenzione e verifica periodica efficacia misure* 12](#_Toc8913687)

[*3.3) Sistema di autorizzazione, minimizzazione e di pseudonimizzazione* 13](#_Toc8913688)

[*3.4) Sicurezza degli impianti e dei luoghi del trattamento dei dati* 13](#_Toc8913689)

[*3.5) Eventuali richieste dell’autorità giudiziaria di documentazione cartacea* 14](#_Toc8913690)

[*4.* *procedura in caso di violazione dei dati personali – Incident responce plan (IRP)* 14](#_Toc8913691)

[*5.* *procedura di riscontro alle richieste di esercizio dei diritti dell’interessato* 16](#_Toc8913692)

[*6.* *revisione delle misure di sicurezza tecniche e organizzative adeguate, audit di controllo e monitoraggio, aggiornamento e formazione.* 17](#_Toc8913693)

[Storico del Documento 18](#_Toc8913694)

La Società **Gowen S.r.l.** con sede in Roma (RM) 00135 Via Salomone Morpurgo n. 8 – p.iva e c.f. 03563891005 (d’ora in avanti anche “la Società”), con il presente documento e quale titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché́ della natura, dell'oggetto, del contesto e delle finalità̀ del trattamento, come anche del rischio di varia probabilità̀ e gravità per i diritti e le libertà delle persone fisiche, procede alla valutazione dei rischi e mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

La valutazione dei rischi e le misure di sicurezza di cui al presente documento interessano il trattamento dei seguenti dati:

* dati relativi ai clienti;
* dati relativi ai fornitori;
* dati relativi ai dipendenti, collaboratori, consulenti e professionisti
* dati utenti.

A seguito di detta valutazione sono state individuate le seguenti misure e procedure che rappresentano una garanzia di sicurezza adeguata secondo le disposizioni del Regolamento UE 2016/679 contro i rischi di distruzione, perdita, indisponibilità̀, modifica, divulgazione e accesso non autorizzati, accesso in modo accidentale o illegale a dati personali trasmessi, conservati o comunque trattati che vengono pertanto attuate con la firma del presente atto.

\*\*\*

# **MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADEGUATE**

*[art. 33]*

Le misure di sicurezza sono adottate e previste, con riferimento ai sopra indicati trattamenti, per limitare al minimo i rischi di:

* divulgazione e accesso non autorizzati
* accesso in modo accidentale o illegale a dati personali trasmessi
* distruzione
* modifica
* perdita
* indisponibilità̀

1. ***designazioni e organigramma privacy***

L’organigramma dei ruoli nella Società per il trattamento dei dati mediante strumenti informatici, telematici e materiali /cartacei è il seguente: v. allegato.

I contatti relativi agli ulteriori responsabili esterni del trattamento dei dati (es. dati sanitari, medico; es. dati dei dipendenti, commercialista, ecc.), possono essere richiesti da parte dei soggetti interessati o ulteriori soggetti aventi titolo mediante comunicazione al titolare del trattamento ovvero al DPO ovvero ancora al referente privacy competente. L’organigramma completo e comprensivo dei soggetti autorizzati è allegato alle presenti misure di sicurezza (all. **A**).

1. ***trattamento con strumenti informatici o telematici***

La Società svolge le attività relative al proprio business per il tramite di strumenti informatici, telematici e cartacei. Pertanto, attraverso tali documenti e per mezzo l’archiviazione informatica degli stessi, avviene parte del trattamento dei dati personali.

### *2.1) Autenticazione informatica*

* I soggetti che possono effettuare il trattamento mediante strumenti informatici sono precipuamente autorizzati mediante nomina disposta nelle forme richieste dal Regolamento EU 679/2016.
* Solo i soggetti di cui sopra sono dotati di credenziali di autenticazione costituite da un codice per l'identificazione a una parola chiave riservata conosciuta solamente dal medesimo (user id - password).
* È vietata la divulgazione o lo scambio di credenziali ad altri soggetti, dipendenti, collaboratori, agenti, professionisti o qualsiasi altra persona anche se esclusivamente per esigenze operative.
* Il soggetto autorizzato all’accesso deve custodire diligentemente le proprie credenziali di autenticazione in modo da garantire l’uso esclusivo dei dispositivi in possesso.
* Le modalità di gestione delle password, la loro composizione e le prescrizioni relative al cambio password sono previste dalla password policy implementata dalla Società (v. **all. 1**).

