Ladisa S.R.L.
Via Guglielmo Lindemann 5/3 – 5/4 Bari (BA)
Pec: ladisa.ristorazione@legalmail.it
https://www.ladisaristorazione.it

MANUALE PROTEZIONE DEI DATI PERSONALI

ED.01 – REV. 01

AGGIORNATO AI SENSI DEL RGPD – 26/10/2026

Il presente documento racchiude le politiche, procedure, valutazioni, istruzioni che la Ladisa Srl intende promuovere al suo interno e rispettare nell'ambito della protezione dei dati personali trattati, in accordo con il Reg. UE 679/2016

SOMMARIO

Indice dei contenuti

1. POLITICA ____ 1
NECESSITÀ DI UNA POLITICA PER IL TRATTAMENTO DEI DATI PERSONALI ____ 1
SICUREZZA DEL TRATTAMENTO ____ 1
NOMINE ____ 2
REGISTRO DEI TRATTAMENTI ED ANALISI DEI RISCHI ____ 3
2. GLOSSARIO ____ 5
3. DIRITTI DELL'INTERESSATO ____ 10
PROCEDURE ____ 11
INFORMATIVA ____ 11
ACCESSO AI DATI ____ 11
RETTIFICA ____ 13
CANCELLAZIONE ____ 14
LIMITAZIONE ____ 15
PORTABILITÀ ____ 16
4. PROCESSO DI GESTIONE DEL RISCHIO ____ 18
CONTESTO ____ 18
CENTRO COTTURA ____ 18
UFFICI ____ 18
ZONA ESTERNA ____ 19
PROCESSI AZIENDALI ____ 19
FASE 1: ANALISI DEI TRATTAMENTI E REQUISITI ____ 21
Attività preliminari alla conduzione dell'analisi dei rischi ____ 22
FASE 2 ANALISI ____ 23
Identificazione dei rischi ____ 24
Classificazione delle informazioni ____ 24
Attività di analisi del rischio ____ 25
Ponderazione dei rischi ____ 27
Criterio di accettabilità ____ 27
FASE 3: TRATTAMENTO DEI RISCHI ____ 28

SOMMARIO

FASE 4: MONITORING, ADEGUAMENTO E MIGLIORAMENTO 32
FASE 5: CULTURA DELLA SICUREZZA 32
5. CONSERVAZIONE DEI DATI E GESTIONE DEGLI ARCHIVI 34
6. GESTIONE EVENTI ED INCIDENTI SULLA SICUREZZA PER LA PRIVACY E DATA BREACH 37
PROCEDURA DI NOTIFICAZIONE IN CASO DI INCIDENTE DI SICUREZZA 37
SCOPO E CAMPO DI APPLICAZIONE 38
DEFINIZIONI E AMBITO DI APPLICAZIONE 39
Definizioni 39
Ambito di applicazione 39
RESPONSABILITÀ 41
Incident Manager 41
Incident Response Team 41
MODALITÀ OPERATIVE 42
Segnalazione da parte di dipendenti e fornitori 42
Segnalazione in arrivo da parte degli interessati 42
Presa in carico, valutazione e Comunicazione 42
Risoluzione incidente 44
7. RESPONSABILE PROTEZIONE DATI PERSONALI 46
7.1 CONSIDERAZIONI INIZIALI 46
7.2 VALUTAZIONE SULLE NECESSITÀ DI NOMINARE UN RPD 46
7.3 CONOSCENZE E COMPETENZE RPD 48
8. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA 51
8.1 CONSIDERAZIONI INIZIALI 51
8.2 TRATTAMENTI EFFETTUATI DALL'AZIENDA E NECESSITÀ DI PROCEDERE AD UNA VALUTAZIONE DI IMPATTO 51
9. VIDEOSORVEGLIANZA E RAPPORTO DI LAVORO 52
10. UTILIZZO DELL'INTELLIGENZA ARTIFICIALE 52
11. INFORMAZIONI SULLA SOCIETA' 61

1. POLITICA

NECESSITÀ DI UNA POLITICA PER IL TRATTAMENTO DEI DATI PERSONALI

Ladisa S.r.l. è un'azienda di ristorazione che si colloca tra i principali players del settore: si occupa di ristorazione collettiva (scolastica, socio-sanitaria, militare, istituzionale, aziendale), ristorazione commerciale (gestione bar e punti ristoro), commercializzazione di derrate alimentari, banqueting. L'azienda progetta e realizza cucine industriali e opera anche nel settore del global service (manutenzione e pulizia).

Ladisa srl produce oggi oltre 22 milioni di pasti e dà lavoro a circa 4000 persone, è presente in Scuole, Università, Ospedali, Ministeri, Forze dell'Ordine, Forze Armate, Enti pubblici in genere. L'azienda presente da Sud a Nord in 17 regioni servendo complessivamente oltre 700 strutture in tutta Italia.

Ladisa S.R.L. (*di seguito l'azienda o l'organizzazione*) riconosce l'importanza della protezione del dato personale in quanto lo stesso è riferibile ad una persona fisica; ciò premesso assicurando una protezione al dato personale si protegge, in definitiva, la persona stessa a cui i dati personali si riferiscono.

In tal senso l'azienda si impegna a considerare in ogni suo processo aziendale di nuova formazione la politica sul rispetto della privacy come centrale, in modo da assicurare il principio di privacy by design; si impegna, inoltre, a rivedere e rielaborare continuamente i workflow aziendali, per rispettare il principio di privacy by default, e quindi, prendere come principale parametro di riferimento circa l'efficienza, efficacia ed utilità dei suddetti workflow per la protezione dei dati personali.

La politica del trattamento dati personali è contenuta, inoltre, nel documento:
"POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E DELLA PRIVACY".

SICUREZZA DEL TRATTAMENTO

L'azienda opera in contesti alquanto eterogenei che possono essere sintetizzati in: "*progettazione ed erogazione di servizi di ristorazione collettiva per enti pubblici e privati: mense scolastiche, sanitarie, militari e della pubblica sicurezza. preparazione, confezionamento in monoporzione e multiporzione, trasporto e distribuzione pasti. gestione bar, tavola calda, gastronomia da asporto. lavorazione, produzione, confezionamento, vendita e preparazione di carne e prodotti a base di carne fresca. produzione di piatti pronti. piattaforma centralizzata per acquisto, trasporto, distribuzione e commercializzazione di merci (no food) e derrate alimentari per la ristorazione collettiva e la grande distribuzione organizzata. erogazione dei servizi di derattizzazione, disinfestazione, pulizia civile ed igiene ambientale. progettazione e*

realizzazione di centri di cottura per la ristorazione collettiva. manutenzione ordinaria di impianti ed attrezzature". Tuttavia tali attività sono accomunate dalla volontà di assicurare in ogni momento e contesto la sicurezza e salute dei lavoratori e degli utenti, nonché, con particolare riferimento alla Privacy, la protezione dei dati personali che l'azienda tratta.

In ragione di ciò l'azienda si impegna ad adottare le misure tecniche ed organizzative adeguate al contesto in cui opera, necessarie a garantire un livello di sicurezza adeguato a eventuali rischi per i diritti e le libertà delle persone fisiche

NOMINE

Il Reg. UE 679/2016 art 4 n 10 individua fra i soggetti del trattamento il titolare, il responsabile, le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

L'azienda, nei suoi rapporti con eventuali responsabili del trattamento dei dati personali che effettuano operazioni per suo conto, si impegna, così come previsto dal REG UE 679/2016 art 28 par 3 a cristallizzare tale nomina in un contratto o altro atto giuridico vincolante, tale da disciplinare la materia della protezione dei dati personali, la durata del trattamento, la natura, la finalità dello stesso, tipo di dati personali, categorie di interessati, obblighi e diritti del titolare del trattamento.

Inoltre, l'art 29 prevede che chiunque agisca sotto l'autorità del titolare o del responsabile e che abbia accesso a dati personali non possa trattare tali dati se non è istruito in tal senso dal titolare, a meno che ciò non sia imposto da una norma di legge.

Al fine di dare istruzioni al personale dipendente dell'azienda, la stessa azienda fornisce specifiche istruzioni sul trattamento del dato personale attraverso una lettera di incarico che il dipendente deve sottoscrivere e accettare e con la quale verrà riconosciuto formalmente come "incaricato al trattamento" e, in quanto tale, tenuto alle istruzioni ricevute circa il suddetto trattamento.

