KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

VALUTAZIONE DEL RISCHIO DI PRIVACY

Registro Delle Attività Di Trattamento di cui L'art.30 del GDPR Sulla Sicurezza

Regolamento 2016/679 generale sulla protezione dei dati

Stato delle revisioni
Versione: 1.0 Data: Firma Titolare del trattamento

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Sommario

1.Scopo e campo di applicazione

Il presente Documento ha l'obiettivo di attestare la conformità delle misure organizzative e di sicurezza nonché fornire indicazioni relative alla produzione, gestione, conservazione e trasmissione delle informazioni aziendali con particolare attenzione a quelle di tipo elettronico che, per loro natura, risultano particolarmente critiche.

In questo Manuale sono altresì individuati i trattamenti, direttamente o attraverso collaborazioni esterne ovvero funzioni accentrate con l'indicazione della natura dei dati e della struttura (ufficio, funzione, etc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati. Si individuano i sistemi informativi impiegati, le precauzioni di tipo tecnologico per garantire la protezione degli strumenti elettronici e il personale coinvolto per tipologia per tutti i livelli prescritti, nonché i disciplinari cui sono assoggettati i vari soggetti coinvolti nei trattamenti.

Per la nostra azienda, i "dati"possono essere di tipo commerciale, rappresentare il portafoglio degli attuali clienti o di quelli futuri, ne conosciamo l'importanza e non dimentichiamo, però, che le potenzialità economiche dei dati sono direttamente proporzionali alla liceità del loro trattamento, raccoglierli nel rispetto della privacy e poterne quindi liberamente usufruire, significa creare valore per l'azienda.

Siamo consapevoli della differenza esistente tra i vari tipi di dati.

- I dati personali sono tutte le informazioni relative a una persona fisica, identificata o identificabile, anche indirettamente mediante riferimento a qualsiasi altra informazione), incluso l'eventuale numero di identificazione personale. Dati personali sono, ad esempio, un indirizzo e-mail o l'immagine fotografica di una persona, il codice fiscale o un numero telefonico, un indirizzo IP o una targa automobilistica. Si ricorda che, in base alle recenti novità legislative, non sono più considerati come dati personali, e quindi, almeno in linea generale, non sono più tutelati dalla normativa sulla privacy, i dati riferibili alle persone giuridiche, ovvero a imprese, enti e associazioni.
- I dati sensibili sono quei particolari dati personali che consentono di rivelare l'origine razziale ed etnica di una persona, le sue convinzioni religiose, filosofiche o di altro genere. Lo sono anche quelli che indicano l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale. Oppure i dati idonei a rivelare lo stato di salute e la vita sessuale. Sono tutte informazioni delicate che possono incidere sulla riservatezza e la dignità dell'individuo. Tra i dati che necessitano di particolari cautele vi sono quelli giudiziari - una categoria che include fra l'altro le informazioni contenute nel casellario giudiziale e quelle connesse alla posizione di imputato o indagato in procedimenti penali – ma anche i dati biometrici o i dati genetici.

Nella nostra realtà la ripartizione dei compiti e delle responsabilità è definita con chiarezza.
La struttura organizzativa è semplice ma per raggiungere gli obiettivi prefissati è stato necessario che ognuno sapesse quali sono le proprie responsabilità, "chi fa cosa" e con quali scadenze.
La catena di comando è particolarmente importante anche quando i "beni" usati sono i dati personali.
Il Codice della privacy evidenzia questa necessità e ci impone di definire bene quali figure hanno la possibilità di trattare dati personali.

- Il titolare del trattamento (data controller) è il soggetto che esercita un potere decisionale, del tutto autonomo, sulle finalità e sulle modalità del trattamento. La qualità di titolare non può essere liberamente determinata dai contraenti ma discende direttamente dai poteri che si esercitano sui dati. Può essere sia una persona fisica (si pensi all'imprenditore individuale) sia una persona giuridica (ad esempio, una società a responsabilità limitata) che tratta i dati (con la raccolta, la registrazione, la comunicazione degli stessi o la loro diffusione).

Il titolare del trattamento, se lo ritiene utile in base all'organizzazione aziendale, può designare uno o più soggetti come:

- responsabile del trattamento (data processor)ed è tenuto a vigilare sulla puntuale osservanza delle istruzioni impartite loro. La nomina deve essere effettuata con un atto scritto in cui siano precisati anche i compiti affidati. Occorre comunque scegliere persone fisiche od organismi (inclusi soggetti esterni all'impresa) che per esperienza, capacità e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, compreso il profilo relativo alla sicurezza.

- Gli incaricati del trattamento sono le persone fisiche che effettuano materialmente le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del titolare (o del responsabile se è stato nominato) secondo precise istruzioni. Per poter svolgere queste operazioni in maniera lecita, è necessario che il personale chiamato a trattare i dati venga opportunamente designato per iscritto individuando puntualmente l'ambito di trattamento consentito.

DATI AZIENDALI

Ragione sociale	KAMEC SRL
Attività economica	46.69.99 COMMERCIO ALL'INGROSSO DI MACCHINE E MACCHINARI PER DEFORMAZIONE LAMIERA
Legale Rappresentante	DI GIULIO ALESSANDRO
Indirizzo della sede attività	VIA VITTORIO EMANUELE III, 47 SORA (FR)
Il titolare del trattamento (data controller)	DI GIULIO ALESSANDRO
Incaricati del trattamento interni	DI GIULIO ALESSANDRO BARTESAGHI MARIA ELISABETTA • Tipologia di trattamento eseguito Amministratore di sistema • Incaricato Custodia Locali

2. Descrizione dell'attività lavorativa

La società Kamec S.r.l. si è costituita in Sora (FR) il 28/09/2020 ha sede legale in Via Vittorio Emanuele III, N. 47, codice fiscale e partita IVA : 03124390604 è regolarmente iscritta alla C.C.I.A.A .DI Frosinone dal 01/10/2020 con codice ADECO attribuito 46.69.99.

