ALCHIMIA
TOSCANA

DOCUMENTO DI CONFORMITA'
DELLE MISURE ADOTTATE DALL'AZIENDA
"ECO.REC SRL"
PER LA TUTELA DEI DATI PERSONALI AL GDPR
Regolamento generale sulla protezione dei dati
(UE/2016/679)

PREMESSA

Il presente **Documento di conformità, delle misure di sicurezza adottate a tutela dei dati personali, alla disciplina privacy vigente, Regolamento UE/2016/679**, ha lo scopo di descrivere il piano di sicurezza adottato dall'azienda **ECO.REC SRL** al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati trattati nell'esercizio della propria attività. Esso svolge la funzione di "fotografare" in modo accurato la situazione dell'azienda rispetto all'adeguamento alla normativa in essere, fornendo prova scritta delle misure adottate.

La modulistica/gli allegati sono presenti al termine del testo. Per quanto fatto in passato in osservanza del Decreto legislativo 196/2003, Codice Privacy, si rimanda alla documentazione interna emessa in precedenza e conservata dall'azienda.

Il presente documento di conformità sarà aggiornato e perfezionato nel suo complesso, in base all'esperienza acquisita ed al progresso tecnico. In questa fase di applicazione della normativa europea, si evidenzia l'incertezza dovuta al **decreto legislativo di armonizzazione dell'ordinamento italiano al Regolamento Ue 2016/679** e la possibilità che siano necessari interventi ravvicinati rispetto a questa emissione.

Il Documento di conformità in versione elettronica e/o cartacea sarà custodito presso la sede, sarà consultabile da coloro ai quali la direzione accorderà l'accesso e costituirà documento di riferimento in caso di controlli.

METODO ANALISI

Al fine di tenere sotto controllo i processi legati alla sicurezza, integrità e disponibilità delle informazioni si è adottato un sistema di gestione basato sulla definizione di ruoli, responsabilità, procedure formali, analisi dei rischi e formazione del personale.
La metodologia seguita nell'elaborazione del presente documento ha portato a graduare le misure di sicurezza poste/da porre in essere e a seguire un percorso così articolato:

1. identificazione, censimento e valutazione dei beni e delle risorse da proteggere;
2. identificazione delle aree e delle criticità aziendali;
3. analisi delle minacce e dei rischi e loro gestione;
4. analisi della situazione iniziale in termini di politiche di sicurezza fisica, logica ed organizzativa;
5. piano operativo;
6. programmazione verifiche e implementazione delle soluzioni adottate.

Al fine di rendere snello e agevolmente consultabile/fruibile il documento si è rimandato al suo interno a:

DOCUMENTI GIÀ PRESENTI IN AZIENDA

Esempi: si è richiamato l'organigramma già presente richiamando il file di riferimento; si è fatto riferimento a regolamenti aziendali già emanati o a procedure già previste per la gestione del sistema qualità…
Si è richiamata infine l'eventuale documentazione privacy pregressa, conservata in un apposito raccoglitore aziendale e comprendente anche il DPS (come richiesto in passato).

MODULISTICA

Si tratto di modulistica interna gestita in modo separato rispetto al testo del documento principale. Ad esempio: informativa resa al personale, clausole contrattuali privacy, vademecum per il personale per il corretto trattamento dei dati, procedure.

IDENTIFICAZIONE, CENSIMENTO E VALUTAZIONE ASSET DA PROTEGGERE

Prima di descrivere i beni e le risorse da proteggere, intesi in termini di patrimonio informativo, infrastrutture, strutture aziendali e risorse professionali, è opportuno descrivere le modalità con cui la Società esercita la sua attività.
La società ha provveduto a censire e proteggere le proprie risorse interne ed esterne, intese in termini di patrimonio informativo, infrastrutture, strutture aziendali e risorse professionali.

Trattamenti dati

L'individuazione delle banche dati in trattamento ha lo scopo di dettagliare e raccogliere in categorie omogenee le informazioni trattate dall'azienda, provvedendo contemporaneamente ad una valutazione dell'importanza dei vari asset. La valutazione dell'importanza è particolarmente utile poiché permette di marginalizzare le informazioni "*di poco valore*" e di focalizzare l'attenzione e l'impiego delle risorse sulle aree critiche e su ciò che riveste reale importanza per la società.
La procedura di censimento si applica all'intero sistema aziendale, distinto però in uffici, sia per i trattamenti cartacei che elettronici. Attualmente i dati trattati dall'azienda vengono comunicati ai soggetti interni ed esterni censiti.

Infrastrutture, strutture, risorse tecniche

La descrizione delle infrastrutture delle strutture e delle risorse tecniche ha lo scopo di raccogliere informazioni sulle aree ed i locali dove il trattamento avviene, sulle macchine ed i programmi utilizzati. Il tutto al fine di valutare lo stato della sicurezza e le minacce ed i rischi contro i quali approntare/incrementare/alleggerire i sistemi di protezione.
La procedura di censimento si applica all'intero sistema aziendale.

Risorse professionali

La descrizione delle risorse professionali ha lo scopo di raccogliere informazioni su professionalità, ruoli e responsabilità relativi alla gestione aziendale. Per risorse professionali s'intendono coloro che eseguono un qualsiasi trattamento dati, siano essi la direzione aziendale, il personale dipendente, amministrativo e non, coloro che si occupano della manutenzione dei computer e del software, i consulenti ecc. La procedura si applica all'intero sistema aziendale e a tutte le professionalità (dipendenti, collaboratori, eventuali stagisti ecc.). Per trattamento s'intende difatti una qualunque operazione o insieme di operazioni, eseguite o meno grazie ad un computer, riguardanti la visione, la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la comunicazione, la

diffusione, la cancellazione e la distruzione di dati. La sicurezza organizzativa attiene alla definizione di ruoli, compiti, responsabilità, e procedure nella gestione della problematica sicurezza.

Ruoli e figure previste dalla normativa:
TITOLARE DEL TRATTAMENTO è l'azienda stessa. Al titolare competono le decisioni circa le finalità, le modalità del trattamento di dati personali, gli strumenti utilizzati, il profilo della sicurezza. È giuridicamente responsabile nei confronti degli interessati.