RESPONSABILE PROTEZIONE DATI PERSONALI (DPO)

Ladisa S.r.l. ha inteso nominare un DPO (Data Protection Officer, ovvero Responsabile della Protezione dei Dati Personali) a garanzia e presidio della corretta applicazione delle procedure interne previste per il trattamento dei dati personali, in conformità al Reg. UE 679/2016 (GDPR).

La figura del DPO, individuato in un consulente esterno esperto in materia di protezione dei dati personali, rappresenta un riferimento per dipendenti, organi apicali, clienti, partner commerciali e stakeholder a vario titolo intesi, e gestisce un autonomo canale di comunicazione al fine di raccogliere segnalazioni sull'errato o inefficace trattamento dei dati particolari.

La nomina del DPO, di durata annuale, viene comunicata all'Autorità Garante per la Privacy, e trova evidenza su tutti i canali istituzionali di Ladisa S.r.l..

Ladisa S.r.l. si è dotata di un DPO su base obbligatoria ai sensi dell'art. 37 GDPR; è una figura professionale indipendente introdotta in Unione Europea dal Regolamento Generale sulla Protezione dei Dati (GDPR), che svolge le seguenti funzioni:

• Consulenza: Informa e fornisce pareri al titolare del trattamento, ai responsabili e ai dipendenti sugli obblighi previsti dal GDPR.

• Sorveglianza: Monitora l'osservanza del regolamento, delle politiche aziendali e valuta le Valutazioni d'Impatto sulla Protezione dei Dati (DPIA).

• Punto di contatto: Funge da interfaccia tra l'organizzazione, gli interessati (i cittadini) e l'Autorità Garante per la Privacy.

• Formazione: Collabora alla sensibilizzazione e alla formazione del personale interno

REGISTRO DEI TRATTAMENTI ED ANALISI DEI RISCHI

Il REG UE 679/2016 prevede all'art 30 che ciascuna azienda che abbia non meno di 250 dipendenti, oppure che effettui trattamenti non occasionali, che possono presentare un rischio per i diritti e le libertà dell'interessato, e che includono il trattamento di categorie particolari di dati di cui all'art 9 par 1 o art. 10 REG UE 679/2016, si doti di un registro delle attività di trattamento.

In esito al censimento ed analisi dei trattamenti effettuati dall'azienda è emerso, in particolare, che la stessa tratta dati di cui all'art 10 relativi a condanne penali e reati, al fine, in particolare, della richiesta di emissione del c.d. rating di legalità di cui all' Art. 5-ter del decreto-legge 1/2012, come modificato dal Decreto legge 29/2012, convertito con modificazioni dalla Legge 62/2012

In ogni caso l'azienda si è dotata di un registro trattamenti che, predisposto in formato elettronico (excel) e stampato, sarà verificato e aggiornato con cadenza semestrale o al sopraggiungere di cambiamenti organizzativi o strutturali significativi.

Sulla base dei trattamenti individuati nel suddetto Registro l'azienda ha provveduto a definire una metodologia per la definizione del processo di gestione del rischio e ad effettuare una analisi dei rischi che possono avere probabilità e gravità diversa per i diritti e le libertà delle persone fisiche come ad esempio quelli che possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

In esito a questa analisi sono state poste in essere o lo saranno secondo quanto indicato nel piano di trattamento dei rischi, misure di sicurezza adeguate rispetto al rischio connesso e che siano in grado in particolare, di assicurare su base permanente la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento.

Bari, li 26.10.2026 Legale Rappresentante Ladisa S.r.l.

Dott. Cesare Pinto

2. GLOSSARIO

L'azienda adotta il seguente glossario al fine di esemplificare le modalità e le procedure a cui tutti i dipendenti aziendali sono tenuti nell'ambito della sicurezza dei dati personali.

In particolare nel seguente elenco si fa riferimento alle definizioni contenute nel RGPD reg 679/2016 e, quindi per:

- *dato personale*: si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile, in maniera diretta o indiretta anche con riferimento ad elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- *trattamento*: si intende qualsiasi operazione compiute con i dati personali o attraverso gli stessi come, a titolo esemplificativo: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, messa a disposizione, raffronto, interconnessione, limitazione, cancellazione, distruzione, ecc.
- *limitazione di trattamento*: si intende il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- *profilazione*: si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- *pseudonimizzazione*: si intende il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- *archivio*: si intende qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- *titolare del trattamento*: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici

applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- *responsabile del trattamento*: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- *responsabile della protezione dei dati personali (anche "DPO")*: è una figura professionale indipendente introdotta in Unione Europea dal Regolamento Generale sulla Protezione dei Dati (GDPR) che ha le seguenti funzioni: informa e fornisce pareri al titolare del trattamento, ai responsabili e ai dipendenti sugli obblighi previsti dal GDPR; monitora l'osservanza del regolamento, delle politiche aziendali e valuta le Valutazioni d'Impatto sulla Protezione dei Dati (DPIA); funge da interfaccia tra l'organizzazione, gli interessati (i cittadini) e l'Autorità Garante per la Privacy; collabora alla sensibilizzazione e alla formazione del personale interno.
- *destinatario*: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
- *terzo*: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- *consenso dell'interessato*: si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- *violazione dei dati personali*: si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- *dati genetici*: si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- *dati biometrici*: si intendono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- *dati relativi alla salute*: si intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- *impresa*: si intende la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- *gruppo imprenditoriale*: si intende un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- *autorità di controllo*: si intende l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- *trattamento transfrontaliero*: si intende:
    - a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
    - b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- "*Attività principali*", L'articolo 37, paragrafo 1, lettere b) e c) del RGPD contiene un riferimento alle "attività principali del titolare del trattamento o del responsabile del trattamento". Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento. Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un DPO. D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

- Si definisce malware qualsiasi software che, una volta eseguito su un sistema informatico, possa apportaremodificheindesiderateodannialsistemastessoeaisuoiutenti. I malware possono effettuare le azioni più diverse sul sistema vittima: possono sottrarre le informazioni memorizzate, danneggiarle o modificarle in maniera ponderata, catturare schermate del dispositivo vittima violando la privacy dei suoi utenti, rubare credenziali degli utenti che usano il sistema, e altro. Non necessariamente i malware creano effetti visibili all'utente; anzi, i malware normalmente sono programmati per non essere rilevati e non creare problemi immediati all'utente, proprio per poter persistere a lungo sul dispositivo e raggiungere nel modo più completo possibile i propri fini. Molti malware sono progettati per colpire il maggior numero possibile di persone ma questo non è sempre necessariamente vero: in alcuni casi un malware può essere disegnato in modo specifico per una vittima ed essere quindi il veicolo di attacchi mirati. I malware usano diversi metodi per entrare nei sistemi: possono nascondersi in un allegato e-mail (documenti pdf, file eseguibili, documenti Microsoft Office, etc.), in un file contenuto in una pendrive USB, su pagine web visitabili durante la navigazione da un browser, e altro. Purtroppo, nuovi malware sempre più complessi nascono ogni giorno, e non esistono dispositivi immuni: tutti i sistemi operativi, tutti i tipi di dispositivi possono essere colpiti da questa grave minaccia.
- I ransomware rappresentano una tipologia specifica di malware il cui obiettivo è impedire alla vittima l'accesso e l'uso di documenti e dispositivi. L'attaccante ricatta quindi la vittima chiedendo un "riscatto" per la liberazione delle risorse inaccessibili. Cryptolocker è solo il più noto nella famiglia dei ransomware (cui abbiamo già accennato nelle precedenti sezioni): software che codificano i dati presenti sulle memorie di massa dei personal computer vittima per impedire l'accesso agli utenti, che possono quindi essere ricattati. I casi di imprese, enti e organizzazioni le cui attività sono state completamente bloccate da questi attacchi sono innumerevoli.
- Firewall è un componente (tipicamente, ma non esclusivamente, hardware) che si interpone tra due reti e permette di imporre regole sul transito di informazioni tra queste. Un uso tipico di un firewall prevede la sua installazione tra la rete aziendale e internet per permettere solo ad utenti e flussi di dati autorizzati di transitare, bloccando invece ogni comunicazione potenzialmente illecita.
- IntrusionDetection/PreventionSystem è un componente che controlla in modo continuo il traffico e le attività in essere nella rete aziendale per identificare e, laddove possibile, prevenire possibili intrusioni non autorizzate.
- Mail/WebFilter è un componente che intercetta ogni mail o dati web in transito da internet verso l'azienda, per identificare e bloccare tempestivamente possibili minacce.