Kamec srl ha per oggetto l'attività di progettazione, costruzione, manutenzione, riparazione, noleggio e commercializzazione di macchine utensili e automazioni meccaniche nuove ed usate e in specie macchinari per deformazione lamiera.
La progettazione, costruzione e commercializzazione di presse, macchine ed impianti industriali di qualsiasi tipo e specie, il commercio e locazione degli stessi, la loro revisione nella sede e presso terzi.
Inoltre svolge attività di assistenza gestionale, economica, tecnica ed informatica alle imprese italiane ed estere, consistente in:

- Consulenza sulla gestione dei processi aziendali in ambito industriale, commerciale, logistico, e/o distributivo ed informatico;
- Indagini di mercato e consulenza nell'ambito del marketing e della pubblicità;
- Supporto nelle attività di sviluppo sui mercati italiani ed esteri in ambito industriale,

commerciale, logistico e/o distributivo ed informatico

- - La gestione dei depositi, servizi di logistica, la custodia e manutenzione di materiali, impianti

e macchinari di terzi.

La compagine sociale è la seguente:

- Di Giulio Alessandro con carica di rappresentante legale, amministratore, socio 30%
- Bartesaghi Maria Elisabetta, socio 70%

L'azienda inoltre si avvale di un ampio ed efficiente organico composto oltre che dalle suddette figure professionali anche da personale dipendente così suddiviso con mansioni diversificate, unitamente a proficue collaborazioni con imprese specializzate nel settore della meccanica

3. Introduzione alla sicurezza delle informazioni

La sicurezza delle informazioni comprende tutte le misure adottate per difendere le informazioni elaborate all'interno di un sistema (ad esempio elettronico, fisico) da accessi non autorizzati, uso, divulgazione, interruzione, modifica, esame, ispezione, registrazione o distruzione. Il modello più utilizzato per guidare lo sviluppo e l'implementazione di un framework per la gestione della sicurezza delle informazioni all'interno di un'organizzazione è rappresentato dalla cosiddetta triade della CIA: riservatezza, integrità e disponibilità delle informazioni.

• La riservatezza è definita come la "proprietà che permette di gestire le informazioni in modo che non siano rese disponibili o divulgate a individui, entità o processi non autorizzati". In pratica, tutte le misure implementate per garantire la riservatezza sono progettate per impedire l'accesso alle informazioni da parte di individui, entità o processi non autorizzati, garantendo nel contempo che gli individui, le entità o i processi autorizzati possano accedervi. Nella maggior parte dei casi le informazioni sono classificate in base alla quantità e al tipo di danno che potrebbe essere fatto se dovesse cadere in mani non intenzionali. Misure più o meno rigorose possono quindi essere implementate in base a queste categorie.

• L'integrità è definita come la proprietà di "accuratezza e completezza". In questo senso, l'integrità implica il mantenimento della coerenza, dell'accuratezza e dell'affidabilità delle informazioni lungo l'intero ciclo di vita. I dati non devono essere modificati durante il trasporto e devono essere prese misure per garantire che i dati non possano essere modificati da individui, entità o processi non autorizzati. Da un punto di vista pratico, ciò significa che i dati non possono essere modificati in modo non autorizzato o non individuato.

• La disponibilità è definita come la proprietà di "informazioni accessibili e utilizzabili quando una parte autorizzata lo richiede". Ciò significa che i sistemi utilizzati per memorizzare ed elaborare le informazioni, così come i canali di comunicazione delle informazioni, funzionano tutti correttamente. In pratica, ciò è assicurato al meglio dalla manutenzione dell'hardware senza compromessi, eseguendo immediatamente riparazioni dell'hardware quando necessario e mantenendo un ambiente operativo del sistema operativo correttamente privo di conflitti software.

Il processo di gestione del rischio comprende quattro fasi principali, come segue:

• Valutazione del rischio: può essere intesa come la generazione di un'istantanea dei rischi attuali. Un rischio è espresso in funzione della probabilità che un risultato avverso (minaccia) si verifichi moltiplicato per la grandezza del risultato avverso (impatto) qualora si verifichi. La valutazione del rischio inizia con l'identificazione delle minacce, seguita dalla determinazione
della pertinente probabilità e dell'impatto di ciascun rischio. Per valutare correttamente il rischio, bisogna prendere in considerazione allo stesso modo sia la probabilità che l'impatto.

• Trattamento del rischio: in base ai risultati della valutazione del rischio, in questa fase l'organizzazione seleziona e implementa misure di sicurezza per il trattamento dei rischi. Le misure possono avere effetti diversi, quali: mitigazione, trasferimento, elusione o conservazione dei rischi. Diverse misure di sicurezza di diversi tipi possono (e dovrebbero) essere utilizzate per trattare i rischi.

• Accettazione del rischio: anche quando i rischi sono stati trattati, i rischi residui rimarranno probabilmente (ad esempio a causa del fatto che alcuni controlli non sono fattibili). Questi rischi dovranno essere accettati. Questa è una decisione di gestione che deve seguire l'accettazione del modo in cui i rischi sono stati trattati.

• Comunicazione del rischio: tutte le parti interessate devono essere informate sui controlli adottati dai rischi e sui rischi accettati.

Al fine di garantire una corretta gestione del rischio si considerano le seguenti definizioni:

• La nozione di impatto: nel processo di valutazione del rischio "tipico", i rischi sono stimati in base al loro potenziale impatto per l'organizzazione. Nel caso del trattamento dei dati personali, tuttavia, gli impatti sono considerati in relazione alle libertà e ai diritti delle persone. Questa è una differenza significativa poiché modifica l'analisi degli impatti nei confronti dei possibili effetti negativi che un individuo può subire, tra cui ad esempio il furto di identità o la frode, la perdita finanziaria, danni fisici o psicologici, umiliazione, danni alla reputazione o addirittura minacce alla vita. Durante l'esecuzione di tale analisi, la scala (ad esempio il numero di individui affetti) potrebbe non essere pertinente: l'impatto è elevato anche se può portare gravi effetti avversi solo a una singola persona. Un'ulteriore sfida è che, al fine di calcolare l'impatto, è necessario prendere in considerazione anche eventuali effetti collaterali secondari sui diritti e le libertà delle persone.

• La gestione dei rischi: a causa della nozione di impatto specifica sulla privacy, il modo in cui i rischi identificati vengono gestiti può anche differire dal processo di valutazione del rischio "tipico". Pertanto, nella gestione dei rischi

di sicurezza per i dati personali, è stato prima di tutto importante definire il contesto generale del trattamento (ad es. Tipi di dati personali, finalità di trattamento, destinatari legittimi, ecc.), che supporterà quindi la definizione di possibili minacce e rischi basati sull'impatto sugli individui.
Verranno infine adottati adeguati controlli tecnici e organizzativi per gestire i rischi, tenendo conto delle specificità relative ai dati personali.