### *2.2) Aggiornamento periodico dell’ambito consentito, manutenzione e verifica periodica efficacia misure;*

* Sono impartite istruzioni scritte ai soggetti eventualmente autorizzati in merito al trattamento, alla custodia e controllo dei file contenenti dati personali, per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento (raccolta, immissione, consultazione, utilizzo, trasmissione, distruzione e conservazione dei dati).
* I referenti privacy – ciascuno per le proprie attribuzioni – devono aggiornare l’individuazione dell’ambito del trattamento consentito ai singoli soggetti (v. punto 2.6), ivi compresi eventuali consulenti/legali precipuamente nominati ai fini di tutela degli interessi della Società.
* Periodicamente e per lo meno ogni 3 mesi il Titolare, coadiuvato dai referenti privacy, verifica la sussistenza di efficacia delle presenti misure di sicurezza, in particolare cura l’aggiornamento del firewall – o ne segnala la necessità al responsabile esterno ove di competenza.
* I referenti privacy – ciascuno per le proprie attribuzioni – si impegnano ad installare tutti gli aggiornamenti di sicurezza e di routine nei tempi tecnici opportuni. Inoltre, con frequenza trimestrale, verificano i dati presenti sul file log del firewall indicativi di eventuali insidie o rischi.
* I referenti privacy – ciascuno per le proprie attribuzioni – verificano periodicamente e comunque almeno ogni 3 mesi la necessità di eventuali aggiornamenti de sistema nel suo complesso.

### *2.3) Protezione degli strumenti elettronici e dei dati da trattamenti illeciti, da accessi non consentiti e da determinati programmi informatici*

Schematicamente e con riferimento proprio alla struttura informatica e tecnica della Società, di seguito i principali elementi descrittivi del sistema di trattamento mediante strumenti informatici e telematici:

* sede della società sita in Via Salomone Morpurgo n. 8 - Roma
* è presente una rete internet e aziendale interna accessibile mediante credenziali di accesso fornite ai soli dipendenti e autorizzati;
* è predisposta una rete “guest” per l’accesso alla rete internet da parte di soggetti esterni ovvero non autorizzati che consente l’accesso alla rete internet ma non anche alla rete aziendale interna;
* è presente un firewall perimetrale UTM (Unfied Threat Management) Zyxel USG60W con attivi i seguenti servizi:
* ANTIVIRUS (BIT DEFENDER): Il servizio Anti-Virus di Zyxel è una tecnologia anti-virus a livello gateway che prende di mira malware noti tra cui virus, trojan, worm, spyware e spyware, Zyxel Anti-Virus esegue la scansione del traffico sui principali protocolli inclusi HTTP, HTTPS, FTP, SMTP e POP3;
* CONTENT FILTERING (CYREN): Content Filtering di ZyXEL, al fine di protegge le reti da attacchi malevoli provenienti da siti Web non autorizzati;
* IDP (TREND MICRO): Protegge la tua attività da una vasta gamma di attacchi e attività sospette, come SQL injection, DoS e applicazioni backdoor dannose;
* APPLICATION PATROL (TREND MICRO): accelera e blocca le applicazioni per aumentare la produttività e prevenire l'abuso della banda larga.
* i singoli computer sono dotati di firewall e antivirus Avast;
* quanto al sistema di backup:
  + è presente n. 1 HD della Trekstor da 2 TB, tutti i giorni esegue il backup incrementale (la notte).
  + è presente n. 1 NAS con 2 HD interni (ognuno da 4 TB), modello MyCloudPR2100, connesso alla rete aziendale sul quale anch’esso viene eseguito il backup incrementale tutti i giorni (la notte). Tale dispositivo NAS è nascosto sopra il controsoffitto della sala server.
  + Tutti i venerdì sera (la procedura dura circa 24 h) viene eseguito un backup incrementale su Microsoft One Drive (il cloud di Office 365), e i dati sono presenti pertanto anche su Cloud online al fine di limitare il rischio di perdita dati in caso di danni hard disk in ufficio;
* a cura del referente privacy IT, sono effettuati, oltre agli aggiornamenti automatici, periodici aggiornamenti del Server e ai computer;
* Posizionamento computer e stampanti
  + n. 9 computer nell’area ufficio;
  + n. 1 stampante multifunzione, n. 5 stampanti di rete e n. 1 plotter per stampe su grandi formati;
* a cura del responsabile del trattamento esterno (tecnico informatico) ovvero del referente privacy competente, sono effettuati, oltre agli aggiornamenti automatici, aggiornamenti periodici dei sistemi informatici e telematici in uso presso la società;
* informazioni generali concernenti l’utilizzo dei sistemi informatici, telematici e di rete
* i computer presenti in sede sono connessi al server mediante credenziali di accesso;
* l’accesso ai singoli computer in dotazione è possibile solo tramite autenticazione mediante credenziali;
* ogni dipendente è dotato di proprie credenziali per l’accesso; la custodia delle credenziali è affidata al responsabile del trattamento;
* l’accesso al gestionale ITALSOFT è effettuabile previa autenticazione mediante credenziali di accesso;
* ogni dipendente è dotato di proprie credenziali per l’accesso al gestionale ITALSOFT la custodia delle credenziali è affidata al referente privacy competente e/o al responsabile del trattamento esterno;
* tutti i dipendenti sono dotati di mail aziendale, gestita attraverso apposito pannello di gestione mail, tutte le password relative agli accessi informatici e telematici mediante credenziali sono gestite, quanto alla policy di cambio password, dalla *Password Policy* implementata dalla Società (v. **all. 1**);
* le cartelle situate nel computer/server, dunque direttamente accessibili dai dipendenti, sono state oggetto di revisione e riorganizzazione. Pertanto, sono previsti accessi limitati e autorizzazioni singole o per area/ufficio alle cartelle. È predisposto ed aggiornato un registro, in formato informatico ovvero cartaceo, delle autorizzazioni di accesso alle cartelle.
* i sistemi antivirus adottati si aggiornano automaticamente anche più volte al giorno al fine di proteggere i dati personali contro il rischio di intrusione e dell’azione di programmi pericolosi di cui all’art. 615-quinquies c.p. (... programma informatico... avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento...);
* i sistemi Windows utilizzati per il trattamento dei dati si aggiornano automaticamente seguendo i calendari di update generati da Microsoft, programmi gestionali al fine di prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti (c.d. patch di sicurezza).
* Particolari cautele sono predisposte sui computer aziendali utilizzati per l’accesso al sistema, tra le quali: gli utenti non devono aprire links o file zip, doc o excel, né, in generale, scaricare su disco allegati di messaggi di posta elettronica di cui non conoscono la provenienza.
* I soggetti autorizzati prima di aprire i messaggi di posta elettronica devono controllare che l’indirizzo mail del mittente sia attendibile.
* I soggetti autorizzati non devono aprire messaggi di posta elettronica provenienti da mittenti non riferibili al lavoro né aprire i messaggi di posta elettronica indicati come spam anche se provengono da mittenti conosciuti; gli utenti non devono aprire mail provenienti da istituti bancari, enti quali ad esempio Agenzia Entrate o similari o da società che normalmente inviano pec e non mail; gli utenti non devono collegarsi a siti web non affidabili.
* L’accesso alla mail aziendale su dispositivi diversi dal computer o dagli strumenti informatici in dotazione è possibile solo se tali dispositivi (es. cellulari e tablet) sono anch’essi resi in dotazione al singolo autorizzato da parte della Società. Per l’utilizzazione di dispositivi diversi, non di proprietà della società, il soggetto deve essere autorizzato dal Titolare o dal referente privacy competente.
* Al fine di evitare accessi non autorizzati e trattamenti non consentiti, gli eventuali supporti rimovibili (cd-rom, chiavette usb, hard disk esterni ecc.) devono essere custoditi in luoghi sicuri e chiusi a chiave.
* i supporti rimovibili (cd-rom, chiavette usb, hard disk esterni ecc.) in uso dagli autorizzati al fine di esecuzione del servizio svolto dalla società possono contenere solamente file o dati a tal fine necessario; è fatto divieto di uso dei predetti dispositivi per diverse finalità.
* i dispositivi di cui sopra, in ogni caso, non possono essere portati al di fuori della sede di lavoro.
* In caso di prolungata assenza o impedimento dell’autorizzato custode dei supporti di cui al punto che precede, i Referenti privacy – ciascuno per le proprie attribuzioni – tengono una copia della chiave del luogo o vi si trovano i supporti rimovibili di cui sopra. Ancora, in caso di necessità urgente e non differibile i Referenti privacy – ciascuno per le proprie attribuzioni – potranno prelevare e utilizzare i suddetti supporti ma solamente per indispensabili ed indifferibili necessità operative o per necessità di intervento e di sicurezza del sistema.