3. DIRITTI DELL'INTERESSATO

L'azienda, nella sua qualità di titolare dei dati trattati, intende assicurare a tutti gli interessati l'esercizio dei diritti che la legge riconosce loro.
In particolare l'Azienda si è dotata di procedure volte ad assicurare il rispetto degli adempimenti previsti dal Reg Ue 679/2016 quali:

1. L'obbligo di informativa ai sensi dell'art 13 e 14 del reg 679/2016;
2. L'obbligo di confermare all'interessato che sia in corso un trattamento di suoi dati personali e, se del caso, di fornirgli l'accesso oltre che comunicargli ulteriori informazioni così come indicato dall'art 15;
3. L'obbligo di assicurare la rettifica (art 16) e la cancellazione (art 17) dei dati personali su richiesta dell'interessato in base alla sussistenza dei requisiti di legge;
4. l'obbligo di limitare il trattamento (art 18) se l'interessato contesta l'esattezza dei dati, o se il trattamento è illecito e l'interessato si oppone alla cancellazione, o se i dati sono necessari al solo interessato al fine di procedere all'accertamento, esercizio, difesa di un diritto in sede giudiziaria, o se l'interessato si è opposto al trattamento ai sensi dell'art 21, paragrafo , in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
5. L'obbligo di assicurare la portabilità dei dati personali (art 20) in un formato strutturato, di uso comune e leggibile da dispositivo automatico
6. L'obbligo di astenersi dal trattamento ulteriore di dati personali in caso di esercizio del diritto di opposizione (art 21) da parte dell'interessato

Inoltre, con riferimento all'art 22, l'azienda non effettua processi decisionali automatizzati, né profilazione sui dati personali che tratta; parimenti, in ossequio alle prescrizioni di cui al Regolamento UE 2024/1689 (AI Act), la Ladisa S.r.l. non utilizza forme di intelligenza artificiale nei processi decisionali.

PROCEDURE

INFORMATIVA

- All'atto della sottoscrizione del **contratto di assunzione** il responsabile del personale fornirà a ciascun dipendente informativa privacy ai sensi dell'art 13 REG UE 679/2016;
- All'atto della sottoscrizione del **contratto di assunzione** il responsabile del personale fornirà a ciascun dipendente che avrà fra i suoi compiti quello di operare direttamente su dati personali trattati dall'azienda in veste di Titolare del trattamento, una lettera di incarico per la funzione di "Incaricato al trattamento" che dovrà essere sottoscritta dal dipendente. L'azienda si assicurerà con verifiche interne semestrali condotte dal Responsabile della Protezione dei Dati (RPD) e dal team di lavoro da egli designato, che tutti i dipendenti che hanno accesso o trattano in qualsiasi modo dati personali abbiano sottoscritto tale lettera di incarico.

  Di ciò sarà data evidenza con un report da presentare all'organo amministrativo da parte del Responsabile della Protezione dei Dati (RPD).
- Dovrà essere resa disponibile in maniera chiara ed immediata agli utenti dei siti internet di proprietà dell'azienda o gesti dalla stessa una informativa in relazione all'uso dei cookies e in relazione ai dati personali trattati attraverso tali pagine web. Ogni sei mesi occorrerà procedere con una verifica ed eventuale aggiornamento della stessa; di ciò sarà data evidenza attraverso un report da sottoporre all'organo amministrativo da parte del Responsabile della Protezione dei Dati (RPD).

ACCESSO AI DATI

L'azienda garantisce l'accesso ai dati personali dell'interessato; in particolare, a seguito di una richiesta pervenuta tramite il sito internet aziendale o inviata alla casella mail o pec aziendale o inviata in forma cartacea presso la sede, il Responsabile della Protezione dei Dati (DPO) o un suo delegato dovrà in particolare garantire:

1) all'interessato il diritto di ottenere dall'azienda la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
   a) le finalità del trattamento;
   b) le categorie di dati personali in questione;
   c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del reg 679/2016, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2) che, qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato venga informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3) la messa a disposizione di una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, l'azienda potrà addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4) il diritto di ottenere che una copia di cui al punto 3 non leda i diritti e le libertà altrui.

Va altresì specificato che un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli per essere consapevole del trattamento e verificarne la liceità.

Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati.

Pertanto l'azienda si impegnerà a garantire ad ogni interessato il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento.

Ove possibile, l'azienda fornirà l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali.

Tale diritto non dovrà ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software.

Tuttavia, queste considerazioni non condurranno ad a un diniego nel fornire all'interessato tutte le informazioni.

Qualora l'azienda tratti una notevole quantità d'informazioni riguardanti l'interessato, richiederà che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.

Inoltre, l'azienda si impegna ad adottare tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online, tutto questo cercando, nei limiti del possibile, di non conservare dati personali al solo scopo di poter rispondere a potenziali richieste.

RETTIFICA

L'azienda si impegna a garantire che l'interessato possa esercitare il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano in tempi ragionevoli e senza ingiustificato ritardo e affida questo compito al Responsabile della Protezione dei Dati (DPO) o un suo delegato. Tenuto conto delle finalità del trattamento, l'azienda si impegna a garantire all'interessato il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

L'azienda si impegna a garantire all'interessato il diritto di ottenere la rettifica dei dati personali che la riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il regolamento 679/2016 o il diritto dell'Unione o degli Stati membri cui è soggetto l'azienda.

In particolare, l'azienda si impegna a garantire all'interessato il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al regolamento 679/2016; ed in particolare se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. In particolare, l'azienda si impegna a garantire all'interessato di poter esercitare questo diritto indipendentemente dal fatto che non sia più un minore.

Tuttavia, dovrebbe essere ritenuta lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

CANCELLAZIONE

L'azienda si impegna a garantire all'interessato, affidando questo compito al Responsabile della Protezione dei Dati (DPO), in particolare, la possibilità di richiedere la cancellazione dei dati personali che lo riguardano ovvero:

1) L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e l'azienda si impegna a cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
   a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
   b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a) del reg 679/2016, e se non sussiste altro fondamento giuridico per il trattamento;
   c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 del reg 679/2016, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2 del reg 679/2016;
   d) i dati personali sono stati trattati illecitamente;
   e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
   f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 del reg 679/2016.
2) L'azienda, qualora avesse reso pubblici dati personali ed è obbligata, ai sensi del paragrafo 1 del reg 679/2016, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotterà le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3) I punti 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
   a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetta l'azienda o per l'esecuzione di un compito svolto nel pubblico interesse;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 del reg 679/2016;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 del reg 679/2016, nella misura in cui il diritto di cui al paragrafo 1 del reg 679/2016 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

LIMITAZIONE

L'azienda si impegna a garantisce all'interessato la possibilità di richiedere la limitazione dei dati personali che lo riguardano; in particolare:

1) L'interessato ha il diritto di ottenere dall'azienda la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
   a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario all'azienda per verificare l'esattezza di tali dati personali;
   b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
   c) benché l'azienda non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del reg 679/2016, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
2) Se il trattamento è limitato a norma del punto 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
3) L'interessato che ha ottenuto la limitazione del trattamento a norma del punto 1 è informato dall'azienda prima che detta limitazione sia revocata.

Le modalità per limitare il trattamento dei dati personali adottate dall'azienda potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da

un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali verrà in linea di massima assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema indicherà chiaramente che il trattamento dei dati personali è stato limitato.

PORTABILITÀ

L'azienda si impegna a garantire all'interessato la possibilità di richiedere la portabilità dei dati personali che lo riguardano:

1) L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti all'azienda e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte dell'azienda qualora:
   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a) del reg 679/2016, o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) del reg 679/2016; e
   b) il trattamento sia effettuato con mezzi automatizzati.
2) Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del punto 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali dall'azienda ad altro titolare del trattamento, se tecnicamente fattibile sia dal punto di vista tecnologico che economico.
3) Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'azienda.
4) Il diritto di cui al punto 1 non deve ledere i diritti e le libertà altrui.