RESPONSABILE DEL TRATTAMENTO soggetto preposto dal titolare al trattamento. La nomina di un responsabile interno era già facoltativa in passato. Attualmente è prevista la necessità di nominare la figura del responsabile della protezione dei dati o **DPO** (Data Protection Officer) solo in casi specifici, nei quali l'azienda **non** rientra. **Non è stato nominato pertanto il DPO.**
Il Regolamento europeo (art. 37) prevede infatti la nomina del DPO è obbligatoria:
a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali;
b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

INCARICATI DEL TRATTAMENTO sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare. Devono attenersi alle istruzioni impartite. La loro designazione è in passato avvenuta per iscritto e individuava l'ambito del trattamento consentito. Il Regolamento Europeo Privacy, pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice), non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento). Gli atti di nomina predisposti in passato rappresentano una ulteriore responsabilizzazione di queste persone attraverso la specifica lettera di attribuzione di incarico. Si tratta senz'altro di una buona prassi volta a poter ulteriormente sostenere la dimostrabilità della compliance al GDPR. **Questa facoltà non deve essere intesa come un obbligo normativo**. **In applicazione del Regolamento Europeo Privacy si è ritenuto di non dover procedere a una nuova nomina degli incaricati.** Hanno inoltre accesso ai dati riguardanti la società tutti i soggetti esterni individuati nello stesso modulo.

ANALISI DELLE MINACCE E DEI RISCHI E DPIA

Minacce

Per minaccia s'intende la possibile causa di un incidente dannoso per l'azienda. Per valore della minaccia s'intende la probabilità/frequenza del concretizzarsi della stessa (da minaccia ad attacco vero e proprio).

1) Minacce naturali

Allagamenti, inondazioni, incendi, esplosioni, fulmini, terremoti, deterioramento dovuto al tempo, black out elettrici, corto circuiti ecc.

2) Guasti tecnici

Fisiologici, dovuti ad esempio al logorio del tempo, e patologici, dovuti alla casualità o alla responsabilità di persone. Tali guasti possono riguardare: le infrastrutture (difetti di costruzione, installazione o funzionamento di una porta o di

un cancello automatico, difetto di chiusura di una finestra, ecc.); le strutture (vizi nella costruzione o nel funzionamento delle serrature di armadi, ecc.); l'hardware (vizi di costruzione, assemblaggio, installazione, manutenzione ecc.); il software (difetti di produzione, installazione, configurazione, manutenzione, aggiornamento ecc.); i guasti su hardware e software possono ovviamente in ultima analisi compromettere il patrimonio informativo.

3) Minacce dovute a comportamenti umani, concretizzabili in:

3a) minacce di tipo fisico accidentali (patrimonio informativo ovvero smarrimento di un fascicolo, alterazione casuale, fortuito trattamento dei dati personali non consentito ecc.; infrastrutture (accesso non autorizzato inconsapevole, ecc.); strutture (danneggiamento fortuito di una serratura, ecc.); hardware (distruzione o danneggiamento fortuito, uso senza istruzioni, poco riposo delle macchine ecc.); software (distruzione e danneggiamento, errori nell'installazione, utilizzo improprio, conflitto tra programmi ecc.); risorse professionali (minaccia causata dalla scarsa consapevolezza o sensibilità alla problematica della sicurezza da parte del personale, ecc.).

3b) minacce di tipo fisico volontarie (esempio accesso doloso ai dati, trattamento erroneo, non consentito, non conforme alla raccolta o eccedente questa, danneggiamento, scassinamento, atti vandalici, mancato rispetto volontario delle istruzioni, sabotaggio).

3c) minacce di penetrazione logica accidentale su: software (intercettazioni accidentali, accesso non consentito a un programma o un file ecc.); risorse professionali (minaccia causata dalla scarsa consapevolezza o sensibilità del personale alla problematica della sicurezza, a vizi di procedura, scarsa cura nella gestione dei dati, negligenza nello svolgimento di un compito particolare, ecc.).

3d) minacce di penetrazione logica volontaria, su hardware (monitoraggio indebito o alterazione della trasmissione dati effettuata da router e server ecc.); software (minacce costituite da intercettazioni, virus, trojan horse, intrusioni, ecc.); risorse professionali (possibili intimidazioni, pressioni, ricatti, che il personale dipendente può subire ma può anche perpetrare, qualora maturi motivi di rivalsa verso l'azienda ecc.).

Rischio, conseguenze sui dati personali

Il rischio dipende dal concretizzarsi di una minaccia specifica. Le **conseguenze** a livello di tutela dei dati sono misurate in relazione a:

- distruzione, danneggiamento o perdita di dati personali
- alterazione di dati personali
- accesso non consentito
- trattamento dati non conforme, erroneo, eccedente, non consentito (specialmente nella forma della comunicazione o diffusione dati)

Il **livello di sicurezza da garantire**, rispetto alle conseguenze sopra elencate, è stabilito in base alla valutazione delle informazioni in termini di importanza. La **valutazione dell'importanza delle informazioni** viene condotta dai responsabili interni, tenendo conto di fattori quantitativi (costo di ripristino dell'informazione lesa o perduta, costo per l'elaborazione dell'informazione tramite risorse alternative) e qualitativi (importanza strategica per l'azienda, conseguenze penali, economiche e in termini di immagine a seguito di violazioni della normativa sulla tutela dei dati).

Valutazione importanza delle informazioni in funzione di

- violazione di una norma di legge/regolamento europeo
- violazione di vincoli contrattuali
- perdite monetarie

- compromissione rapporti con il personale
- interruzione della continuità del business
- lesione dell'immagine
- mancato raggiungimento dell'adeguamento ad uno standard

MISURE A TUTELA DEI DATI PERSONALI

Stato della sicurezza, gestione dell'informazione e del consenso

Il Codice italiano in materia di protezione dei dati personali, all'art. 13 ha previsto a coloro che trattano dati personali di terzi, di rendere a questi un'esauriente informativa, oralmente o per iscritto. L'azienda ha previsto in passato appositi moduli d'informativa per i soggetti fisici e le persone giuridiche, i cui dati vengono trattati nell'esercizio della propria attività di lavoro e d'ufficio. I moduli d'informativa contengono tutte le indicazioni richieste dalla normativa ovvero: i motivi del conferimento dati, le modalità di raccolta, i requisiti dei dati, le finalità del trattamento, la natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di un eventuale rifiuto di conferirli, i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi, i diritti degli interessati, la ragione sociale la sede del titolare cui rivolgersi per l'esercizio dei diritti riconosciuti dall'art. 7, l'identità del Responsabile se designato.

Il **Regolamento UE 2016/679 agli artt. 13 e 14** disciplina le informazioni da fornire all'interessato del quale si raccolgano i dati. Il Garante ha affermato che il consenso ottenuto prima della data di efficacia del GDPR continua a costituire valida base giuridica del trattamento purché sia stato raccolto con modalità tali per cui risulti "libero, specifico, informato".

Notificazione ed Autorizzazione

In **passato** si era provveduto a valutare come **non necessaria** la notifica del trattamento effettuato dalla società all'Autorità Garante per la Protezione dei Dati Personali. Nessun trattamento effettuato era difatti presente tra quelli da notificare, elencati all'art. 37 del Codice sulla tutela dei dati personali.
Per quanto riguarda l'Autorizzazione al trattamento dei dati sensibili, l'Autorizzazione Generale concessa dal Garante per il trattamento dati in osservanza d'obblighi contabili, retributivi, previdenziali, assistenziali, fiscali e assicurativi, nell'ambito dei rapporti di lavoro, copriva pienamente l'attività della società. Nessuna azione è richiesta all'azienda rispetto a questi due adempimenti previsti in passato.