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Dati identificativi soggetto a cui appartiene il registro (TITOLARE)

Denominazione	**Di Giulio Alessandro**
Indirizzo	*Numero civico*
Provincia	FR *CAP* 03039
Città	SORA
Nazione	Italia
P.IVA / C.F.	/ **DGLLSN92C21I838C**
Data Fine Rapporto	N/A

Trattamento (Dati Clienti)

Descr. breve	Trattamento Dati Clienti
Sedi del trattamento	Vittorio Emanuele III 47 - Sora - 03039
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Data inizio incarico	22/02/2021
Data fine incarico	N/A
Finalità del trattamento	Adempimenti commerciali , contabili e fiscali Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
Categorie di dati trattati	Ragione Sociale/Cognome e Nome, Codice Fiscale ed altri numeri di identificazione, Coordinate Bancarie, Indirizzo, Indirizzo E-Mail , Numero di telefono/cellulare
Categorie di interessati	Consulenti e liberi professionisti, anche in forma associata
	Dipendenti, collaboratori, visitatori, persone che hanno accesso ai locali aziendali o che hanno consumato pasti o bevande previa registrazione e/o prenotazione
Data inizio del trattamento	22/02/2021
Durata del trattamento	10 Anno/i
Dati raccolti presso interessato	Si
Prevista profilazione	No
Relativo a minori	No
Relativo a minori di 14 anni	No
Il trattamento prevede il consenso degli interessati almeno per una finalità	Si

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Trattamento implementabile in base a valutazione DPIA	Non prevista/Effettuata
Il trattamento prevede la compilazione della PIA / DPIA	No
Fonte di raccolta dei dati trattati	N/A
Categoria di destinatari ai quali possono essere comunicati	Banche, camere di commercio, professionisti ai quali ci rivolgiamo per adempiere ad obblighi fiscali e legali
	Camere di commercio, industria, artigianato ed agricoltura
	Consulenti e liberi professionisti in forma singola o associata
	Istituti di credito.
	Uffici giudiziari
Destinatari ai quali i dati possono essere comunicati	Ministero economia e finanze Nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600)
Paese / Organizzazione estera dove i dati possono essere trasferiti	Non sono previsti trasferimenti verso paesi / organizzazioni estere.
Eccezioni al trattamento di dati ex. artt. 9/10	Non sono presenti eccezioni per le quali possono essere effettuati trattamenti di dati cosidetti "sensibili" in deroga a quanto previsto dall'art.9 del Regolamento Europeo.
Elenco Responsabili	
Denominazione Responsabile	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Asset (DELL DESKTOP-38O9BJS)	
Categoria	Hardware
Tipologia	Information Asset
Descrizione	
Data Acquisizione	22/02/2021
Data Dismissione	N/A
Responsabile / Soggetto autorizzato	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Liv. di riservatezza garantito	Alto
Liv. di integrità dei dati garantito	Alto

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Liv. di disponibilità dei dati garantito	Alto
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Rischio Accessi esterni non autorizzati (Medio)	
Vulnerabilità analizzata e valore	Mancanza procedure di accesso con credenziali (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Contromisura (Registrazione accessi)	
Autore dell'analisi	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Rischio Azione di virus informatici, ransomware e altri codici malevoli (Medio)	
Vulnerabilità analizzata e valore	Mancanza di software Antivirus, Antimalware, Antiransomware (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Contromisura (Antivirus)	
Autore dell'analisi	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Furto di apparecchiature o documenti (Medio)

Vulnerabilità analizzata e valore	Storage non protetto (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Sistema di allarme)

Autore dell'analisi	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Guasto di apparecchiature (Medio)

Vulnerabilità analizzata e valore	Manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Manutenzione periodica apparecchiature)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Malfunzionamento hardware (Medio)

Vulnerabilità analizzata e valore	Manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Assistenza)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Mancanza di alimentazione elettrica (Alto)

Vulnerabilità analizzata e valore	Sensibilità alle variazioni di tensione (Basso)

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Gruppo di continuità/stabilizzatore)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Ingressi non autorizzati a locali/aree ad accesso ristretto (Medio)

Vulnerabilità analizzata e valore	Mancata sorveglianza delle aree protette (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Spamming o tecniche di sabotaggio (Medio)

Vulnerabilità analizzata e valore	Mancanza di software antispam (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Contromisura (Antispam)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Trattamento illecito dei dati (Alto)

Vulnerabilità analizzata e valore	Assenza di procedure di monitoraggio delle strutture di elaborazione delle informazioni (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Formazione)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Trattamento (Dati Fornitori)	
Sedi del trattamento	Vittorio Emanuele III 47 - Sora - 03039
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Data inizio incarico	22/02/2021
Data fine incarico	N/A
Finalità del trattamento	Adempimenti commerciali , contabili e fiscali Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
Categorie di dati trattati	Ragione Sociale/Cognome e Nome, Codice Fiscale ed altri numeri di identificazione, Coordinate Bancarie, Indirizzo, Indirizzo E-Mail , Numero di telefono/cellulare
Categorie di interessati	Clienti o Utenti
	Dipendenti, collaboratori, visitatori, persone che hanno accesso ai locali aziendali o che hanno consumato pasti o bevande previa registrazione e/o prenotazione
	Consulenti e liberi professionisti, anche in forma associata
Data inizio del trattamento	22/02/2021
Durata del trattamento	10 Anno/i
Dati raccolti presso interessato	Si
Prevista profilazione	No
Relativo a minori	No
Relativo a minori di 14 anni	No
Il trattamento prevede il consenso degli interessati almeno per una finalità	Si
Trattamento implementabile in base a valutazione DPIA	Non prevista/Effettuata
Il trattamento prevede la compilazione della PIA / DPIA	No
Fonte di raccolta dei dati trattati	N/A
Categoria di destinatari ai quali possono essere comunicati	Banche, camere di commercio, professionisti ai quali ci rivolgiamo per adempiere ad obblighi fiscali e legali

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Destinatari ai quali i dati possono essere comunicati	Consulenti e liberi professionisti in forma singola o associata
	Enti governativi, professionisti ai quali ci rivolgiamo per adempiere agli obblighi previsti.
	Enti pubblici economici
	Ministero economia e finanze Nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600)
Paese / Organizzazione estera dove i dati possono essere trasferiti	Non sono previsti trasferimenti verso paesi / organizzazioni estere.
Eccezioni al trattamento di dati ex. artt. 9/10	Non sono presenti eccezioni per le quali possono essere effettuati trattamenti di dati cosidetti "sensibili" in deroga a quanto previsto dall'art.9 del Regolamento Europeo.