Al fine di rafforzare ulteriormente il controllo sui propri dati, l'azienda di impegna nei limiti ragionevoli a fornire all'interessato, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. Tale diritto dovrebbe applicarsi qualora l'interessato ha fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto l'azienda o per l'esecuzione di un compito svolto nel pubblico interesse. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non comporta l'obbligo per l'azienda di adottare o mantenere sistemi di trattamento tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza al regolamento 679/2016. Inoltre

tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto.

4. PROCESSO DI GESTIONE DEL RISCHIO

CONTESTO

Il sito è composto da due immobili e da un'area esterna situati in Zona A.S.I. (Consorzio per lo sviluppo industriale di Bari) Bari-Modugno, classificata in zona sismica 3:

- Immobile adibito a centro di cottura e deposito derrate alimentari;
- Immobile adibito ad uffici;
- Area esterna con i locali tecnici

CENTRO COTTURA

L'immobile adibito a centro cottura, si estende a piano terra per circa 5000 mq., mentre il piano interrato, di pari superficie, è adibito a deposito derrate alimentari. Al di sopra del piano terra è presente una copertura caricata con unità terminali degli impianti termici e aeraulici, nonché per la predisposizione di un impianto fotovoltaico da installare.

- Centro cottura piano terra: deposito detersivi, zona arrivo derrate alimentari con bilico, dispensa, preparazione verdure, preparazione carni rosse, preparazione carni bianche, preparazione pesce, preparazione piatti freddi, zona cotture per diete speciali e celiaci, confezionamento, lavaggio pentole, lavaggio contenitori, zona smistamento, zona preparazione secondi e contorni, zona lavaggio pentole, lavastoviglie, area sosta carrelli e lavaggio, macelleria per disosso anatomico carni bianche e carni rosse, magazzino prodotti sanificanti, locale rifiuti, spogliatoio personale con servizi igienici, docce e armadietti. Locale per la realizzazione di una futura pasticceria.
- Centro cottura piano interrato (-1) – cella frigorifera surgelati, scaffalature flow rail, locale ricarica batterie per carrelli elettrici, archivio, servizi igienici.

All'interno dei locali della zona cottura si ha un riscaldamento/raffrescamento con macchine a soffitto e sacchi ventilazione.

UFFICI

La palazzina uffici consta di un edificio pluriplano (tre piani fuori terra), ciascuno esteso per circa 580 mq. L'immobile è fisicamente e strutturalmente separato dal corpo di fabbrica adibito a centro cottura. L'immobile si può qualificare distributivamente come doppio strutturale e triplo distributivo.

Il piano terra è adibito a reception, vani tecnici, sala formazione, sala mensa, bar, gruppo servizi igienici, i piani superiori sono occupati da uffici di amministrazione, direzione e gruppi servizi igienici.

ZONA ESTERNA

In quest'area è ubicato il locale antincendio con relativa vasca e pompe, la cabina elettrica, il locale gruppo generatore ed un'area destinata al parcheggio dei mezzi aziendali. L'intera struttura, dagli impianti alle attrezzature, è stata progettata e realizzata per assicurare elevati standard: di Qualità, Sicurezza Alimentare e Sostenibilità Ambientale ed Energetica.

Ulteriori informazioni sul contesto sono riportate nel documento "Analisi del contesto" del 10/01/2018 e suoi aggiornamenti.

PROCESSI AZIENDALI

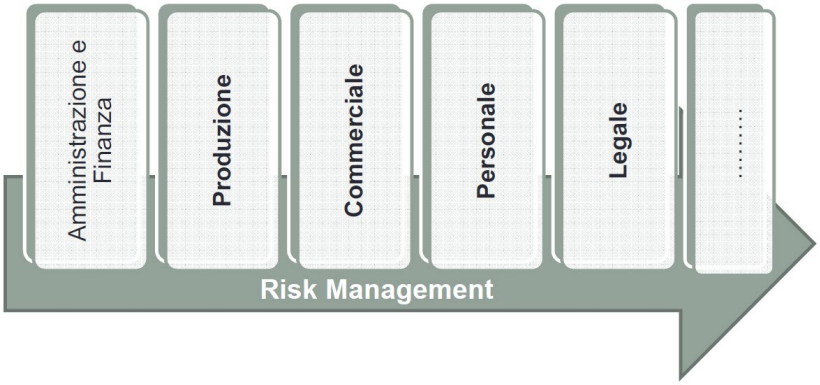
L'azienda è una società di servizi e svolge principalmente le seguenti attività:

- progettazione ed erogazione di servizi di ristorazione collettiva per enti pubblici e privati: mense scolastiche, sanitarie, militari e della pubblica sicurezza. preparazione, confezionamento in monoporzione e multi-porzione, trasporto e distribuzione pasti. gestione bar, tavola calda, gastronomia da asporto. lavorazione, produzione, confezionamento, vendita e preparazione di carne e prodotti a base di carne fresca. produzione di piatti pronti.
- Piattaforma centralizzata per acquisto, trasporto, distribuzione e commercializzazione di merci (no food) e derrate alimentari per la ristorazione collettiva e la grande distribuzione organizzata.
- Erogazione dei servizi di derattizzazione, disinfestazione, pulizia civile ed igiene ambientale.
- Progettazione e realizzazione di centri di cottura per la ristorazione collettiva.
- Manutenzione ordinaria di impianti ed attrezzature.

Nello svolgere le sue attività l'azienda ha diversi siti in quanto parte delle attività vengono erogate anche presso le sedi della committenza.

All'interno del "MANUALE DEL SISTEMA DI GESTIONE INTEGRATO PER LA QUALITA', L'AMBIENTE, L'ENERGIA, LA SALUTE E SICUREZZA SUL LAVORO E LA RESPONSABILITA' SOCIALE edizione 1 revisione 1 del 26/10/20126" sono riporti i processi aziendali che trattano i dati definiti nel registro dei trattamenti.

Oggi il risk management abbraccia orizzontalmente tutte le attività aziendali che vengono sempre toccate da questa disciplina in quanto tutte esposte a rischi e tutte possono partecipare alla loro buona gestione.



L'azienda ha compreso che per poter superare in modo efficace ed efficiente le "crisi", a cui può andare in incontro con probabilità sempre crescente, è necessario approcciarsi ai rischi in modo professionale misurandoli e, dove essi assumano livelli non accettabili, adottando misure di protezione e prevenzione in grado di ricondurre tali rischi ad un livello accettabile. Devono quindi essere applicate la disciplina del "risk management" che secondo la ISO 3100 significa che l'organizzazione deve **gestire il rischio come sistema.**

Per risk management si intende quell'insieme di attività, fra loro coordinate, per guidare e tenere sotto controllo i rischi a cui è esposta l'organizzazione documentando i requisiti, le specifiche, le linee guida e le caratteristiche che possono essere utilizzate in modo coerente per garantire gli obiettivi e le politiche aziendali nonché il rispetto di leggi e regolamenti ed in particolare il REG 679/2018.