*2.4) Utilizzazione di un sistema di autorizzazione, minimizzazione e di pseudonimizzazione*

* I referenti privacy – ciascuno per le proprie attribuzioni – devono assicurarsi che le password utilizzate da ciascun soggetto limitino l’accesso ai soli dati per i quali lo stesso è stato autorizzato al trattamento.
* Sono individuati e configurati i profili di autorizzazione per ogni soggetto o per classi omogenee di soggetti anteriormente all’inizio del trattamento in modo da limitare l’accesso ai soli dati necessari per le operazioni di trattamento autorizzate e per limitare l’utilizzo di eventuali dispositivi mobili.
* I referenti privacy – ciascuno per le proprie attribuzioni – devono verificare periodicamente, e comunque almeno ogni mese, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, cioè che siano ancora attuali e che sia corretto l’abbinamento con i soggetti autorizzati.
* I referenti privacy – ciascuno per le proprie attribuzioni – si assicurano che i dati personali soggetti a trattamento siano trattati soltanto da i soggetti precipuamente autorizzati con specifico atto di nomina munito delle prescrizioni di condotta.

### *2.5) Procedura di custodia e procedura di valutazione dell’efficacia delle misure di sicurezza*

* Sono indicati per iscritto nella nomina a soggetti autorizzato i dati ai quali possono accedere.
* L’accesso agli archivi informatici o comunque ai file contenenti dati particolari o giudiziari è consentito solo al Titolare ovvero ai referenti privacy.
* Il sistema informatico è strutturato in modo da limitare l’accesso a singole cartelle a soggetti privi di autorizzazione e, invece, permettere l’accesso ai soli autorizzati. Tali diversificazioni sono strutturate sia limitando o permettendo l’accesso a singoli soggetti ovvero limitando / permettendo l’accesso a gruppi di soggetti suddivisi per area / ufficio (v. anche 2.6).
* I referenti privacy – ciascuno per le proprie attribuzioni – devono aggiornare l’individuazione dell’ambito del trattamento consentito ai singoli soggetti o gruppi di soggetti ivi compresi eventuali consulenti/legali precipuamente nominati ai fini di tutela degli interessi della Società.
* la Società applica una *Record Retention Policy* (v. all. **2**) per la gestione della conservazione e la successiva cancellazione dei dati;

Tale policy prevede limiti di conservazione – spirati i quali il documento è soggetto a eliminazione / distruzione – diversificati a seconda della tipologia di documento e dunque dei dati presenti all’interno del documento stesso prevedendo una ripartizione così suddivisa: documenti conservabili fino 30 giorni; documenti conservabili da 30 giorni fino ad un massimo di 12 mesi; documenti conservabili da 1 a 5 anni; documenti conservabili fino a 10 anni; documenti conservabili senza previsione di un termine definito.

* i dati degli utenti del sito nonché degli utenti richiedenti informazioni commerciali ovvero operative a mezzo del form presente sul medesimo sito (http://www.gowen.it/contatta-gowen-srl.html), saranno conservati, commisurando il grado di indispensabilità, per il solo tempo necessario a raggiungere lo scopo dell’attività in oggetto e dunque per il tempo necessario a gestire la richiesta dell’utente e a fornire il relativo riscontro. In ogni caso, i dati degli utenti non vengono conservati dalla società per un periodo superiore a 365 giorni.
* I referenti privacy – ciascuno per le proprie attribuzioni – verificano periodicamente e comunque almeno ogni 3 mesi la corretta implementazione delle procedure di custodia dei dati informatici e se necessario propone la revisione degli standard adottati.

### *2.6) Sicurezza degli impianti e dei luoghi ove avviene il trattamento dei dati*

* Le sedi della Società sono dotate di allarme collegato a cerniere magnetiche installate sulle porte di ingresso nonché connesso a sensori di movimento. Il sistema avvisa il Titolare ovvero altri soggetti specificatamente indicati dallo stesso Titolare mediante sms eventuali rilevazioni anomale.
* Si accede alla sede della società disattivando l’allarme e mediante chiavi fisiche per le serrature di ingresso. Ogni soggetto autorizzato è dotato delle chiavi di accesso alla sede;
* Il Titolare, coadiuvato dal referente privacy e dal responsabile della sicurezza dei luoghi di lavoro, verifica periodicamente e comunque almeno ogni 3 mesi il corretto funzionamento, degli impianti e delle tecnologie preposte alla sicurezza dei dati quali gruppi di continuità, impianto antincendio e allarme.