Sicurezza fisica

Il ruolo della sicurezza fisica è quello di proteggere le aree, le strutture, l'hardware ed il software, adibiti al trattamento dei dati personali, ed il personale stesso che si occupa del trattamento. La procedura si applica all'intero sistema aziendale.

Sicurezza logica, situazione attuale, raccomandazioni e suggerimenti

La sicurezza informatica può essere definita come l'insieme delle misure (di carattere tecnologico ma anche organizzativo, che tratteremo di seguito) atte a garantire l'autenticazione dell'utente, la disponibilità, l'integrità e la riservatezza delle informazioni e dei servizi, gestiti in modo digitale.

In particolare, s'intende per autenticazione, la conferma dell'identità dichiarata da un organismo o un utente (internet banking, stipula di contratti on line, telelavoro ad esempio). La disponibilità è invece la conferma che i dati sono accessibili e i servizi funzionano anche in caso di interruzioni dovute alle cause più disparate (venir meno dell'alimentazione elettrica, eventi naturali, pirateria informatica per esempio). L'integrità dei dati è la conferma che i dati trasmessi, ricevuti o conservati sono completi e non alterati. Infine la riservatezza, ovvero la protezione dei dati trasmessi ricevuti o conservati al fine di evitarne l'intercettazione e la lettura da parte di persone non autorizzate.

Le contromisure di sicurezza logica sono misure di carattere tecnologico quali: il controllo degli accessi che permette l'identificazione degli utenti, la presenza di antivirus, il controllo del software attraverso l'aggiornamento costante dei prodotti (installazione di patch), la verifica periodica dell'installazione e della configurazione dei prodotti software, la configurazione della rete e il suo monitoraggio, l'uso della crittografia, le procedure di back-up, le procedure di business continuity.

Sensibilizzazione e formazione degli incaricati

La formazione è programmata anche per la tutela dei dati personali al momento dell'ingresso in servizio e per tutta la durata del rapporto di lavoro.

Verifiche dei risultati, azioni correttive e preventive

Una volta emanate le norme comportamentali è necessario verificare le misure tecnologiche ed organizzative adottate e misurare i risultati ottenuti.
A livello di verifiche è necessario: tenere sotto controllo le aree critiche; sincerarsi periodicamente del rispetto delle procedure; verificare le intrusioni o tentativi di intrusione e in caso di intrusione rispondere nella maniera più appropriata all'attacco; valutare il feed back degli incaricati; misurare i risultati raggiunti nell'attuazione del sistema di gestione delle informazioni.

A titolo esemplificativo si indicano come oggetto di verifica:

- le condizioni di acceso fisico ai locali dove si svolge il trattamento
- la corretta gestione delle parole chiave
- il rispetto dei livelli di accesso stabiliti dalla direzione
- l'integrità delle copie di back-up
- la corretta conservazione dei documenti cartacei
- la sicurezza delle trasmissioni in rete
- la correttezza della trasmissione dati via mail e cellulare

- il rispetto delle regole per la comunicazione dei dati via telefono
- il livello di formazione degli incaricati

Sintesi delle misure da implementare

Dopo aver descritto quanto fatto dalla società per la tutela dei dati personali sintetizziamo in una serie di tabelle il piano operativo per il futuro. Il piano è stato concordato con la direzione e si basa su risultati d'analisi e scelte di gestione che dovranno essere continuamente messe in discussione. Questo al fine di garantire la capacità dell'azienda di mantenere nel tempo la sicurezza del proprio patrimonio informativo, anche in presenza degli inevitabili cambiamenti dovuti a fattori esterni o interni all'azienda.

Il presente documento è stato compilato sulla base delle informazioni acquisite dalla società. La responsabilità circa la rispondenza a verità di quanto dichiarato e l'osservanza delle linee guida suggerite non fanno ovviamente carico alla nostra organizzazione. L'affidamento a professionisti esterni specializzati in materia di tutela dei dati personali, garantisce un costante aggiornamento, grazie anche al servizio di consulenza a cui la società ha aderito.
La società dovrà proseguire nell'opera di adeguamento dell'organizzazione alla normativa, verificando nel tempo, l'efficacia e la validità delle misure di sicurezza adottate.

DOCUMENTAZIONE

La **ECO.REC SRL** opera nel settore del trattamento e smaltimento di rifiuti (oli esausti) per conto di aziende aventi sedi operative in tutta Italia. L'attività di promozione avviene attraverso canali soprattutto tradizionali, ovvero passaparola. L'azienda ha un sito web; è presente una Pagina Facebook aziendale attraverso la quale non avvengono trattative o comunicazioni.

Descrizione delle banche dati in trattamento: l'azienda effettua, nell'esercizio della propria attività, il trattamento di dati personali di tipo sia comune che sensibile. Le informazioni trattate riguardano dipendenti, candidati all'instaurazione di un rapporto di lavoro, fornitori, clienti, consulenti, altre società, banche, assicurazioni, poste, enti previdenziali e d'assistenza, associazioni varie, soggetti pubblici ecc. Si tratta di persone fisiche e giuridiche legate alla società attualmente o anche in senso potenziale (informazioni pre-contrattuali).

Il trattamento dei dati comuni effettuato comprende a titolo esemplificativo: ragione sociale, indirizzo della sede, partita IVA, qualifica del soggetto, potenziale e/o attuale interlocutore della società, numero di fax, indirizzo di posta elettronica (per i fornitori di servizi e materiali ed i clienti), generalità di candidati all'instaurazione di un rapporto lavorativo ecc. La tutela di questa tipologia di dati richiede solitamente un ordinario livello d'attenzione, trattandosi di dati facilmente recuperabili e spesso in regime di piena conoscibilità giuridica.

I dati sensibili vengono in rilievo in relazione alla gestione del personale (assistenza e previdenza sociale, trattenute sindacali ad esempio). Da tenere in considerazione anche i dati, detti "semi-sensibili", da collocarsi appunto a metà tra dati comuni e sensibili (relativi alla situazione finanziaria di un soggetto come l'inserimento nelle liste di sospettati di

frode, le informazioni contenute nelle centrali rischi ed in generale i dati concernenti l'affidabilità ed alla puntualità nei pagamenti ecc.).

Livello d'importanza medio-alto, è stato infine attribuito a quei dati personali che, pur non avendo intrinsecamente natura particolare, possono essere in qualche modo discriminanti a seconda dell'uso che ne viene fatto (es: le schede valutative dei dipendenti ecc.).