Posso essere utili ai fine di questo processo i seguenti standard:

- ISO Guide 73:2009 Risk management – Vocabulary
- ISO 31000:2009 Risk management - Principles and guidelines
- ISO/IEC 31010:2009 Risk management - Risk assessment techniques
- ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000

Il regolamento 679/2016 non definisce esplicitamente la definizione di "rischio" legato alla privacy. Per questo motivo l'azienda utilizza la seguente definizione estratta dalla norma ISO 31000:2010:

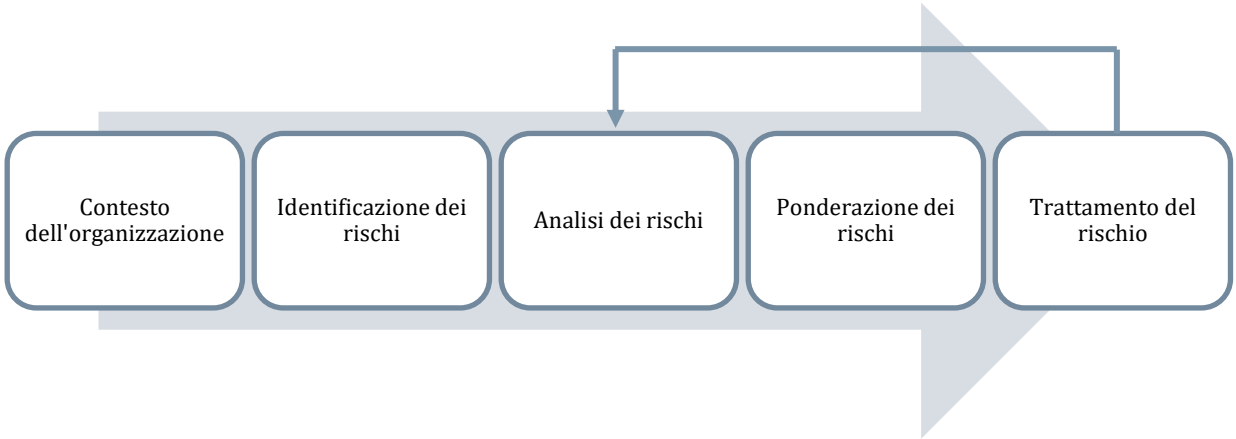
"Il rischio è l'effetto dell'incertezza sul raggiungimento degli obiettivi"

Nell'ottica privacy, l'obiettivo, viene declinato con l'impegno da parte dell'azienda nel garantire i diritti e le libertà degli interessati in accordo ai suoi processi di business.

L'azienda gestirà il rischio con la realizzazione di due attività fondamentali, fra loro interconnesse:

- Processo tecnico, ovvero il macro processo composto dalle seguenti fasi:
  - identificazione rischi
  - analisi rischi
  - valutazione per verificare se debbano intervenire modifiche (opportuni trattamenti del rischio) per soddisfare i criteri di rischio dell'organizzazione.
- Processo manageriale, con riferimento al processo di gestione del rischio e durante la sua realizzazione:
  - si comunica con i portatori di interessi e si consultano gli stessi;
  - si pianificano le attività e si monitora e riesamina il rischio, ed i controlli che lo stanno modificando, per accertarsi che non sia richiesto alcun ulteriore trattamento.

Questi due macro processi possono essere visti fusi ed interconnessi nel seguente workflow:



Successivamente si riportano analiticamente tutte le fasi identificate per questo processo.

FASE 1: ANALISI DEI TRATTAMENTI E REQUISITI

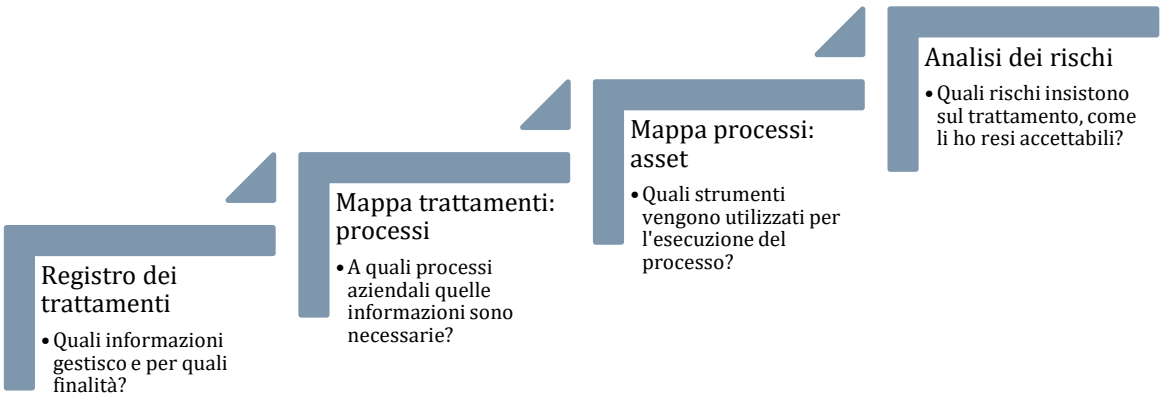
In attuazione dell'art. 35/9 e in conformità all'orientamento degli standard ISO al contesto e agli stakeholder, si definiscono i requisiti di sicurezza in base alle aspettative dei diversi soggetti interessati, agli obiettivi aziendali e tenendo conto di tutte le richieste legali, contrattuali e dei regolatori di tutti i paesi di destinazione dei servizi/prodotti e pertinenti al tipo di attività.

Oltre a questi requisiti il regolamento e la ISO / IEC 27001 richiedono anche di tener conto del contesto esterno (p.e. situazione attuale delle minacce alla sicurezza, eventi ed incidenti di sicurezza avvenuti, stato dell'arte) e del contesto interno (p.e. il processo operativo sostenuto, la consapevolezza e le competenze informatiche degli utenti, l'infrastruttura disponibile). Con ciò ogni valutazione d'impatto deve tener conto della situazione specifica ed essere elaborata in modo individuale.

Sia il regolamento UE che anche le normative richiedono un'analisi sistematica dei trattamenti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento (vedi art. 6, 9 e 10), l'informazione e i diritti dell'interessato (art. 12 – 22) e una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità (vedi principi fondamentali art. 5). Si analizzano sia trattamenti digitalizzati che cartacei. L'organizzazione dovrà discute l'adeguatezza, la pertinenza e la necessità dei dati. Se si eliminano i dati non assolutamente necessari, si aumenta l'efficienza dei processi. In tal modo si cambia dal big data alla logistica delle informazioni: solo agli utenti autorizzati, nei momenti strettamente necessari, si mettono a disposizione i dati pertinenti. Inoltre, l'analisi dei trattamenti offre anche un'ottima opportunità di digitalizzazione e miglioramento dell'efficienza. Grazie all'analisi i trattamenti si stabilisce anche il registro delle attività di trattamento richiesto dall'art. 30 del regolamento e la necessaria disponibilità dei servizi (vedi art. 32).

Attività preliminari alla conduzione dell'analisi dei rischi

Di seguito si riporta uno schema esemplificativo delle attività prodromiche all'attività di analisi dei rischi



FASE 2 ANALISI

Nella fase successiva si definisce per ogni trattamento/processo i documenti/ archivi associati e i servizi IT associati con i componenti tecnici di supporto di tutti livelli dell'architettura e le loro interazioni in un modo olistico e sistemico.

I criteri di rischio sono l'elemento base della gestione del rischio, da riesaminare periodicamente, e sono punto di riferimento che consente di portare a fattor comune tutte le tipologie di rischio gravanti sull'organizzazione in quanto riflettono i valori, gli obiettivi e le risorse dell'organizzazione coerenti con la politica per la gestione del rischio.

La valutazione del rischio risulta strettamente legata alla ISO 31010 dove vengono esposte le tecniche di gestione del rischio la ISO 31000 le richiama esplicitamente.

Partendo dai processi/trattamenti e la classificazione dei dati e le richieste stabiliti si deduce a base delle relazioni definite le richieste privacy per ogni componente/archivio e per l'intero ciclo di vita dell'informazione e del sistema/prodotto/atto.

Visto che la componente più debole definisce il livello di sicurezza del sistema, è particolarmente importante per servizi aperti o connessi in modo flessibile. Vista la dinamica dell'organizzazione si deve senz'altro analizzare ogni processo/trattamento se si tratta dati "critici". Conciò in pratica è più efficiente di analizzare una tale organizzazione/azienda in un unico progetto con tutti processi/ trattamenti e l'intera struttura IT, invece di analizzare ogni trattamento distinto con tutti i suoi servizi connessi.

Successivamente si analizzano, con i collaboratori interessati e sulla base di un catalogo di riconosciute minacce (ad esempio, ISO 27000 serie, COBIT, US NIST serie SP 800, linee guida del garante) tenendo conto anche dei codici di condotta, delle richieste definite e della situazione individuale, i potenziali impatti con la loro probabilità e severità per l'intero ciclo di vita.

In considerazione delle misure preventive già attuate si stimano i rischi rimanenti ed il criterio di accettabilità, il titolare del trattamento decide ed approva formalmente, eventualmente coinvolgendo il DPO e tutte le figure interessate, se il livello di rischio residuo è accettabile, o si pianifica/investe e si realizzano ulteriori azioni preventive considerando sempre l'equilibrio tra sicurezza – costi/oneri e/o usabilità dei trattamenti o, in caso di rischio elevato, si consulta il Garante per la protezione dei dati personali (art. 36).