### *2.7) Eventuali richieste dell’autorità giudiziaria di documentazione informatica*

* Nel caso di richieste investigative dell’autorità giudiziaria o di polizia giudiziaria ovvero di tutela dei beni della Società, i Referenti privacy – ciascuno per le proprie attribuzioni – ovvero il Titolare del Trattamento, dispongono l’estrazione della documentazione informatica richiesta contenente dati personali su di un supporto esterno criptato custodito in cassetta di sicurezza chiusa a chiave in attesa di consegna dei file all’autorità richiedente.
* Avvenuta la trasmissione, i Referenti privacy – ciascuno per le proprie attribuzioni – ovvero il Titolare del Trattamento, dispongono precise misure (dunque da valutarsi caso per caso) relativamente alla necessità di conservazione o archiviazione dei file oggetto di trasferimento.
* Al termine delle necessità previste, nel caso in cui non vi sia necessità di conservazione o archiviazione, i referenti privacy – ciascuno per le proprie attribuzioni – devono provvedere a eliminare o rendere inutilizzabili i file sui quali sono presenti i dati trattati alla fine del trattamento in modo da impedire la dispersione degli stessi e l’accesso a soggetti non autorizzati.

1. ***trattamento senza strumenti elettronici***

La Società svolge le attività relative al proprio business anche per il tramite di documenti cartacei. Pertanto, attraverso tali documenti cartacei e per mezzo l’archiviazione cartacea degli stessi, avviene parte del trattamento dei dati personali.

### *3.1) Aggiornamento periodico dell’ambito consentito e verifica periodica efficacia misure*

* Sono impartite istruzioni scritte ai soggetti eventualmente autorizzati in merito alla custodia e controllo dei documenti con dati personali, per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento (raccolta, immissione, consultazione, utilizzo, trasmissione, distruzione e conservazione dei dati).
* Il referente privacy deve aggiornare l’individuazione dell’ambito del trattamento consentito ai singoli soggetti (ulteriori Responsabili o autorizzati), ivi compresi eventuali consulenti/legali precipuamente nominati ai fini di tutela degli interessi della Società.
* Il referente privacy operativo verifica periodicamente e comunque almeno ogni 3 mesi la corretta implementazione delle procedure di custodia dei dati cartacei e se necessario propone la revisione degli standard adottati.

### *3.2) Procedure di custodia e conservazione di atti e documenti e manutenzione e verifica periodica efficacia misure*

* Sono indicati per iscritto nell’incarico ai soggetti eventualmente autorizzati i dati conservati su supporto cartaceo ai quali possono accedere.
* Nell’ufficio amministrativo sono presenti tre armadi i quali contengono rispettivamente:
  + archivio fatture dei fornitori divise in base all’oggetto della fornitura;
  + archivio delle fatture dell’anno precedente a quello in corso;
  + archivio cartaceo dei documenti della società (bilanci, verbali di assemblea, statuti, atti costitutivi, polizze assicurative, ecc.)
* Nell’ufficio tecnico sono presenti tre armadi i quali contengono rispettivamente:
  + archivio e gestione documentale delle commesse dal contratto al verbale di collaudo comprese le fatture inerenti alla commessa stessa;
  + archivio e gestione di documentazione di bandi di gara in attesa di aggiudicazione e offerte in attesa di eventuali incarichi;
  + archivio di brochure di fornitori per analisi prezzi
* Nel magazzino sono presenti documenti cartacei relativi alle commesse degli anni precedenti al 2014.
* L’accesso agli archivi contenenti dati dei dipendenti ovvero ancora dati particolari o giudiziari è consentito solo al Titolare ovvero alle persone autorizzate attraverso specifica autorizzazione scritta da parte del titolare del trattamento contenuta nell’incarico.
* Gli armadi e i cassetti dove sono custoditi i dati laddove possibile sono chiusi a chiave dal Titolare (e la relativa chiave è dallo stesso custodita) ovvero in alternativa sono allocati in armadi tenuti da soggetti autorizzati.
* I dati particolari e i dati giudiziari ai sensi degli artt. 9-10 del Regolamento UE 2016/679 devono essere presenti in armadi o contenitori chiusi a chiave e separati da quelli contenenti i dati comuni.
* I documenti contenenti dati personali particolari o giudiziari affidati ai soggetti a cui è consentito l’accesso per lo svolgimento dei relativi compiti, devono essere controllati e custoditi dai medesimi soggetti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
* la Società applica una *Record Retention Policy* (v. all. **2**) per la gestione della conservazione e la successiva cancellazione dei dati;