I dati trattati sono entrati ed entrano in possesso della società:
a) a seguito di conferimento di volta in volta da parte degli interessati (clienti, utenti, fornitori, candidati all'instaurazione di un rapporto di lavoro) che richiedono informazioni direttamente o attraverso richieste telefoniche o provenienti dal sito web (anche nel contesto d'attività pre-contrattuali);
c) per l'esecuzione delle prestazioni contrattuali pattuite.
Il trattamento è di tipo misto, ovvero relativo a dati registrati su cartaceo (archivi, tabulati, agende, fogli liberi...) e a livello informatico (dati in formato elettronico, dati in transito ecc.).

Il trattamento è finalizzato:
a) all'esercizio dell'attività di commercializzazione e realizzazione dei servizi offerti dal preventivo alla consegna finale del lavoro, incluso l'espletamento di pratiche pre-contrattuali;
b) all'adempimento di tutte le attività necessarie e funzionali alle lettere a) e b) all'adempimento di specifici obblighi amministrativi, contabili, retributivi, previdenziali, assistenziali e fiscali, imposti dalla gestione del trattamento giuridico ed economico del personale e dei collaboratori, dei clienti, dei fornitori, dei consulenti ecc. e dall'intrattenimento di rapporti con banche, assicurazioni ed istituzioni;
c) occasionalmente alla selezione del personale.
Il trattamento riguarda solo le categorie di dati, d'interessati e di destinatari della comunicazione strettamente collegate ai fini appena citati. La conservazione dei dati è limitata al periodo necessario all'adempimento degli obblighi citati, alle esigenze commerciali e agli obblighi imposti dalla legge.

Censimento infrastrutture, strutture

L**'**azienda **ECO.REC SRL** ha sede legale e operativa a Montescudaio (PI) in località Poggio Gagliardo in un capannone industriale artigianale che comprende: 2 uffici direzionali, un archivio adibito anche a sala server, un ufficio amministrativo al piano primo e i locali magazzino e l'impianto di trattamento al piano terra.
Si provvede anche all'attività propedeutica di invio/ricezione dei documenti, alla trasmissione ed alla conservazione della documentazione richiesta dalla legge ai fini contabili.
L'azienda ha in dotazione 8 PC collegati in rete. Non sono in uso pc portatili. Negli uffici è disponibile un collegamento wireless. La gestione del sistema informatico è stata delegata ad una ditta esterna (ditta individuale) che cura la manutenzione del server e le stampanti**.**

Risorse professionali

I soggetti esterni più significativi individuati ai fini del trattamento dati sono:
Studio gestione paghe/commercialista

Legale/i

Assicurazioni

Consulenti sicurezza lavoro

Medico competente

Manutenzione/assistenza informatica

Manutenzione elettrica e elettronica

Per i soggetti dell'elenco sopra citato, che operano in autonomia, e per tutti quelli che l'azienda valuterà in seguito di inserire nell'elenco stesso, si è redatto un modulo da far controfirmare dove il soggetto esterno attesta di conoscere la normativa vigente ed agire conformemente ad essa nel trattamento dei dati trasmessi dall'azienda.

Analisi delle minacce

In considerazione dell'attività svolta dall'azienda e del relativo trattamento dati in essere <u>non è necessaria la DPIA</u> (Data Protection Impact Assessment) poiché l'articolo 35, comma 1, del GDPR prevede che il processo di DPIA sia obbligatorio quando un trattamento di dati personali "presenti un rischio elevato per i diritti e le libertà delle persone fisiche"[1]. Si è comunque effettuata un'analisi delle minacce e dei rischi in quanto strumento necessario e utile per i titolari del trattamento al fine di rispettare la legge in materia di protezione dei dati.

Pur non avendo fatto una DPIA si sono comunque valutate le minacce e i rischi in funzione della scelta/implementazione delle misure di sicurezza a protezione dei dati adottate/da adottare.

L'analisi delle minacce e dei rischi è stata fatta presso l'azienda in occasione dell'incontro avuto dalla direzione con il consulente privacy esterno. In tale occasione sono emerse le seguenti risultanze:

Quanto alle **minacce naturali**: l'ubicazione della struttura non la espone a fattori particolari sia per quanto riguarda gli archivi cartacei che quelli informatici. Sono presenti le dotazioni richieste ai fini della sicurezza del lavoro.

Quanto ai **guasti tecnici**: si rientra nella norma. Inevitabile la possibile rottura del disco a cui si ovvia con i sistemi di salvataggi dati in uso. Stessa cosa dicasi per i possibili black out a cui si ovvia con sistemi di continuità e di autoalimentazione.

Per le minacce rappresentate da **comportamenti umani** tenuti da insider ed outsider si distingue:

- per gli archivi fisici (non accettabili minacce relative a imprudenza imperizia negligenza, errore materiale, invio scorretto materiale, rallentamento dell'operatività, invio o diffusione non autorizzata di informazioni) solo la sensibilizzazione e la formazione del personale e dei collaboratori, può costituire contromisura efficace in tal senso si è stipulato un contratto di consulenza professionale specifica per la materia privacy e si sono adottate azioni di sensibilizzazione/formazione del personale;
- per il sistema informatico su cui operano gli amministrativi (non accettabili minacce relative a imprudenza imperizia negligenza, rallentamento dell'operatività, Installazione uso di software non autorizzato, software che provoca danni virus/trojan/worms, accessi esterni a servizi applicazioni elaboratori non autorizzati, alterazione non autorizzata delle configurazioni, lettura di dati su video non autorizzata, spamming e altre tecniche di sabotaggio) sono attive efficaci misure antintrusione, antivirus ed antispamming, ci sono livelli di accesso predefiniti, salvaschermo tot min ecc.

[1] Articolo 35 comma 1 - Valutazione d'impatto sulla protezione dei dati
Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. (omissis.)

Per le minacce da uso risorse aziendali per attività illecite/illegali, uso risorse aziendali per profitto personale, furto fisico, sabotaggio distruzione, furto elettronico, sabotaggio distruzione/diffusione dati, comportamenti sleali o fraudolenti, la probabilità si ritiene bassa.
Per le minacce costituite da errata interpretazione della normativa, imprudenza, imperizia e/o negligenza e rallentamento dell'operatività, solo la sensibilizzazione e la formazione del personale e dei collaboratori, può costituire contromisura efficace. Si vedano le contromisure dettagliatamente descritte nel paragrafo **"Misure a tutela dei dati".**

Analisi dei rischi

Pur non avendo fatto una DPIA si sono comunque valutate le minacce e i rischi in funzione della scelta/implementazione delle misure di sicurezza a protezione dei dati adottate/da adottare.
L'analisi dei rischi è stata fatta presso l'azienda in occasione dell'incontro avuto dalla direzione con il consulente. In tale occasione sono emerse le seguenti risultanze:

DIREZIONE/CONTABILITA'

Ha massimo livello di accesso ai dati. Si effettua il trattamento di dati di tipo strategico, valutativo, contrattuale, verbali ed altro ancora. Svolge anche l'attività propedeutica all'elaborazione paghe e dei contributi dei dipendenti e la gestione del personale in senso ampio (profili, gestione ore permessi ferie, cartellini identificativi, CV). Sono in trattamento, nella forma della presa visione, dell'accesso, praticamente tutte le tipologie di dati. I dati relativi ai dipendenti vengono raccolti in azienda e poi trasmessi allo Studio del consulente del lavoro.