Elenco Responsabili

Denominazione Responsabile	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Trattamento (Dati necessari alla prevenzione dal contagio da COVID-19)

Descr. breve	Dati necessari alla prevenzione dal contagio da COVID-19, o alla verifica di possibili contatti con soggetti contagiati o asintomatici
Descr. estesa	Dati necessari alla prevenzione dal contagio da COVID-19, o alla verifica di possibili contatti con soggetti contagiati o asintomatici
Sedi del trattamento	Vittorio Emanuele III 47 - Sora - 03039
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Data inizio incarico	22/02/2021
Data fine incarico	N/A
Finalità del trattamento	Prevenzione dal contagio da COVID-19 Motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni; obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20)
	Tutela della salute delle persone in azienda, nel luogo di lavoro o nell'esercizio commerciale Motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni; obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20)
	Collaborazione con le autorità pubbliche e, in particolare le autorità sanitarie qualora si rendesse necessaria una verifica rispetto a possibili situazione di pericolo di diffusione del contagio Motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni; obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20)
Categorie di dati trattati	Temperatura corporea rilevata in tempo reale, senza registrazione o conservazione, salvo l'ipotesi in cui questo sia previsto
	Dati identificativi, registrazione del superamento della soglia di temperatura, questa solo qualora sia necessario documentare le ragioni che hanno impedito l'accesso ai locali aziendali o la permanenza negli stessi; nonchè, in tale caso, la registrazione dati relativi all'isolamento temporaneo, quali l'orario di uscita e le circostanze riferite dall'interessato a giustificazione dall'uscita dall'isolamento temporaneo
	Situazioni di pericolo di contagio da Covid-19, compresi dati relativi allo stato di salute, quali, a titolo esemplificativo, la temperatura corporea/sintomi influenzali; provenienza/non provenienza dalle zone a rischio epidemiologico; presenza/assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19
	Dati relativi allo stato di salute riguardanti la "avvenuta negativizzazione" del tampone Covid-19
Categorie di interessati	Dipendenti, collaboratori, visitatori, persone che hanno accesso ai locali aziendali o che hanno consumato pasti o bevande previa registrazione e/o prenotazione
Data inizio del trattamento	22/02/2021
Durata del trattamento	10 Anno/i
Dati raccolti presso interessato	Si

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Prevista profilazione	No
Relativo a minori	No
Relativo a minori di 14 anni	No
Il trattamento prevede il consenso degli interessati almeno per una finalità	Si
Trattamento implementabile in base a valutazione DPIA	Non prevista/Effettuata
Il trattamento prevede la compilazione della PIA / DPIA	No
Fonte di raccolta dei dati trattati	N/A
Categoria di destinatari ai quali possono essere comunicati	DEST_1 I dati possono essere conosciuti da autorizzati al trattamento; da designati al trattamento e in particolare dal responsabile dell'ufficio del personale; dal medico competente.
	DEST_2 I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità Sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore/avventore risultato positivo al COVID-19).I dati possono essere comunicati alle pubbliche autorità che li dovessero chiedere.
	DEST_3 I dati non sono trasferiti all'estero e non si effettuano profilazioni o decisioni automatizzate.
Destinatari ai quali i dati possono essere comunicati	ASL Aggiornamento del registro delle cause di morte
	ASL ed Aziende ospedaliere Trasmissione delle informazioni, di carattere sanitario, relative all'interessato
	Autorità giudiziaria Avviamento delle procedure di ricovero relative ai soggetti interdetti o inabilitati
	INAIL Verifica della liquidazione in caso di equo indennizzo ai sensi del d.P.R. n. 1124/1965
	Ministero economia e finanze Nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600)
Paese / Organizzazione estera dove i dati possono essere trasferiti	Non sono previsti trasferimenti verso paesi / organizzazioni estere.
Eccezioni al trattamento di dati ex. artt. 9/10	Archiviazione nel pubblico interesse Archiviazione nel pubblico interesse

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Elenco Responsabili	
Denominazione Responsabile	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Soggetti Autorizzati	
Anagrafica	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Tipo incarico	Soggetto autorizzato generico
Data Inizio Incarico	22/02/2021
Data Fine Incarico	
Data Fine Rapporto	
Permessi	Lettura, Modifica, Inserimento, Cancellazione, Stampa, Manutenzione
Asset (DELL DESKTOP-38O9BJS)	
Categoria	Hardware
Tipologia	Information Asset
Descrizione	
Data Acquisizione	22/02/2021
Data Dismissione	N/A
Responsabile / Soggetto autorizzato	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Liv. di riservatezza garantito	Alto
Liv. di integrità dei dati garantito	Alto
Liv. di disponibilità dei dati garantito	Alto
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Rischio Accessi esterni non autorizzati (Medio)	
Vulnerabilità analizzata e valore	Mancanza procedure di accesso con credenziali (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021
Contromisura (Registrazione accessi)	

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Autore dell'analisi	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Azione di virus informatici, ransomware e altri codici malevoli (Medio)

Vulnerabilità analizzata e valore	Mancanza di software Antivirus, Antimalware, Antiransomware (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Antivirus)

Autore dell'analisi	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Furto di apparecchiature o documenti (Medio)

Vulnerabilità analizzata e valore	Storage non protetto (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Sistema di allarme)

Autore dell'analisi	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Guasto di apparecchiature (Medio)

Vulnerabilità analizzata e valore	Manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Manutenzione periodica apparecchiature)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Malfunzionamento hardware (Medio)

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Vulnerabilità analizzata e valore	Manutenzione insufficiente e/o installazione difettosa dei supporti di memorizzazione (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Assistenza)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Mancanza di alimentazione elettrica (Alto)

Vulnerabilità analizzata e valore	Sensibilità alle variazioni di tensione (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Gruppo di continuità/stabilizzatore)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Ingressi non autorizzati a locali/aree ad accesso ristretto (Medio)

Vulnerabilità analizzata e valore	Mancata sorveglianza delle aree protette (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Spamming o tecniche di sabotaggio (Medio)

Vulnerabilità analizzata e valore	Mancanza di software antispam (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Antispam)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Rischio Trattamento illecito dei dati (Alto)

Vulnerabilità analizzata e valore	Assenza di procedure di monitoraggio delle strutture di elaborazione delle informazioni (Basso)
Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Data analisi del rischio	22/02/2021
Probabilità verifica minaccia	Mai verificatosi ma possibile
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