Secondo studi scientifici, una gestione semplice ed efficiente delle misure di sicurezza è essenziale per l'attuazione.

Le misure preventive comprendono sia misure organizzative (separazione dei compiti, concetto di ruolo e responsabilità, gestione degli utenti e loro diritti, gestione degli accessi fisici, rintracciabilità, misurazione, controlli e verifiche, gestione degli asset e dei supporti rimovibili, istruzione e promozione della consapevolezza) che misure tecniche (controlli di plausibilità ed integrità, autentificazione, logging, criptografia, firma digitale, sicurezza della transazione, sicurezza del database, disponibilità delle connessioni) e riguardano l'intero ciclo di vita, dall'acquisizione/produzione di informazioni/sistemi alla divulgazione e fino all'archiviazione ed alla distruzione.

In tale modo si adattano sia l'art. 25 (privacy by design e by default) del regolamento che anche l'art. 32 (sicurezza) e l'art. 35 (valutazione d'impatto sulla protezione dei dati).

Per gli accettabili rischi rimanenti si definisce, in considerazione delle richieste legislative e contrattuali, un eventuale piano di continuità per la diminuzione degli impatti in caso d'emergenza e la riattivazione del servizio e si verificano eventuali riserve ed assicurazioni.

Identificazione dei rischi

è il processo di ricerca, di individuazione e di descrizione dei rischi, inclusa l'identificazione delle loro fonti, degli eventi e delle relative cause e potenziali conseguenze ed aree di impatto. Per una adeguata identificazione saranno presi in considerazione almeno:

- le fonti di rischio,
- le aree di impatto,
- gli eventi,
- le cause e
- le potenziali conseguenze di questi ultimi oltre a
- l'esame di dati storici,
- le analisi teoriche e
- le opinioni di esperti.

Inoltre dovranno essere considerati i rischi derivanti dalla perdita di resilienza dei sistemi informatici intesa come la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati

Classificazione delle informazioni

Le informazioni dovranno almeno essere classificate secondo quanto identificato nel regolamento 679/2016.

Attività di analisi del rischio

è il processo di comprensione delle componenti del rischio e quindi della sua natura e del suo livello per la realizzazione delle successive fasi di ponderazione del rischio e di suo trattamento. Gli elementi fondamentali dell'analisi del rischio sono:

- la sua misurazione in termini di dimensionamento sia delle conseguenze sia della verosimiglianza;
- l'individuazione e definizione di tutti i fattori che possono influenzarlo e possono variare i parametri di verosimiglianza e conseguenze;
- l'analisi di tutte le possibili conseguenze dirette ed indirette.

L'analisi dei rischi sarà condotta in maniera semi-quantitativa.

Individuazione delle componenti del rischio generico:

Definizioni riportate nello standard ISO 27002:

- **Riservatezza**: Assicurarsi che le informazioni siano accessibili solo a chi sia stato identificato e disponga dell'appropriato grado di autorizzazione.
- **Integrità**: Salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.
- **Disponibilità e resilienza**: Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e ai beni collegati quando richiesto. Il concetto di resilienza dei sistemi e dei servizi informatici che trattano i dati personali si riferisce, in termini molto generali, alla capacità intrinseca di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura al fine di assicurare sempre la disponibilità dei servizi che vengono forniti e la adeguata protezione dei dati che vengono trattati con tali sistemi.

Questi tre elementi, costituiscono la base per la sicurezza delle informazioni così come definito negli standard ISO 27001 e ISO 27002 nonché citati più volte dal REG 679/2016.

- Incidenze sulla perdita di:
  - Riservatezza [***r***]
  - Integrità [***i***]
  - Disponibilità e resilienza [***d***]
- Probabilità o verosimiglianza di accadimento [***p***]

In parentesi quadre è indicata la lettera riportata nella formula sottostante.

Le componenti di rischio saranno stimate secondo la seguente scala qualitativa: Basso, Medio, Alto alle quali saranno associate i valori numeri 1,2,3. Per quantificare il valore di ogni componente del rischio ci si affiderà alle informazioni storiche che l'azienda possiede e all'esperienza degli addetti nonché l'avvallo di un esperto esterno con comprovate esperienza nel settore.

Ad ogni rischio verrà associato un indice per la sua valutazione, attraverso la seguente formula:

$$\boldsymbol{idx} = (\boldsymbol{r} + \boldsymbol{i} + \boldsymbol{d}) * \boldsymbol{p}$$

L'indice potrà variare da un minimo di 3 ad un valore massimo di 27.

Componenti idx		Basso [1]	Medio [2]	Alto [3]
Valore r+i+d	3	3	6	9
	4	4	8	12
	5	5	10	15
	6	6	12	18
	7	7	14	21
	8	8	16	24
	9	9	18	27

In considerazione delle finalità specifiche dell'analisi dei rischi ovvero analizzare e ponderare i rischi associati alla perdita di privacy e quindi alla perdita dei diritti degli interessati, nella stima dei valori di gravità di riservatezza, integrità e disponibilità nonché della probabilità di accadimento si dovranno prendere in considerazione i rischi per i diritti e le libertà delle persone fisiche dai quali possono derivare trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da

segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;

- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Ponderazione dei rischi

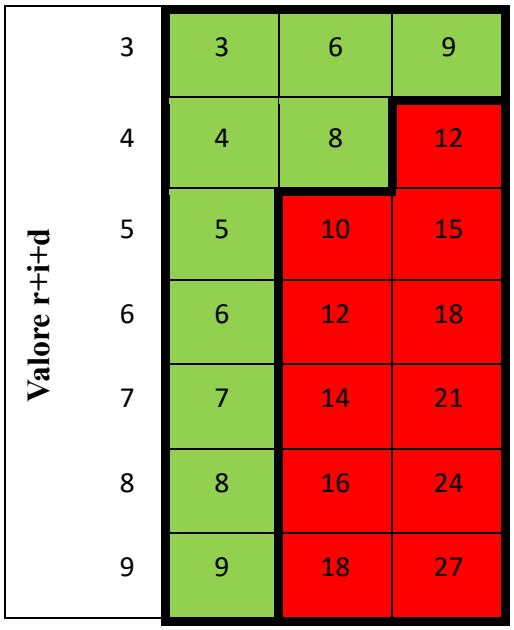
È il processo di paragone dei risultati dell'analisi del rischio con i criteri di rischio definiti per stabilire se il rischio sia da considerarsi accettabile o non accettabile consentendo quindi, in tale ultimo caso, l'avvio del processo di suo trattamento per ricondurlo ad una sua accettabilità. Si sostanzia nel confronto tra il livello di rischio derivante dall'analisi rischi ed i criteri di rischio stabiliti durante l'esame del contesto per definire i trattamenti a cui sottoporre i rischi.

Questo modo di procedere permette di effettuare una valutazione del rischio in grado di produrre risultati coerenti, validi e confrontabili tra loro per ogni rischio individuato (6.1.2 b); inoltre per ogni rischio sarà identificato un responsabile "risk-owner" per il suo controllo e monitoraggio.

Criterio di accettabilità

Rispetto all'indice definito, il rischio si riterrà accettabile se il suo valore è al disotto o al più uguale al valore 9. In tabella si evidenziano in verde le zone accettabili ed in rosso quelle non accettabili.

Componenti idx	Basso [1]	Medio [2]	Alto [3]



FASE 3: TRATTAMENTO DEI RISCHI

Tutti i rischi che hanno un valore al di sopra del criterio di accettabilità devono essere mitigati attraverso le seguenti tipologie di interventi:

- Evitare il rischio (es: chiusura di un'attività giudicata non rispondente ai criteri);
- Assumere il rischio (es: perseguire una opportunità);
- Rimuovere la fonte di rischio (es: rimozione di un masso pericoloso);
- Modificare la probabilità (es: sistemi di sicurezza);
- Modificare le conseguenze (es: parcellizzare ove possibile le attività produttive);
- Trasferire il rischio su altre parti (es: assicurazioni);
- Ritenere coscientemente il rischio con una decisione informata.

Per tanto le misure preventive, registrate in un apposito documento, si integrano nei processi/trattamenti con controlli e misurazioni associati, si elaborano ed istruiscono le istruzioni di condotta e/o si trasferiscono a terzi tramite contratti di fornitura/outsourcing (attuazione dell'art. 28).