Criticità media

La gravità risulta minima per molti dati. Vista l'attenzione alla limitazione all'accesso agli uffici, l'alterazione di dati e l'accesso non consentito agli stessi sono a frequenza molto bassa. L'azienda è gestita da un gruppo familiare per cui è basso il rischio di volontà di manomissione o alterazione dei dati.

PROFILO DI RISCHIO MEDIO PER TRATTAMENTO NON CONFORME

UFFICIO COMMERCIALE

L'ufficio svolge il compito di approvvigionamento clienti e gestione della stipula dei contratti di acquisto di materiali e servizi. I rapporti con i clienti e fornitori implicano il trattamento di dati comuni per l'esecuzione delle prestazioni contrattuali e/o precontrattuali.

Criticità alta

I soggetti che si occupano di gestione del parco clienti sono limitati numericamente e consapevoli del ruolo svolto. Accesso non consentito dati particolari occasionale per la consuetudine di conservare fuori dal campo visivo e protetti in armadi i documenti contenenti dati sensibili. Attive user id e password, previsti livelli di accesso differenziati per gli utenti.

PROFILO DI RISCHIO MEDIO PER TRATTAMENTO NON CONFORME

SEGRETERIA/AMMINISTRAZIONE

L'ufficio gestisce i rapporti con i fornitori e i clienti; ciò implica il trattamento di dati comuni per l'esecuzione delle prestazioni operative e amministrative. Si occupa parzialmente di gestione bancaria e fiscale e amministrazione

contabile. Alta importanza in termini di costo di conseguenze penali ed economiche in caso di violazioni della normativa in materia di tutela dei dati.

Criticità alta

I soggetti sono limitati numericamente e consapevoli del ruolo svolto. Accesso non consentito dati particolari occasionale per la consuetudine di conservare fuori dal campo visivo e protetti in armadi chiusi a chiave i documenti contenenti dati sensibili. Attive user id e password, previsti livelli di accesso differenziati per gli utenti.

PROFILO DI RISCHIO MEDIO PER TRATTAMENTO NON CONFORME

INFORMATION TECNOLOGY

L'assistenza informativa avviene con il supporto di un soggetto esterno, che si occupa di configurazione e funzionamento di tutti i server. L'area rileva per importanza e criticità effettuando operazioni su dati in trattamento presso le altre aree ed occupandosi di misure di sicurezza. La rilevanza è dunque tecnica. Gestendo le misure di sicurezza attribuiamo,

Criticità media

PROFILO DI RISCHIO MEDIO PER TRATTAMENTO NON CONFORME/DISTRUZIONE DI DATI

Tale soggetto esterno possiede i requisiti di idoneità, esperienza ed affidabilità che costituiscono garanzia del rispetto delle disposizioni vigenti in materia di trattamento e sicurezza dei dati. Il soggetto opera come titolare autonomo del trattamento ma si è previsto un attestato di conformità da far firmare.

ALTRI SOGGETTI ESTERNI RILEVANTI PER IL TRATTAMENTO DATI[2]:

CONTENZIOSO ED ASSISTENZA LEGALE
CONSULENTE GESTIONE PAGHE/COMMERCIALISTA
ASSICURAZIONI
SICUREZZA SUL LAVORO
MEDICO COMPETENTE
ALTRI CONSULENTI/COLLABORATORI ESTERNI
In trattamento da parte dei soggetti elencati, dati comuni, semi-sensibili (finanziari), sensibili e anche giudiziari.

Criticità alta

Trattamento dati non conforme, in eccesso, non consentito, grave la comunicazione o diffusione impropria di dati finanziari o giudiziari, la quale è fonte di possibile contenzioso e crea tensioni nei rapporti professionali. Di massima gravità la comunicazione o diffusione di dati sulla salute, la quale configura violazione di legge, è fonte di possibile contenzioso e crea tensioni nei rapporti di lavoro e sfiducia verso la serietà dell'azienda.

PROFILO DI RISCHIO MEDIO PER TRATTAMENTO NON CONFORME

Una volta trasmessi i dati è il soggetto esterno a provvedere al loro trattamento in autonomia. Tali soggetti possiedono quei requisiti di idoneità, esperienza ed affidabilità che costituiscono garanzia del rispetto delle disposizioni vigenti in

2

materia di trattamento e sicurezza dei dati. Il soggetto opera come titolare autonomo del trattamento ma si è previsto un attestato di conformità da far firmare.

DOCUMENTI DI SUPPORTO

Misure a tutela dei dati personali, gestione dell'informazione e del consenso

TRATTAMENTI INTERESSATI: tutti i trattamenti relativi a direzione, dipendenti, collaboratori, clienti e fornitori.
RISCHIO CONTRASTATO: Trattamento non conforme, in eccesso
MINACCIA rappresentata da comportamenti umani di insider
AMBITO APPLICAZIONE: tutta l'azienda nei rapporti interni e con l'esterno

MISURE	ADOTTATE	DA ADOTTARE	Periodicità dei controlli	Responsabilità dei controlli
1. INFORMATIVA DIPENDENTI	X	–	In caso di mutamenti dell'attività o della normativa	Titolare
2. INFORMATIVA CANDIDATI	X	–	In caso di mutamenti dell'attività o della normativa	Titolare
3. INFORMATIVA E CONSENSO CLIENTI E UTENTI	X	–	Adottata in passato, adesso nell'ambito dei rapporti contrattuali non è più necessario ottenere il consenso	Titolare
4. INFORMATIVA FORNITORI	X	–	Adottata in passato, adesso nell'ambito dei rapporti contrattuali non è più necessario darla per iscritto e ottenere il consenso	Titolare
5. DISTRIBUZIONE POLICY PRIVACY PER IL PERSONALE	X	–	In caso di mutamenti dell'attività o della normativa	Titolare

In generale:

Gestione di informativa a consenso

Il Garante ha affermato che il consenso ottenuto prima della data di efficacia del GDPR continua a costituire valida base giuridica del trattamento purché sia stato raccolto con modalità tali per cui risulti "libero, specifico, informato". **La pregressa documentazione in materia di informativa e consenso è dunque ancora valida. Si è provveduto ad aggiornare la modulistica con i nuovi riferimenti al Regolamento UE 2016/679 e agli artt. 13 e 14 relativi alle informazioni da fornire all'interessato del quale si raccolgano i dati.**

1. INFORMATIVA E CONSENSO DIPENDENTI

L´informativa è stata consegnata in passato a mano ai dipendenti i quali hanno controfirmato per presa visione. L'informativa è stata aggiornata e sarà consegnata insieme al vademecum. La si utilizzerà in caso di nuove assunzioni con consegna a mano.