Tale policy prevede limiti di conservazione – spirati i quali il documento è soggetto a eliminazione / distruzione – diversificati a seconda della tipologia di documento e dunque dei dati presenti all’interno del documento stesso prevedendo una ripartizione così suddivisa: documenti conservabili fino 30 giorni; documenti conservabili da 30 giorni fino ad un massimo di 12 mesi; documenti conservabili da 1 a 5 anni; documenti conservabili fino a 10 anni; documenti conservabili senza previsione di un termine definito.

* la documentazione inerente a rapporti contrattuali o negoziali non più in essere e dei quali non è possibile procedere alla cancellazione / distruzione in quanto la loro conservazione è necessaria ai fini aziendali ed in particolare per finalità fiscali, tributarie o finanziarie ovvero per legittimo interesse della società ovvero ancora relative ad obblighi di legge è oggetto di conservazione separata a cura del Titolare.
* il Libro Unico del Lavoro presente nei cantieri ove opera la società deve essere conservato in luogo protetto e sicuro.
* i soggetti autorizzati al trattamento del Libro Unico del Lavoro sono informati dal Titolare o dal referente privacy in merito alle misure di sicurezza da adottare e attuare.
* Il Titolare e il referente privacy verificano periodicamente e comunque almeno ogni 3 mesi la corretta implementazione delle procedure di custodia dei dati cartacei e se necessario propone la revisione degli standard adottati.

### *3.3) Sistema di autorizzazione, minimizzazione e di pseudonimizzazione*

* Il referente privacy competente si assicura che i dati personali soggetti a trattamento siano trattati soltanto da i soggetti precipuamente autorizzati con specifico atto di nomina munito delle prescrizioni di condotta.
* Sono individuati profili di autorizzazione per ogni soggetto o per classi omogenee di soggetti anteriormente all’inizio del trattamento in modo da limitare l’accesso ai soli dati necessari per le operazioni di trattamento autorizzate.
* Il referente privacy competente deve verificare periodicamente, e comunque almeno ogni 3 mesi, la sussistenza delle autorizzazioni, cioè che siano ancora attuali e che sia corretto l’abbinamento con i soggetti autorizzati.
* I fascicoli e i faldoni non intestati a società sono pseudonimizzati e pertanto dalla copertina esterna non è possibile evincere i dati di intestazione degli stessi.
* Il referente privacy competente si assicura che tale prescrizione sia adottata e che gli identificativi degli interessati siano conservati separatamente e adeguatamente protetti.

### *3.4) Sicurezza degli impianti e dei luoghi del trattamento dei dati*

* Le sedi della Società sono dotate di allarme collegato a cerniere magnetiche installate sulle porte di ingresso nonché connesso a sensori di movimento. Il sistema avvisa il Titolare ovvero altri soggetti specificatamente indicati dallo stesso Titolare mediante sms eventuali rilevazioni anomale.
* Si accede alla sede della società disattivando l’allarme e mediante chiavi fisiche per le serrature di ingresso. Ogni soggetto autorizzato è dotato delle chiavi di accesso alla sede;
* Il Titolare, coadiuvato dal referente privacy e dal responsabile della sicurezza dei luoghi di lavoro, verifica periodicamente e comunque almeno ogni 3 mesi il corretto funzionamento, degli impianti e delle tecnologie preposte alla sicurezza dei dati quali gruppi di continuità, impianto antincendio e allarme.