Contromisura (Formazione)

Autore dell'analisi	Alessandro Di Giulio codice fiscale DGLLSN92C21I838C
Data compilazione	22/02/2021
Descrizione breve	
Descrizione	
Data adozione	22/02/2021
Data prossima verifica	22/02/2021
Stato adozione	Adottata
Data creazione	22/02/2021
Data ultimo aggiornamento	22/02/2021

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Trattamento (Dati personali dei Lavoratori)	
Sedi del trattamento	Vittorio Emanuele III 47 - Sora - 03039
Data creazione	21/02/2021
Data ultimo aggiornamento	21/02/2021
Data inizio incarico	22/02/2021
Data fine incarico	N/A
Finalità del trattamento	Gestione del personale Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
	Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso l'ente Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
	Trattamento giuridico ed economico del personale Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso
Categorie di dati trattati	Dati biometrici
	Certificati di qualità professionali
	Cognome, nome, Data Arrivo, sesso,data di Nascita,Comune di nascita,Provincia di Nascita,Stato di Nascita,Tipo Documento, Numero Documento, Luogo rilascio documento
	Indirizzo e-mail
	Coordinate bancarie
	Cognome e Nome, CF, Indirizzo, E-mail, Telefono/cellulare, Coordinate Bancarie, Adesione a Sindacati, Attività sindacale, Appartenenza a categorie protette, Composizione nucleo familiare, Dati reddituali, Stato di malattia/infortunio/maternità
	Situazioni di pericolo di contagio da Covid-19, compresi dati relativi allo stato di salute, quali, a titolo esemplificativo, la temperatura corporea/sintomi influenzali; provenienza/non provenienza dalle zone a rischio epidemiologico; presenza/assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19
	Dati relativi allo stato di salute riguardanti la "avvenuta negativizzazione" del tampone Covid-19
	Idoneità al lavoro
Categorie di interessati	Consulenti e liberi professionisti, anche in forma associata
Data inizio del trattamento	22/02/2021
Durata del trattamento	10 Anno/i
Dati raccolti presso interessato	Si
Prevista profilazione	No
Relativo a minori	No

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Registro delle attività di trattamento

(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

Relativo a minori di 14 anni	No
Il trattamento prevede il consenso degli interessati almeno per una finalità	Si
Trattamento implementabile in base a valutazione DPIA	Non prevista/Effettuata
Il trattamento prevede la compilazione della PIA / DPIA	No
Fonte di raccolta dei dati trattati	N/A
Categoria di destinatari ai quali possono essere comunicati	Consulenti e liberi professionisti in forma singola o associata
	DEST_1 I dati possono essere conosciuti da autorizzati al trattamento; da designati al trattamento e in particolare dal responsabile dell'ufficio del personale; dal medico competente.
	DEST_2 I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità Sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore/avventore risultato positivo al COVID-19).I dati possono essere comunicati alle pubbliche autorità che li dovessero chiedere.
	DEST_3 I dati non sono trasferiti all'estero e non si effettuano profilazioni o decisioni automatizzate.
Destinatari ai quali i dati possono essere comunicati	INAIL Verifica della liquidazione in caso di equo indennizzo ai sensi del d.P.R. n. 1124/1965
	INPS Fini assistenziali e previdenziali, nonché per rilevazione di eventuali patologie o infortuni sul lavoro
	ISTAT Rilevazioni annuali della cause di morte
Paese / Organizzazione estera dove i dati possono essere trasferiti	Non sono previsti trasferimenti verso paesi / organizzazioni estere.
Eccezioni al trattamento di dati ex. artt. 9/10	Non sono presenti eccezioni per le quali possono essere effettuati trattamenti di dati cosidetti "sensibili" in deroga a quanto previsto dall'art.9 del Regolamento Europeo.
Elenco Responsabili	
Denominazione Responsabile	Maria Elisabetta Bartesaghi codice fiscale BRTMLS66C65D416I

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Valutazione Rischio Trattamento

Trattamento Dati necessari alla prevenzione dal contagio da COVID-19

Dati necessari alla prevenzione dal contagio da COVID-19, o alla verifica di possibili contatti con soggetti contagiati o asintomatici

Categoria Dati

Tipo Dato	Categoria
Dati comuni e sensibili	Temperatura corporea rilevata in tempo reale, senza registrazione o conservazione, salvo l'ipotesi in cui questo sia previsto
Dati comuni e sensibili	Dati identificativi, registrazione del superamento della soglia di temperatura, questa solo qualora sia necessario documentare le ragioni che hanno impedito l'accesso ai locali aziendali o la permanenza negli stessi; nonchè, in tale caso, la registrazione dati relativi all'isolamento temporaneo, quali l'orario di uscita e le circostanze riferite dall'interessato a giustificazione dall'uscita dall'isolamento temporaneo
Dati comuni e sensibili	Situazioni di pericolo di contagio da Covid-19, compresi dati relativi allo stato di salute, quali, a titolo esemplificativo, la temperatura corporea/sintomi influenzali; provenienza/non provenienza dalle zone a rischio epidemiologico; presenza/assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19
Dati comuni e sensibili	Dati relativi allo stato di salute riguardanti la "avvenuta negativizzazione" del tampone Covid-19

Finalità

Finalità	Criterio di Liceità	Normativa Di Riferimento
Prevenzione dal contagio da COVID-19	Motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni; obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20)	Normativa Nazionale

Tutela della salute delle persone in azienda, nel luogo di lavoro o nell'esercizio commerciale	Motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni; obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20)	Normativa Nazionale
Collaborazione con le autorità pubbliche e, in particolare le autorità sanitarie qualora si rendesse necessaria una verifica rispetto a possibili situazione di pericolo di diffusione del contagio	Motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni; obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20)	Normativa Nazionale

Asset

Nome	Categoria	Tipologia	Descrizione
DELL DESKTOP-38O9BJS	Hardware	Information Asset	

Luogo Trattamento

Anagrafica	Ruolo	Indirizzo
Di Giulio Alessandro	Titolare	Non Presente
Bartesaghi Maria Elisabetta	Responsabile	Non Presente

Interessati

Categoria	Note
Dipendenti, collaboratori, visitatori, persone che hanno accesso ai locali aziendali o che hanno consumato pasti o bevande previa registrazione e/o prenotazione	

Destinatari

Categoria/Destinatario	Descrizione
DEST_1	I dati possono essere conosciuti da autorizzati al trattamento; da designati al trattamento e in particolare dal responsabile dell'ufficio del personale; dal medico competente.