I dati dei dipendenti in trattamento dono solo quelli trattati per finalità amministrative e contabili ovvero per finalità legate all'assolvimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi,

alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.L'informativa ai dipendenti non prevede più la richiesta di consenso al trattamento per i dati sensibili. Non è necessario il consenso scritto dell'interessato poiché il trattamento dei dati sensibili avviene in rapporto a specifici obblighi o compiti previsti dalla legge per la gestione del rapporto di lavoro.

2. INFORMATIVA CANDIDATI

I candidati all´atto della presentazione e della consegna del curriculum inseriscono la clausola relativa al trattamento dei dati autorizzandoci di fatto. In aggiunta si è prevista un'informativa cartacea che viene data in occasione del primo colloquio. I dati sono trattati solo a fini di selezione del personale.

3. INFORMATIVA/CONSENSO CLIENTI E UTENTI

Clienti e utenti sono stati informati in passato. Per la tipologia del business esercitato clienti e fornitori sono acquisiti da molto tempo e per la natura del business stesso il rischio di contenzioso/problematiche con tali soggetti è molto basso.
Si è predisposta al termine del presente documento una clausola contrattuale privacy. Per le comunicazioni informative e promozionali si è integrato il modulo in uso per i contratti. prevedendo un consenso modulare.

4. INFORMATIVA FORNITORI

E´ stata fornita in passato. La pregressa documentazione in materia di informativa e consenso è dunque ancora valida. L'informativa ai fornitori nell'ambito di attività contrattuali/precontrattuali non è necessaria. Nessuna ulteriore azione è richiesta. Si è predisposta al termine del presente documento una clausola contrattuale privacy.

5. DISTRIBUZIONE POLICY PRIVACY PER IL PERSONALE

Alla politica sulla pricavy è stata data idonea diffusione attraverso una distribuzione cartacea con firma per ricezione, si veda esempio di verbale, allegato n. 5.

Misure a tutela dei dati personali, stato della sicurezza fisica

TRATTAMENTI INTERESSATI: tutti i trattamenti relativi a direzione, dipendenti, collaboratori, clienti e fornitori.
RISCHIO CONTRASTATO: distruzione, danneggiamento, perdita dati, accesso dati non consentito
MINACCIA rappresentata da comportamenti umani di insider ed outsider, minacce naturali, guasti tecnici.
AMBITO APPLICAZIONE: tutta l'azienda.

MISURE	ADOTTATE	DA ADOTTARE	Periodicità dei controlli	Responsabilità dei controlli
6. ACCESSI	X	_	quotidiana	Addetto al bancone in ingresso, personale impiegatizio
7. PROCEDURA REGISTRAZIONE INGRESSI	_	_	Ritenuta non necessaria	-
8. ALLARME ANTINTRUSIONE COLLEGATO A SOCIETÀ	X	_	Manutenzione da parte dell'istallatore, consultazione in caso di effrazione	Addetti installazione/manutenzione sistema

VIGILANZA				
9. VIGILANZA E VIDEOSORVEGLIANZA	X	_	Quotidiana	Addetti esterni
10. ARMADI CHIUSI A CHIAVE PER LA DOCUMENTAZIONE RISERVATA	X	_	quotidiana	Titolare
11. ARCHIVIAZIONE SEPARATA CV IN DIRECTORY APPOSITE	X	_	Alla ricezione	Incaricata amministrativa
12. SICUREZZA DOCUMENTI CARTACEI E SUPPORTI INFORMATICI	X	_	Quotidiana	Titolare
13. DOCUMENTI RISERVATI RESI ILLEGGIBILI PRIMA DI ESSERE GETTATI	X	_	Quotidiana	Titolare
14. CONTENITORI MUNITI DI SERRATURA PER ASPORTAZIONE PER TEMPO CONSIDEREVOLE DATI RISERVATI ALL'ESTERNO	_	X	Al momento contenitore chiuso con cerniere non trasparente, consegna brevi manu	Titolare
15. PROTEZIONE FISICA SERVER ED ALTRO HW, ALIMENTAZIONE E CONTINUITÀ ELETTRICA	X	_	Costante	Titolare, tecnico interno, professionista esterno
16. RILEVAZIONE PRESENZE	X	_	Ritenuta non necessaria negli uffici	Titolare
17. USO CARTELLINI IDENTIFICATIVI	X	_	Ritenuta non necessaria negli uffici	Titolare

6. ACCESSI

La reception svolge funzione di controllo accessi. L'ufficio non è aperto al pubblico.

7. PROCEDURA REGISTRAZIONE INGRESSI

Non è attiva una procedura di registrazione per le dimensioni aziendali e poiché i visitatori sono accompagnati personalmente. Sono accolti con e senza appuntamento anche se solitamente hanno un appuntamento fissato.

8. ALLARME/I

E' attivo un sistema antintrusione volumetrico a protezione della proprietà

9. ARMADI

Sono presenti armadi per la conservazione dei documenti. I documenti ritenuti riservati sono riposti in tali armadi.

10. ARCHIVIAZIONE SEPARATA CV

Se il CV non è d'interesse viene distrutto, altrimenti viene tenuto nel mobile adibito ai documenti del personale.

11. SICUREZZA DOCUMENTI CARTACEI E SUPPORTI INFORMATICI

I documenti cartacei più importanti sono conservati in armadi e/o cassetti tenuti chiusi e i locali sono tutti ad accesso selezionato. Dopo l'orario di lavoro non sono ammessi accessi.

12. TRITADOCUMENTI

Tutti i documenti contenenti dati personali o aziendali riservati che si ritiene debbano essere eliminati sono distrutti in modo da renderli illeggibili.

13. CONTENITORI PER TRASPORTO ALL'ESTERNO

Nel rapporto con i consulenti/studi ect. i dati sono consegnati direttamente ai soggetti terzi che collaborano con l'azienda e chi li riceve provvede in proprio al trasporto. I documenti che vengono portati all'esterno da parte del personale (principalmente offerte commerciali e documenti tecnici) sono inseriti in cartelline non trasparenti e lì tenuti fino al loro utilizzo presso il cliente o fino alla consegna al cliente.

14. PROTEZIONE FISICA SERVER E ALTRO HARDWARE

La zona Server è isolata rispetto agli uffici dove ha accesso personale esterno o i dipendenti. Per la protezione da danneggiamenti accidentali o intenzionali, l'azienda è dotata di stabilizzatori di corrente per assicurare la continuità elettrica. Nello specifico per la protezione dagli sbalzi e dall'interruzione di energia elettrica, è stato acquistato un gruppo di continuità per il server con autonomia di almeno 30 minuti. Analoga autonomia sarebbe ottimale per i personal computer degli uffici amministrativi. Sono presenti inoltre le dotazioni standard richieste dalle normative in materia di sicurezza dei luoghi di lavoro. Sugli estintori è attivo un abbonamento di controllo.