### *3.5) Eventuali richieste dell’autorità giudiziaria di documentazione cartacea*

* Nel caso di richieste investigative dell’autorità giudiziaria o di polizia giudiziaria ovvero di tutela dei beni della Società, i Referenti privacy – ciascuno per le proprie attribuzioni – ovvero il Titolare del Trattamento, dispongono l’estrazione della documentazione cartacea richiesta contenente dati personali su di un supporto esterno custodito in cassetta di sicurezza chiusa a chiave in attesa di consegna dei file all’autorità richiedente.
* Avvenuta la trasmissione, i Referenti privacy – ciascuno per le proprie attribuzioni – ovvero il Titolare del Trattamento, dispongono precise misure (dunque da valutarsi caso per caso) relativamente alla necessità di conservazione o archiviazione dei documenti oggetto di trasferimento.
* Al termine delle necessità previste, nel caso in cui non vi sia necessità di ulteriore conservazione o archiviazione, il referente privacy competente provvede a distruggere o rendere inutilizzabili i supporti cartacei sui quali sono presenti i dati trattati alla fine del trattamento in modo da impedire la dispersione degli stessi e l’accesso a soggetti non autorizzati.

1. ***procedura in caso di violazione dei dati personali – Incident responce plan (IRP)***

*[art. 33 e ss. Reg. EU 679/2016]*

Il Regolamento UE 2016/679 (RGPD) prevede che in caso di violazione dei dati personali, il Titolare del trattamento deve mettere in atto tutte le misure organizzative e tecniche per salvaguardare i dati personali e notificare tale violazione al Garante per la protezione dei dati personali, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare la violazione anche agli interessati senza ingiustificato ritardo.

Per violazione della sicurezza (*data breach*) si intende la distruzione accidentale o illecita, la perdita, l’alterazione, la divulgazione o l’accesso non autorizzato ai dati personali trattati dal Titolare. In sintesi, le violazioni in oggetto possono essere classificate in base ai seguenti tre ben noti principi di sicurezza delle informazioni in:

* “Confidentiality Breach”: divulgazione non autorizzata o accidentale di dati personali [es. furto o smarrimento di strumenti informatici (computer, cellulari, tablet, ecc.); furto o smarrimento di documenti cartacei contenenti dati personali; invio a mezzo mail di dati personali a soggetti non autorizzati alla ricezione; sospetto accesso informatico non autorizzato (hacking)];
* “Integrity Breach”: alterazione o modifica accidentale o non autorizzata di dati personali;
* “Availability Breach”: perdita non autorizzata o accidentale dell’accesso ai dati personali o quale distruzione/eliminazione/cancellazione dei dati personali [es. eliminazione di dati accidentale o effettuata da soggetti non autorizzati; in assenza di backup o impossibilità recupero, smarrimento/perdita di chi chiavi per la decriptazione di file o documenti];

Possono essere indice di una violazione dei dati personali:

- il furto, lo smarrimento, il malfunzionamento o un comportamento anomalo dei dispositivi hardware o software utilizzati nell’attività di lavoro (p.es. computer fisso o portatile, tablet, smartphone, pennetta usb, CD, software gestionali, ecc.);

- la perdita o la sottrazione delle credenziali utilizzate per l’accesso ai dispositivi hardware o software (user id, password, pin, ecc.);

- la perdita, la cancellazione o il danneggiamento anche accidentale di file informatici, email o di documenti contenenti dati;

- la perdita, la sottrazione, il danneggiamento o il malfunzionamento delle chiavi fisiche o delle serrature per l’accesso agli archivi cartacei;

- l’invio di una e-mail o di un allegato o comunque l’invio di una comunicazione, di un file o di un documento a un soggetto diverso dal destinatario originario o in una modalità o forma diversa da quella prevista.

La società ha adottato una procedura di gestione delle violazioni dei dati personali in ottemperanza alle previsioni normative del GDPR.

A tal proposito, si rinvia integralmente al documento “*Incident responce plan” (IRP)* adottato (v. **all. 3**).

1. ***procedura di riscontro alle richieste di esercizio dei diritti dell’interessato***

Il Regolamento UE 2016/679 (GDPR) attribuisce all’interessato, ossia la persona fisica alla quale si riferiscono i dati personali trattati, determinati diritti da esercitare nei confronti della Società, quale Titolare del trattamento, fra cui il diritto di accesso ai propri dati personali, l’aggiornamento, l’integrazione, la cancellazione, la trasformazione dei dati e il blocco del trattamento (artt. 15 – 22).

Il Regolamento UE in oggetto stabilisce che il Titolare deve agevolare l’esercizio dei suddetti diritti dell’interessato e darvi riscontro senza “ingiustificato ritardo” e, comunque, al più tardi entro un mese dal ricevimento della richiesta, salvo proroga di due mesi per la complessità e il numero delle richieste.