DEST_2	I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità Sanitaria per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore/avventore risultato positivo al COVID-19).I dati possono essere comunicati alle pubbliche autorità che li dovessero chiedere.
DEST_3	I dati non sono trasferiti all'estero e non si effettuano profilazioni o decisioni automatizzate.
ASL	Aggiornamento del registro delle cause di morte
ASL ed Aziende ospedaliere	Trasmissione delle informazioni, di carattere sanitario, relative all'interessato
Autorità giudiziaria	Avviamento delle procedure di ricovero relative ai soggetti interdetti o inabilitati
INAIL	Verifica della liquidazione in caso di equo indennizzo ai sensi del d.P.R. n. 1124/1965
Ministero economia e finanze	Nel caso in cui l'ente svolga funzioni di centro assistenza fiscale (ai sensi dell'art. 17 del d.m. 31.05.1999, n. 164 e nel rispetto dell'art. 12 bis del d.P.R. 29.09.1973, n. 600)

Valutazione Impatto

Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.

Basso

Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.

Basso

Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.

Basso

L'impatto finale Impostato della minaccia è: Basso

Valutazione Probabilita

RISORSE DI RETE E TECNICHE

Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?

NO

È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?

NO

Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?

NO

Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?

NO

Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?

NO

PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI

I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?

NO

L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?

NO

I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?

NO

I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?

NO

Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro?

NO

PARTI/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?

NO

Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore/terza parte (responsabile del trattamento)?

NO

Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?

NO

Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?

NO

Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?

NO

SETTORE DI OPERATIVITÀ E SCALA DI TRATTAMENTO

Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?

NO

La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?

NO

Hai ricevuto notifiche e/o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?

NO

Un'operazione di elaborazione riguarda un grande volume di individui e/o dati personali?

NO

Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?

NO

La probabilità di occorrenza finale Impostata della minaccia è: Basso

Valutazione Rischio

Probabilità \ Impatto	Basso	Medio	Alto/Molto Alto
Basso	X		
Medio			
Alto/Molto Alto			

La valutazione finale Impostata del rischio è: *Basso Basso*

Misure di Sicurezza

KAMEC s.r.l.
Via Vittorio Emanuele III, 47 | 03039 Sora (FR)
P.IVA - C.F 03124390604 | BA6ET11
+39 388 4359030
info@kamecsrl.com - service@kamecsrl.com

Livello	Categoria	Descrizione	Cod. Iso 27001	Data Adozione	Data Verifica	Note
Basso	Politica di sicurezza e procedure per la protezione dei dati personali	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	A.5 Politica di sicurezza			
Basso	Politica di sicurezza e procedure per la protezione dei dati personali	La politica di sicurezza dovrebbe essere revisionata erivista, se necessario, su base annuale.	A.5 Politica di sicurezza			
Basso	Ruoli e responsabilità	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni			
Basso	Ruoli e responsabilità	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni			

Basso	Politica di controllo degli accessi	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati .	A.9.1.1 Politica di controllo degli accessi			
Basso	Gestione risorse/asset	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	A.8 Asset management			
Basso	Gestione risorse/asset	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	A.8 Asset management			

Basso	Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	A. 12.1 Procedure operative e responsabilità			
Basso	Gestione delle operazioni di sviluppo software e dei test di sviluppo	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	A. 12.1 Procedure operative e responsabilità			

Basso	Responsabili del trattamento	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori/outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	A.15 Rapporti con i fornitori			
Basso	Responsabili del trattamento	Al rilevamento di una violazione dei dati personali (databreach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	A.15 Rapporti con i fornitori			

Basso	Responsabili del trattamento	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	A.15 Rapporti con i fornitori			
Basso	Gestione degli incidenti/Violazione dei dati personali (Personal databreaches)	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni			
Basso	Gestione degli incidenti/Violazione dei dati personali (Personal databreaches)	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna.. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	A.16 Gestione degli incidenti sulla sicurezza delle informazioni			

Basso	Business continuity	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente/violazione di dati personali).	A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa			
Basso	Obblighi di confidenzialità imposti al personale	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione .	A.7 Sicurezza delle risorse umane			

Basso	Formazione	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione			
Basso	Controllo degli accessi e autenticazione	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	A.9 Controllo degli accessi			
Basso	Controllo degli accessi e autenticazione	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	A.9 Controllo degli accessi			

Basso	Controllo degli accessi e autenticazione	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente/password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	A.9 Controllo degli accessi			
Basso	Controllo degli accessi e autenticazione	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	A.9 Controllo degli accessi			
Basso	Generazione di file di log e monitoraggio	Dovrebbero essere generati file di log per ogni sistema/applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	A.12.4 Registrazione e monitoraggio			
Basso	Generazione di file di log e monitoraggio	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento	A.12.4 Registrazione e monitoraggio			

Basso	Sicurezza di Server e Database	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	A. 12 Operations security			
Basso	Sicurezza di Server e Database	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR) .	A. 12 Operations security			
Basso	Sicurezza delle Postazioni di lavoro	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione			
Basso	Sicurezza delle Postazioni di lavoro	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione			
Basso	Sicurezza delle Postazioni di lavoro	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione			
Basso	Sicurezza delle Postazioni di lavoro	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione			

Basso	Sicurezza delle Postazioni di lavoro	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	A. 14.1 Requisiti di sicurezza dei sistemi di informazione			
Basso	Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica	Ogni volta che l'accesso viene eseguito tramite Internet , la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	A.13 Communications Security			
Basso	Back-ups	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	A.12.3 Back-Up			
Basso	Back-ups	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	A.12.3 Back-Up			
Basso	Back-ups	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	A.12.3 Back-Up			
Basso	Back-ups	I backup completi devono essere eseguiti regolarmente.	A.12.3 Back-Up			
Basso	Dispositivi mobili/ portatili	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	A. 6.2 Dispositivi mobili e teleworking			

Basso	Dispositivi mobili/ portatili	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	A. 6.2 Dispositivi mobili e teleworking			
Basso	Dispositivi mobili/ portatili	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	A. 6.2 Dispositivi mobili e teleworking			
Basso	Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto			
Basso	Sicurezza del ciclo di vita delle applicazioni	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto			
Basso	Sicurezza del ciclo di vita delle applicazioni	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto			