Misure a tutela dei dati personali, stato della sicurezza logica e organizzativa

TRATTAMENTI INTERESSATI: tutti i trattamenti relativi a direzione, dipendenti, collaboratori, clienti e fornitori.
RISCHIO CONTRASTATO: distruzione, danneggiamento, perdita dati, accesso dati non consentito, trattamento non conforme, in eccesso
MINACCIA rappresentata da comportamenti umani di insider ed outsider, guasti tecnici.
AMBITO APPLICAZIONE: tutta l'azienda.

MISURE	ADOTTATE	DA ADOTTARE	Periodicità dei controlli	Responsabilità dei controlli

18. LIVELLI ACCESSO	X	_	Semestrale	Titolare
19. ASSEGNAZIONE/SCELTA PAROLE CHIAVE	X	_	Semestrale o trimestrale	Titolare
20. LIVELLI ACCESSO E TELEASSISTENZA	X	_		
21. NOMINA DEL RESPONSABILE	_	_	Non più necessaria	Titolare
22. REDAZIONE MODULI NOMINE INCARICATI CON ISTRUZIONI SCRITTE AGLI INCARICATI	_	_	Non più necessaria, fatta in passato	Titolare
23. ATTESTATI CONFORMITA' OPERATO SOGGETTI ESTERNI CHE TRATTANO DATI AZIENDALI	X	_	Revisione in caso di mutamenti sostanziali/variazioni normative	Titolare
24. CLAUSOLE NEGLI ACCORDI CONTRATTUALI CON SOGGETTI ESTERNI	X	_	Al momento della stipula del contratto e in occasioni di variazioni dello stesso	Titolare
25. PROCEDURE DI ACCESSO SELEZIONATO AGLI ARCHIVI CARTACEI	X	_	Semestrale	Titolare
26. FIREWALL	X	_	Periodico secondo i suggerimenti del consulente informatico	Titolare e consulente informatico
27. PROGRAMMI ANTIVIRUS	X	_	Aggiornamento quotidiano	Titolare e consulente informatico
28. SICUREZZA DEL SOFTWARE	X	_	Periodico secondo i suggerimenti del consulente informatico	Titolare e consulente informatico
29. MONITORAGGIO DEL SISTEMA DI PROTEZIONE, TEST D'INTRUSIONE	X	_	Periodica ed almeno semestrale	Titolare e consulente informatico
30. REDAZIONE REPORT SCRITTI SUL MONITORAGGIO DEL SISTEMA DI PROTEZIONE	X	_	Stessa periodicità del monotiraggio	Titolare e consulente informatico
31. BACKUP	X	_	quotidiana	Titolare e consulente informatico
32. CONSERVAZIONE PERIODICA, ESTERNA AGLI UFFICI DI BACK UP	X	_	Periodicamente	Consulente informatico
33. BUSINESS CONTINUITY	X	_	Da stabilire	Titolare e consulente informatico
34. INCIDENTI E DISASTER RECOVERY	_	X	Da stabilire	Titolare e consulente informatico

35. CANCELLAZIONE DEFINITIVA DATI PARTICOLARI	X	_	All'occorrenza	Titolare
36. PROCEDURA RISPOSTA ALLE ISTANZE DEGLI INTERESSATI	X	_	In corso di approntamento. Revisione all'occorenza in seguito	Titolare
37. DISPOSIZIONI AZIENDALI PER LA CUSTODIA DEI DATI QUANDO SI VIAGGIA	X	_	Vedere manuale Qualità	Titolare
38. VEFIFICHE PRIVACY (AUDIT)	X	_	Fatta.	Titolare
39. CONSULENZA ESTERNA SPECIALIZZATA IN MATERIA TUTELA DEI DATI PERSONALI	X	_	Costante	Titolare

15. LIVELLI ACCESSO IMPIEGATI AMMINISTRATIVI

Tutte le cartelle possono essere accessibili a tutti, ad 1 o più utenti. Gli accessi sono determinati secondo l'organigramma e secondo le direttive della direzione aziendale. Internet: garantisce gli stessi accessi.

16. ASSEGNAZIONE/SCELTA PAROLE CHIAVE

Gli account utente sono gestiti da un server. La scadenza delle password utente è anch'essa gestita dal server di dominio e rispettanti le regole di complessità come imposto dalle norme vigenti. Quanto alla procedura di gestione delle password, si è previsto nel vademecum il caso di assenza o impedimento dell'utente e di necessità di accesso da parte dell'azienda (indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema). Il titolare, o chi da lui autorizzato, accede alle risorse riconducibili all'utente stesso e l'incaricato al suo rientro provvede a sostituire la password. L'incaricato viene informato tempestivamente dell'intervento effettuato.
I portatili aziendali sono sottoposti ai medesimi vincoli delle macchine fisse. Per l'accesso ad alcune delle risorse condivise è necessario identificarsi tramite il codice utente e la password, altre cartelle sono destinate allo scambio di file di interesse comune.

17. NOMINA DEL RESPONSABILE

La nomina di un responsabile interno era già facoltativa in passato. Attualmente è prevista la necessità di nominare la figura del **DPO** (Data Protection Officer) solo in casi specifici, nei quali l'azienda non rientra (art. 37). **Non è stato nominato pertanto il DPO.** Si occupa internamente della tutela dei dati personali il titolare quale persona idonea, sulla base della sua esperienza e conoscenza, ad assicurare il rispetto della normativa.

18. REDAZIONE MODULI NOMINE INCARICATI CON ISTRUZIONI SCRITTE AGLI INCARICATI

Il Regolamento Europeo Privacy, pur non prevedendo espressamente la figura dell'"incaricato" del trattamento (ex art. 30 Codice), non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati

personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento). **In applicazione del Regolamento Europeo Privacy si è ritenuto di non dover procedere a una nuova nomina degli incaricati.**

19. NOMINE ESTERNE

I fornitori esterni sono censiti dal sistema, sono ritenuti dall'azienda titolari autonomi del trattamento dei dati trasmessi. Una volta trasmessi i dati difatti è il soggetto esterno a provvedere al loro trattamento in autonomia. Tali soggetti possiedono quei requisiti di idoneità, esperienza ed affidabilità che costituiscono garanzia del rispetto delle disposizioni vigenti in materia di trattamento e sicurezza dei dati. Il soggetti operano come titolari autonomi del trattamento ma si è previsto un attestato di conformità da far firmare **"Attestazione di conformità della propria struttura e del proprio operato al Regolamento Privacy Europeo (UE/2016/679).**