A tal proposito, la Società, in ottemperanza alle previsioni normative del GDPR, ha predisposto e adottato la procedura di *Subject Access Request* a cui si rinvia integralmente (v. **all. 4**) con le azioni e le misure da intraprendere da parte del personale al fine di fornire riscontro alle richieste degli interessati in modo tempestivo e conforme alle disposizioni della normativa sulla protezione dei dati personali.

Tale procedura indica soggetti, tempi e modalità individuate dalla Società per ottemperare alle previsioni normative del GDPR. Sinteticamente:

* 1. ricevere, monitorare e gestire le richieste dell’interessato al trattamento dei dati personali, secondo le istruzioni indicate nella procedura (*v. fase 1 SAR*);
  2. procedere all’istruttoria della richiesta per individuare e gestire i dati personali, gli uffici e le aree interne della Società coinvolti nella richiesta e gli eventuali responsabili del trattamento a cui i dati sono affidati ed informare la Società in merito alla richiesta dell’interessato ed a tutte le informazioni e verifiche effettuate e richiedere le misure da adottare (*v. fase 2 SAR*);
  3. fornire il necessario ausilio alla Società per determinare le azioni e le misure da intraprendere per fornire il riscontro tempestivo alla richiesta dell’interessato e verificare eventuali elementi di non legittimità della richiesta (*v. fase 3 SAR*);
  4. coordinare e verificare l’adozione delle misure tecniche e organizzative stabilite dalla Società interpellando il Responsabile IT e i responsabili degli uffici e delle aree coinvolti e gli eventuali responsabili esterni del trattamento (*v. fase 4 SAR*);
  5. procedere alla redazione della bozza di comunicazione di riscontro da fornire all’interessato (accoglimento, rigetto o proroga) da sottoporre alla Società e registrarne la prova dell’invio (*v. fase 5 SAR*);
  6. provvedere alla compilazione del registro dei diritti degli interessati inserendo le informazioni sulla richiesta ricevuta, l’attività svolta e il riscontro, positivo o negativo, fornito all’interessato (*v. fase 6 SAR*).

Inoltre, al fine di salvaguardare le richieste degli interessati e garantire un efficiente e tempestivo riscontro, il Titolare ovvero il referente privacy competente, dovranno verificare che i canali di comunicazione della Società verso l’esterno siano funzionanti ed efficienti e che il personale autorizzato e incaricato alla gestione e ricezione delle comunicazioni dall’esterno sia a conoscenza e abbia ricevuto le necessarie istruzioni per gestire la ricezione delle richieste degli interessati.

1. ***revisione delle misure di sicurezza tecniche e organizzative adeguate, audit di controllo e monitoraggio, aggiornamento e formazione.***

Come evincibile dai paragrafi che precedono, la società prevede un monitoraggio costante delle misure di sicurezza implementate e dei protocolli adottati. Ciò avviene anche per il tramite di specifiche indicazioni demandate mediante nomina specifica ai referenti privacy.

Tali controlli e monitoraggi sono previsti, per alcuni ambiti, con cadenza trimestrale.

Inoltre, la società prevede un audit di controllo e monitoraggio dell’intero sistema di protezione dei dati personali scadenzato ad intervalli semestrali.

Gli autorizzati e i referenti sono formati in ordine ad elementi base della normativa in materia di protezione dei dati personali oltre che in ordine alle misure e alle policies adottate dalla società.

Al termine dell’audit di controllo semestrale, alla luce delle risultanze, effettuate le eventuali modifiche alle misure di sicurezza organizzative e tecniche e, ancora eventualmente, proceduto a nuova valutazione di impatto, si procede a nuovo aggiornamento e formazione degli autorizzati e dei referenti privacy.

\*\*\*

In allegato:

1. *Organigramma privacy*
   1. *Password policy;*
   2. *Record Retention Policy (RRP);*
   3. *Incident responce plan* (*IRP*);
   4. *Subject access reques* (*SAR*);

Roma, \_\_/\_\_\_/2019 Il Titolare del trattamento

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*\*\*

## **Storico del Documento**

|  |  |  |  |
| --- | --- | --- | --- |
| **Creato da** | **Data** | **Approvato da:** | **Data** |
| Gowen s.r.l. | 16/05/2019 |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rev.** | **Modificato da** | **Data** | **Approvato da:** | **Data** |
| 01 |  |  |  |  |
| 02 |  |  |  |  |
| 03 |  |  |  |  |