Basso	Sicurezza del ciclo di vita delle applicazioni	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto			
Basso	Sicurezza del ciclo di vita delle applicazioni	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.	A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto			
Basso	Cancellazione/ eliminazione dei dati	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.	A. 8.3.2 Smaltimento di supporti e 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura			
Basso	Cancellazione/ eliminazione dei dati	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	A. 8.3.2 Smaltimento di supporti e 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura			
Basso	Sicurezza fisica	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	A.11 - Sicurezza fisica e ambientale			

6.Minacce

Minacce a cui sono sottoposte le risorse hardware
Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

Minacce a cui sono sottoposte le risorse connesse in rete
Le principali minacce alle risorse connesse in rete possono provenire dall'interno, dall'esterno o da una combinazione interno/esterno e sono relative:

- all'utilizzo della LAN/Intranet (interne);
- ai punti di contatto con il mondo esterno attraverso Internet (esterne);
- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

IP spoofing
L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo
spoofing si manifesta come attività di “falsificazione” di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Packet sniffing
Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina “obiettivo” sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

Port scanning
Serie programmata di tentativi di accesso diretti a evidenziare, in base alle “risposte” fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una “intrusione”. Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

Highjacking
Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.

Social engineering
Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

Buffer overflow
Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

Spamming
Saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.

Password cracking
Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

Trojan
Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

Worm
Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

Logic bomb
Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

Malware e MMC (Malicious Mobile Code)
Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

DOS (Denial of Service)
Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.
DDOS (Distributed Denial of Service)
Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete.

7.Strumento di memorizzazione

Descrizione sintetica	Dispositivi di accesso
Anagrafica ed informazioni varie dipendenti	Cartaceo PC
CUD e paghe dipendenti	Cartaceo PC
Dichiarazione dei redditi	Cartaceo PC
Documenti per adempimenti contabili e fiscali	Cartaceo PC
Fatture acquisto fornitori	Cartaceo PC
Fatture vendita clienti	Cartaceo PC
Rubrica indirizzi posta elettronica	Cartaceo PC
Rubrica indirizzi e numeri telefono	Cartaceo PC

Archivi cartacei

Vengono trattati e/o conservati i documenti che possono contenere dati personali degli Interessati. L'archivio cartaceo viene comunque gestito nel pieno rispetto delle idonee misure di sicurezza in relazione al tipo di documentazione in esso contenuta. Gli eventuali atti e documenti contenenti dati personali sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. L'accesso agli archivi è controllato e consentito solo agli incaricati a ciò espressamente autorizzati. Quando gli archivi non sono dotati di strumenti per il controllo degli accessi, le persone che vi accedono sono preventivamente autorizzate. La documentazione viene conservata all'interno di armadi con serratura.

8.Trattamenti affidati all'esterno

L'obiettivo di questa sezione è la redazione di un quadro sintetico delle attività trasferite a terzi che comportano il trattamento dei dati personali.
Il titolare dell'azienda a cui le attività sono affidate dichiara di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali, e come tali sono soggetti all'applicazione del codice della protezione dei dati personali.
Il titolare dichiara di ottemperare agli obblighi previsti dal codice per la protezione dei dati personali.
Il titolare si impegna a relazionare sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Attività esternalizzate

Soggetto Esterno incaricato	Descrizione sintetica	Attività delegata
Salvatori Rosalba	Consulenza contabile e fiscale	Contabilità generale, adempimenti contabili e fiscali
Mauro Visca	Consulenza del Lavoro	Buste paga, uniemens, 770, cud
Unipol sai	Assicurazioni	Polizze assicurative
Nitro Vittorio	Medico del lavoro	Visite Mediche

Gestione, custodia e aggiornamento della parola chiave (Password)

Il PC è protetto da una username e password , così come per l'accesso ai server , che rispetta i requisiti minimi di complessità (8 caratteri alfanumerici con lettere maiuscole e minuscole) e che viene regolarmente cambiata ogni 90 giorni.
La password di accesso presenta le seguenti caratteristiche:

A) Non corrisponde al nome utente o ai dati personali dell'utente
B) Ha una lunghezza di almeno otto caratteri alfa-numerici
C) Non corrisponde ad una semplice parola rintracciabile in un dizionario
D) Non contiene riferimenti agevolmente riconducibili all'Incaricato

9.Istruzione operativa per la protezione dei personal computer e supporti di memoria portatili

La seguente istruzione operativa intende dare indicazioni sulle modalità più appropriate per proteggere dati personali, archiviati su supporti informatizzati portatili, come personal computer portatili, o supporto di memoria asportabile, in modo da garantire:

- Protezione contro la perdita fisica dell'apparato
- Protezione contro accesso non autorizzato ai dati
- Copia di rispetto di dati archiviati sull'apparato
- Trasferimento controllato e sicuro dei dati dall'apparato portatile alla rete informatica aziendale.

La protezione contro la sottrazione o smarrimento

Purtroppo la sottrazione di personal computer o supporto di memoria asportabile è assai frequente, sia perché esso può essere dimenticato, sia perché può essere facilmente sottratto, se lasciato incustodito.
Anche la copertura assicurativa contro il furto copre soltanto il valore commerciale della macchina e non dei dati che contiene.
Ecco la ragione per la quale la miglior protezione contro la sottrazione o smarrimento di un personal computer portatile sta in una estrema attenzione alla sua vulnerabilità, ed all'utilizzo sistematico di normali procedure cautelative.
Ad esempio:
-l'utilizzo sistematico di piccoli lacci in acciaio, con serratura. Molti personal computer portatili sono già predisposti per l'aggancio di questo dispositivo di sicurezza.
Si raccomanda inoltre di non lasciare mai incustodito il personal computer, ma di porlo nella apposita cassaforte o comunque metterlo in un armadio chiuso a chiave.
Il personal computer non deve mai esser lasciato abbandonato in una sala di attesa, deve essere tenuto legato alle proprie valigie e, in linea generale, deve essere sempre messo in un ricettacolo sicuro, quando viene abbandonato, anche temporaneamente, fuori dell'azienda ed anche all'interno della azienda, durante periodi di minor presidio.