20. PREVISTA CLAUSOLA GARANZIA PRIVACY E RELATIVA PROCEDURA

Si è prevista una clausola contrattuale privacy da inserire in futuro nei contratti con i **soggetti esterni ai quali l'azienda comunica dati personali (gestione paghe, sicurezza lavoro, legali etc.)** in modo da gestire la questione tutela dei dati personali in modo standardizzato. Questa clausola potrà essere inserita in futuro. Al momento per garantirsi con i soggetti esterni con i quali si collabora di è previsto di richiedere la firma del modulo di cui al punto che precede. **Clausola in allegato 4.**
Clausola privacy per clienti; modificato il documento con cui si effettua l'offerta commerciale prevedendo un'informativa separata per il trattamento a fini contrattuali rispetto a quello a fini di informazione e promozione e prevedendo l'aggiunta di un box da fleggare e della specifica dicitura di cui all' **allegato 5.**

21. PROCEDURE ACCESSO SELEZIONATO AGLI ARCHIVI

Non ci sono accessi dopo la chiusura della azienda. I dati del personale sono conservati in armadi accessibili solo al personale autorizzato.

22. FIREWALL

A protezione del sistema informatico dalle intrusioni esterne è presente un Firewall

23. PROGRAMMI ANTIVIRUS

Per la protezione da virus informatici è attivo un Antivirus centralizzato con Installazione su server della consolle di management, che gestisce aggiornamenti sia di definizioni che di programma in automatico.

24. SICUREZZA DEL SOFTWARE

Controllo del software, inteso come aggiornamento e verifica periodica dell'installazione e della configurazione dei prodotti software. Sono evidenziate periodicamente eventuali patch, fix o system-pack per la rimozione di errori o malfunzionamenti o per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

25. BACKUP DEI DATI

Backup dei server principali effettuato una volta al giorno, tutti i giorni, conservazione delle ultime due copie integrali.

26. CONSERVAZIONE ESTERNA SUPPORTI BACK UP

Per garantire una maggior sicurezza conservazione delle ultime due copie integrali di backup.

27. BUSINESS CONTINUITY

Il backup dei dati schedulato e incrementale, la conservazione su un supporto di storage garantiscono il recupero dei dati e il ripristino dell'operatività aziendale.

28. INCIDENTI E DISASTER RECOVERY

Non è attivo un vero e proprio disaster recovery plan, ovvero un piano che permetta di gestire una situazione di emergenza causata da un disastro che ha danneggiato le risorse informatiche (priorità di ripristino, tempi massimi di ripristino dei componenti del sistema informatico, reperibilità dei tecnici interni ed esterni, l'assegnazione di specifiche di responsabilità durante l'emergenza, le possibilità e modalità di continuazione dell'attività con metodi alternativi ecc.). Alcuni degli incaricati sono stati istruiti a reagire nelle situazioni di emergenza, ma solo verbalmente. Sarebbe necessario prevedere una procedura scritta.

29. CANCELLAZIONE DEFINITIVA DATI

A livello di PC e di Server, nel caso di attribuzione ad altro utente, i dischi vengono riformattati.

30. PROCEDURA DI RISPOSTA ALLE ISTANZE DEGLI INTERESSATI

Si è individuata la persona incaricata di rispondere e comunicati tempi e modi della risposta da fornire all'interessato che effettua la richiesta. In caso di ricezione di una richiesta sarà consultato il consulente al fine di rispondere correttamente e tempestivamente. In corso di redazione la relativa procedura. Nel frattempo ogni problematica sarà gestita con il supporto del consulente.

31. VERIFICHE PRIVACY (AUDIT)

Le verifiche verranno effettuate occasionalmente. Si provvederà a elaborare un modello di procedura da seguire per analizzare elementi quali: le condizioni di acceso fisico ai locali dove si svolge il trattamento, la corretta gestione delle parole chiave, l'integrità delle copie di back-up, la corretta conservazione dei documenti cartacei, la correttezza della trasmissione dati via mail e whatsapp ect. All'interno della società devono essere ancora attivate delle procedure specifiche privacy volte a definire e regolamentare i processi relativi alla misurazione, l'analisi ed il miglioramento del sistema di gestione dei dati. La verifica dovrà essere svolta da un soggetto individuato dalla direzione - che con l'eventuale aiuto di altri collaboratori, determinerà il contenuto esatto della verifica e ne richiederà l'approvazione della direzione. A seguito della verifica i responsabili delle aree coinvolte nelle quali si sono riscontrate violazioni, concorderanno con il responsabile della privacy i tempi e i modi per porre in essere misure correttive.

32. FORMAZIONE DIFFUSA PERSONALE

Sintesi delle misure da implementare

SOGGETTI INTERESSATI: tutto il personale.
RISCHIO CONTRASTATO: accesso dati non consentito, trattamento non conforme, in eccesso

MINACCIA rappresentata da comportamenti umani di insider.

MISURE	Da adottare subito	Da adottare in seguito	Periodicità dei controlli	Responsabilità dei controlli
Organizzazione e archiviazione di un nuovo Piano Privacy (documento di conformità aziendale)	X	_	All'occorrenza	Titolare
Conferma consenso per invio newsletter	X	_	Revisione in caso di mutamenti normativi o indicazioni provvedimenti/pareri del Garante	Titolare
Far entrare nelle operazioni quotidiane l'uso della modulistica suggerita	_	X	Revisione in caso di mutamenti normativi o indicazioni provvedimenti/pareri del Garante	Titolare
Invio ai soggetti esterni e richiesta di firma attestazioni conformità	_	X	Periodicamente	Titolare
Tritadocumenti per rendere più rapida la distruzione documenti	_	X		
Audit	_	X	Periodicamente	Svolta internamente, sotto controllo del titolare

La disponibilità e integrità dei dati è tutelata soprattutto a livello centralizzato e l'azienda ha attuato idonee misure di sicurezza.

È assicurata la presenza di dotazioni, in termini di arredi e strumentazioni, idonee alla custodia delle informazioni.

La riservatezza dei dati è invece rimessa in gran parte al comportamento dei singoli individui. Si sottolinea come la riduzione dei rischi può effettuarsi solo attraverso la sensibilizzazione e la formazione del personale sui comportamenti da tenere per il rispetto della normativa.

Si dovranno attivare le procedure previste e ottenere controfirmate dai soggetti esterni che collaborano con l'azienda, le attestazioni di conformità. La modulistica dovrà entrare a far parte della prassi quotidiana.

Nell'attuazione del piano operativo infine, si dovrà tenere conto anche dell'evoluzione organizzativa e logistica dell'amministrazione, della caduta d'attenzione delle persone coinvolte e del cambiamento delle persone che occupano i ruoli interessati. Nel caso in cui il piano non segua tempestivamente questi cambiamenti perde d'efficacia in breve tempo.