Visto che diversi studi scientifici sottolineano l'importanza della consapevolezza per la sicurezza da parte degli utenti, si offre una sufficiente formazione e un appropriato sostegno agli utenti.

L'integrazione ottimale della sicurezza dell'informazione, dell'ergonomia del sistema, dell'orientamento agli utenti e della gestione della qualità sostiene un'implementazione efficiente ed efficace.

Vanno altresì considerate in modo particolare i trattamenti dei rischi e le contro misure legate a:

- Gestione sistema di autenticazione e di autorizzazione:
  Il primo aspetto da tenere in considerazione è relativo alla corretta definizione delle password che devono essere di una complessità adeguata. Le recenti best practices suggeriscono di forzare gli utenti a scegliere password lunghe almeno 12 caratteri, che contengano almeno un numero e un carattere non alfanumerico e che non contengano termini noti del vocabolario o informazioni facilmente riconducibili all'utente (nomi di familiari, animali domestici, date di anniversari e qualunque informazione possa essere facilmente trovata sui social network). L'uso di password complesse protegge l'utente nel caso in cui un attaccante riuscisse a impossessarsi di una database di password codificate, dato che renderebbe molto costoso per l'attaccante cercare di identificare le password provando tutte le combinazioni possibili (il cosiddetto "attacco a forza bruta"). In caso di compromissione delle password è opportuno che, per tutte le utenze coinvolte, sia intrapreso un processo di ripristino che porti alla modifica di tutte le password. Il secondo aspetto è relativo alla corretta educazione degli utenti nell'uso delle password. In particolare gli utenti devono essere invitati a non utilizzare mai due volte una stessa password. Questa pratica diminuisce la possibilità che la compromissione di un'utenza su un servizio personale permetta a un attaccante di accedere a un servizio aziendale solo perché il relativo utente ha utilizzato la stessa password per entrambe le utenze. Le password devono inoltre essere conservate in modo sicuro dall'utente (preferibilmente memorizzandole) evitando la proliferazione di documenti non protetti contenenti liste di credenziali o appunti facilmente accessibili da chiunque. A questo scopo potrebbe essere utile valutare l'impiego di software di supporto come i password manager che semplificano la gestione di un numero enorme di password in modo sicuro. Un contributo significativo alla semplificazione delle procedure di gestione delle password da parte degli utenti può essere dato dall'adozione a livello tecnico di soluzioni di Single Sign On (SSO) grazie alle quali una singola utenza può essere utilizzata per accedere a più servizi. In particolari contesti la gestionedelleidentitàdigitalipuòesseredemandataafornitoriterziingradodigarantirel'applicazion e corretta delle politiche sopra citate attraverso strumenti standardizzati integrabili all'interno delle infrastrutture informatiche aziendali. Vale la pena infine citare che anchea livello governativo il Sistema Pubblico di Identità Digitale (SPID) [10] fornisce una valida soluzione per gestire le utenze di cittadini che devono accedere in modo sicuro a servizi offerti dalla Pubblica Amministrazione. Da alcuni anni molti fornitori di servizi cloud permettono di migliorare la sicurezza delle utenze abilitando la cosiddetta autenticazione a due fattori. In questo caso l'utente, per poter accedere ai servizi protetti, oltre a dover inserire la propria password, dovrà fornire una ulteriore informazione segreta a cui avrà accesso attraverso un meccanismo

alternativo che non richiede necessariamente l'uso di internet (tipicamente un messaggio SMS, un token digitale o una smartcard). Duplicando i fattori richiesti per l'autenticazione si riduce la possibilità che, a seguito della compromissione di uno dei due (tipicamente la password), un attaccante possa accedere indebitamente a sistemi e servizi prima che l'utenza possa essere nuovamente messa in sicurezza. Ogni volta che questo sia tecnicamente ed economicamente possibile, l'autenticazione a due fattori dovrebbe essere sempre abilitata. È infine necessario che l'azienda imponga un corretto uso delle utenze, impedendo la condivisione delle stesse tra più persone e proteggendo gli accessi, siano essi locali o remoti, attraverso opportune tecnologie (es. canali cifrati). I diritti per l'accesso ai servizi, dispositivi e informazioni associati alle utenze dovrebbero essere gestiti secondo il criterio del minimo privilegio: ogni utente deve poter accedere esclusivamente a quanto strettamente necessario per lo svolgimento delle proprie mansioni. I diritti di accesso devono essere periodicamente aggiornati e le utenze non più in uso tempestivamente disabilitate.

- Gestione del sistema antivirus
- Gestione del sistema anti-intrusione
- Gestione del sistema di backup/restore:
    - Individuazione dei dispositivi
    - Individuazione degli archivi
    - Definizione delle frequenze
    - Definizione delle modalità (backup completo, incrementale, differenziale)
    - Definizione dei criteri di rotazione dei dispositivi
    - Definizione dei criteri di archiviazione dei dispositivi
    - Definizione delle procedure di verifica
    - Strumenti di segnalazione di eventuali errori
- Il regolamento 679/2016 inoltre, attribuisce rilievo anche al concetto di disaster recovery, che consiste nella capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute ad incidenti fisici o tecnici, allo scopo di ripristinare la disponibilità e l'accesso dei dati personali oggetto di trattamento. A tale riguardo, sarà quindi importante per i titolari predisporre un programma specifico attraverso cui analizzare innanzitutto i rischi che potrebbero andare a colpire il sistema informatico; prevedere poi le adeguate misure da adottare per minimizzarli; ed infine predisporre un piano di emergenza che permetta di attuare un sistema alternativo di elaborazione dei dati da utilizzare in attesa della completa riattivazione.
- Sistemi per assicurare la continuità di alimentazione
    - Sistemi ridondanti o ad alta affidabilità
    - RAID / Cluster / SAN …

- Procedure di sviluppo e avviamento di nuove applicazioni
- Gestione degli aggiornamenti dei programmi
- Organizzazione degli archivi degli utenti
- Protezione delle aree e dei locali (generali o specifici ai locali informatici)
    - Sistemi anti-intrusione
    - Vigilanza e controllo accessi
    - Sistemi anti-incendio.
- Prevenzione e mitigazione:

  La prevenzione degli incidenti di sicurezza parte dall'applicazione di buone pratiche per la messa in sicurezza dei sistemi informativi e dei computer, siano essi personali o aziendali. Su tutti i dispositivi è presente software, sotto forma di applicazioni e sistemi operativi, che deve essere aggiornato costantemente nel tempo per sanare vulnerabilità note. Le vulnerabilità sono rappresentate da difetti ed errori, involontariamente inseriti nel software dal produttore durante la sua realizzazione. Questi rappresentano dei punti deboli sfruttabili da criminali per compromettere il funzionamento dei sistemi o accedere illecitamente a informazioni e dati aziendali. All'identificazione di una vulnerabilità in un software segue normalmente il rilascio di un aggiornamento da parte del produttore. L'applicazione dell'aggiornamento risolve la vulnerabilità e impedisce che la stessa possa essere sfruttata da cyber-criminali per future intrusioni.

  Per tutti i motivi sopra citati è opportuno pertanto che:

    - l'azienda disponga delle licenze per il software impiegato in modo da poter accedere agli aggiornamenti offerti dal produttore in maniera tempestiva;
    - laddove possibile e ragionevole sia configurato l'aggiornamento automatico del software. Questo, in particolare, per i personal computer utilizzati dai dipendenti, che rappresentano spesso uno tra i bersagli più semplici da compromettere;
    - su tutti i sistemi sui quali non sia possibile un aggiornamento automatico, è opportuno che venga predisposto un processo di acquisizione delle patch, identificazione di quelle critiche e la loro successiva applicazione. La tempestività di questo processo è un fattore determinante, dato che nuove vulnerabilità possono essere sfruttate dagli attaccanti nel giro di poche ore dal momento del loro annuncio pubblico;
    - sia pianificata la dismissione del software non più supportato dal produttore e la sua sostituzione con prodotti per i quali gli aggiornamenti vengano garantiti.