Protezione contro l'accesso non autorizzato

Se un personal computer portatile o supporto di memoria asportabile è rubato o smarrito, il vero problema non è tanto nel valore della macchina, ma nell'informazioni che contiene.
È perciò necessario rendere quest'informazione non accessibile a soggetti non autorizzati.
Come noto, l'utilizzo delle parole chiave fornisce un certo livello di controllo dell'accesso, ma solo se esse vengono utilizzate sistematicamente e vengono periodicamente aggiornate.
Per applicazioni particolarmente critiche, si consiglia all'incaricato di prendere contatto con il proprio responsabile del trattamento di dati personali, per esaminare congiuntamente la possibilità di utilizzare dispositivi biometrici, che oggi possono essere applicati con relativa facilità anche a computer portatili.
È probabile che nel giro di qualche anno i dispositivi biometrici verranno messi a disposizione direttamente dal fabbricante dei computer portatili, ma per adesso è richiesta la installazione di un dispositivo supplementare, di costo contenuto ed utilizzo oltremodo facile.
Tra le varie tecnologie disponibili, una delle più semplici e di più facile utilizzo è composta da un piccolo dispositivo, che si collega tramite porta USB direttamente al computer portatile, e che permette di leggere l'impronta digitale dell'incaricato del trattamento, abilitato all'utilizzo delle personal computer portatile.

La realizzazione di copie di backup

È indispensabile effettuare con frequenza copie di backup dei dati, archiviati su personal computer portatili o supporto di memoria asportabile.
Le tecniche da utilizzare per i personal computer portatili non sono molto diverse da quelle che vengono utilizzate per garantire la salvaguardia dei dati, archiviati nel sistema informativo aziendale.
Esistono già numerose soluzioni che vengono offerte dagli specialisti di software, come ad esempio la possibilità di salvare su una area separata del disco tutte le variazioni incrementali che sono state eseguite, scaricandole automaticamente alla prima connessione possibile.

Inoltre, il tempo richiesto per effettuare dei backup viene molto ridotto quando vengono usate delle tecniche di compressione, che contribuiscono ad una maggiore facilità d'uso da parte dell'utente.
Nella procedura di backup per i dati presenti su personal computer portatili, occorre prendere in esame la possibilità di effettuare backup e singoli, oppure una copia completa dei dati presenti.
Fra le varie procedure, bisogna anche attivare quella relativa alla possibilità di effettuare una copia completa di tutti i dati presenti, per fronteggiare eventuali situazioni di emergenza.
Tutti i fabbricanti di personal computer mettono a disposizione dei CD, che devono essere utilizzati per avviare la procedura di recupero dei dati, nel caso si siano verificate delle anomalie di trattamento.
Non bisogna però dimenticare che i CD possono permettere di ripristinare il sistema operativo ed altri file essenziali, ma non le applicazioni e i dati personali archiviati.

Attenzione alle reti senza fili

È indispensabile che l'utilizzo di reti senza fili venga controllato, di concerto con il responsabile del trattamento, per essere certi che le protezioni informatiche siano attive ed evitare quindi la possibilità che, in fase di colloquio attraverso la rete senza fili, i dati personali in transito possono essere intercettati da soggetti non autorizzati.
Oggi sono disponibili numerose tecniche di sicurezza per le reti senza fili, che comprendono degli applicativi crittografici di grande resistenza.
Si faccia anche attenzione che i problemi da risolvere non riguardano soltanto la protezione del dato in transito, ma anche l'autenticazione dell'utente.
Per una rassegna di queste problematiche e per avere indicazioni precise, si raccomanda di non attivare il collegamento su reti senza fili, se non si sono prima presi appropriati provvedimenti protettivi.

Riepilogo

Diamo di seguito un riepilogo sommario delle più importanti misure di sicurezza da adottare, in caso di utilizzo di strumenti informatizzati portatili.

- Utilizzate sempre il codice identificativo personale e le parole chiave, cambiandole ogni qual volta abbiate la sensazione che esse non ne siano sufficientemente sicuro; laddove possibile, utilizzate sempre almeno 8 caratteri, mescolando caratteri maiuscoli e minuscoli.
- La parola chiave deve essere preferibilmente priva di significato e non deve mai essere comunicata a soggetti terzi, anche se fiduciari.
- Ricordate che in caso di trattamento di dati sensibili la parola chiave deve essere cambiata almeno ogni tre mesi, e se questo intervallo viene ridotto, tanto meglio.
- Si raccomanda di evitare di utilizzare la stessa parola chiave sia sui computer portatili che su quelli fissi.
- Accertatevi di effettuare con frequenza la copia di backup dei dati archiviati sul personal computer portatile o supporto di memoria asportabile, sia trasferendoli su supporti informatizzati portatili.
- In questo caso, si faccia attenzione a che le modalità di custodia di questi supporti portatili debbono essere simili a quelle applicate al computer portatile principale.
- Non tenete mai insieme la copie di backup ed il personal computer, per evitare che un eventuale furto possa coinvolgere sia i dati del personal computer portatile, che quelli di backup.
- Tutte le precauzioni che vengono prese all'interno della azienda per filtrare virus e messaggi di posta elettronica non autorizzati potrebbero non essere attive, quando il personal computer viene collegato a una presa telefonica di un albergo. Si faccia quindi particolare attenzione, quando ci si collega ad Internet attraverso reti non dotate di appropriati filtri, al tipo di messaggio che viene ricevuto.
- Ci si accerti che il software anti virus, presente sul personal computer portatile, sia costantemente aggiornato.
- Ci si accerti che il sistema operativo ed altri applicativi residenti siano sempre aggiornati e che il firewall,se presente, abbi un profilo di attività aggiornato
- Quando ci si collega ad Internet, la prima operazione da fare è sempre quella di aggiornare il software anti virus , il software di base ed i software applicativi residenti; successivamente procedere con altre operazioni
- Se scoprite che il vostro personal computer è infetto da virus, chiedete subito istruzioni al responsabile del trattamento sugli interventi da attuare, e non effettuate ulteriori elaborazioni.
- Collegatevi regolarmente al sito Internet del venditore degli applicativi residenti su personal computer portatile, in modo da avere sempre a disposizione gli ultimi aggiornamenti, che molto spesso sono mirati non solo a migliorare la flessibilità d'uso dell'applicativo, ma anche e soprattutto la sua sicurezza.
- Non lasciate mai il personal computer collegato ad Internet senza il vostro presidio; anzi, cercate di tenervi collegati soltanto per il minimo tempo necessario per effettuare le operazioni desiderate.
- Non permettete ad alcuna persona, anche di fiducia, di accedere al vostro personal computer portatile.
- Esaminate, con il responsabile del trattamento, l'opportunità di installare un firewall anche sul personal computer portatile. Questi dispositivi, se impostati correttamente e regolarmente aggiornati, possono offrire un contributo determinante alla sicurezza da intrusioni non autorizzate.