  Laddove l'aggiornamento non fosse possibile (per motivi di continuità del servizio, economici, o altro) è necessario accettare il rischio residuo, possibilmente documentandolo, ed eventualmente

porre in essere opportune azioni di mitigazione (es. isolamento o distacco dalla rete del software non sicuro). Non si può escludere che i sistemi possano essere compromessi o violati anche nel caso di applicazione degli aggiornamenti. Questo potrebbe, ad esempio, accadere nel caso in cui una vulnerabilità fosse nota a cyber-criminali prima del rilascio del relativo aggiornamento da parte del produttore del software. In questo caso, la vulnerabilità prende il nome di 0-day, e risulta particolarmente pericolosa, proprio per l'assenza di una chiara strategia di protezione. In questi casi (relativamente rari) si possono adottare temporaneamente delle misure di mitigazione e contenimento, in attesa del rilascio di un aggiornamento che risolva la vulnerabilità.

FASE 4: MONITORING, ADEGUAMENTO E MIGLIORAMENTO

Per garantire una sicurezza sostenibile, le misure di sicurezza devono essere continuamente adattate alle nuove esigenze e ai cambiamenti del contesto. Necessarie misure e potenziali riconosciuti in audits o dall'analisi degli eventi ed eventuali incidenti o da rapporti, indagini ed altro, vengono integrati secondo l'approccio descritto sopra in modo sistemico e rintracciabile. Inoltre, si deve rispettare questo approccio anche per eventuali cambiamenti (changes) dei sistemi e/o componenti o nuovi progetti/sistemi.

La serie ISO/IEC 20000, IT service management, offre ulteriore sostegno per un sostenibile servizio sicuro. In tal modo si soddisfa la richiesta del regolamento (art. 32, 1d) per il test, la verifica e la valutazione periodica dell'efficacia delle misure adattate al fine di garantire la sicurezza del trattamento in modo sostenibile.

Per tanto l'azienda effettuerà almeno una volta l'anno un riesame dell'analisi dei rischi o al sopraggiungere di fattori interni ed esterni significativi sia dal punto di vista organizzativo, tecnico o legislativo.

FASE 5: CULTURA DELLA SICUREZZA

Un'adeguata cultura della sicurezza con una sensibilizzazione continua sia degli esperti che di tutti i responsabili ed incaricati, nonché l'impegno visibile del management promuovono l'attuazione sostenibile. Il continuo adeguamento interdisciplinare di procedure, metodi e strumenti in conformità alla serie ISO 27000 assicura un adempimento sostenibile del regolamento. In tal modo la sicurezza dell'informazione deve diventare parte integrante di una gestione aziendale responsabile e essere attuata ogni giorno da tutti come parte integrante dei processi di lavoro.

A parte della conformità legale, la valutazione dell'impatto sistemico ed interdisciplinare condotta con i responsabili, promuove anche la consapevolezza per la sicurezza, la comprensione per le interdipendenze

tra i trattamenti e componenti tecnici, come anche la trasparenza, l'efficienza, l'efficacia e la sistematica individuazione e riduzione di potenziali nuovi minacce. Studi scientifici dimostrano che un'adeguata garanzia per la protezione dei dati personali promuove la fiducia e la soddisfazione dei clienti/cittadini e dei collaboratori. Inoltre, si tutela la conoscenza e l'innovazione dell'organizzazione, assicurando il successo dell'azienda/organizzazione.

5. CONSERVAZIONE DEI DATI E GESTIONE DEGLI ARCHIVI

Gli elementi informativi da conservare costituiscono parte dei **beni** dell'azienda. Così come definito nella ISO 27002, per bene o asset si deve intendere: "*qualsiasi cosa cha abbia valore per l'organizzazione"* ed in particolare i dati personali o particolari categorie di dati.

L'azienda tratta dati personali di varia natura, appartenenti a diverse categorie di interessati, così come specificato nel registro trattamenti e queste informazioni sono quindi un *bene* da proteggere e gestire.

Ciascuno di questi dati è archiviato e conservato per il tempo strettamente necessario al perseguimento della finalità per la quale è iniziato il trattamento.

I responsabili degli asset devono definire, relativamente ai loro asset, appropriate regole di controllo di accesso, diritti di accesso e limitazioni per i ruoli specifici degli utenti, con un livello di dettaglio e una severità di controllo proporzionali al rischio relativo alla sicurezza delle informazioni.

Tale soggetto è tenuto, così come previsto nella lettera di incarico quale Incaricato al Trattamento, alla gestione dello stesso archivio in maniera da assicurare che la conservazione del dato sia effettuata per il periodo effettivamente necessario e stabilito dall'azienda nel Registro Trattamenti, così come, d'altra parte, comunicato all'interessato nell'informativa allo stesso resa ai sensi dell'art 13 e 14 del REG UE 679/2016.

Il controllo degli accessi è sia logico che fisico e questi aspetti devono essere considerati assieme.

Utenti e fornitori di servizi devono ricevere una chiara dichiarazione dei requisiti di business da soddisfare dai controlli di accesso a queste informazioni.

Nella concessione dei privilegi per accedere ad un archivio sia fisico che logico si devono tenere in conto i seguenti principi:

- **la necessità di conoscere (need-to-know)**: si è autorizzati ad accedere solo alle informazioni di cui si ha bisogno per eseguire i propri compiti (differenti compiti/ruoli implicano necessità differenti di conoscenza e quindi differenti profili di accesso);
- **la necessità d'uso (need-to-use)**: si è autorizzati ad accedere solo alle strutture di elaborazione delle informazioni (apparecchiature IT, applicazioni, archivi cartacei, locali) di cui si ha necessità per eseguire il proprio compito/lavoro/ruolo.

Questi principi sono utili anche a garantire la privacy by-design e by-default per ciò che riguarda la conservazione dei dati e gestione degli archivi.

Per tanto, l'azienda adotta un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi sia cartacei che digitale alle informazioni critiche.

Tutti gli utenti devono quindi:

1) mantenere riservate le informazioni segrete di autenticazione, assicurandosi che non vengano divulgate a nessun'altra terza parte, incluso personale con autorità;
2) evitare di tenere una registrazione (per esempio su carta, documenti software o dispositivi portatili) delle informazioni segrete di autenticazione, a meno che questa possa essere memorizzata in modo sicuro e il metodo di memorizzazione sia stato approvato (per esempio una cassaforte software per le password);
3) modificare le informazioni segrete di autenticazione ogni qualvolta vi sia un'indicazione della loro possibile compromissione;
4) quando le password sono usate come informazioni segrete di autenticazione, selezionare password di qualità con lunghezza minima sufficiente, che siano:
   a) facili da ricordare;
   b) non basate su qualcosa che qualcun altro possa facilmente indovinare od ottenere utilizzando informazioni relative alla persona, per esempio nomi, numeri di telefono e date di nascita, ecc.;
   c) non vulnerabili ad attacchi a dizionario (ossia non composte da parole incluse nei dizionari);
   d) prive di caratteri consecutivi identici, formate da soli caratteri alfanumerici o numerici;
   e) se temporanee, cambiate al primo log-on;
5) non condividere informazioni segrete di autenticazione di utenti individuali;
6) assicurare un'adeguata protezione delle password quando sono usate come informazioni segrete di autenticazione in procedure automatiche di log-on e sono memorizzate;
7) non usare le stesse informazioni segrete di autenticazione per scopi aziendali e non;
8) tenere in conto le misure minime di sicurezza di cui all'allegato B DEL CODICE PRIVACY (d. lgs 196/03) o altre prescrizioni successivamente imposte da norme di legge.

Ciascun archivio, cartaceo o digitale, pertanto, è sottoposto a controllo periodico da parte del dipendente che lo detiene ed a cui è affidato ovvero che ne è "responsabile".

Il dipendente che ha in gestione l'archivio (perché formalmente a lui affidato o a causa dell'espletamento dei suoi compiti in ragione del suo ufficio) assicura il rispetto della sicurezza di tali archivi, in particolare:

- provvedendo alla sicurezza fisica dell'archivio ovvero:
  - evitare l'accesso a persone non autorizzate;

  - conservare in modo appropriato le chiavi/badge per l'accesso all'archivio;
  - non lasciare l'archivio incustodito;
  - prestare le dovute accortezza in caso di calamità naturali, attacchi malevoli o accidenti.
- provvedendo a verificare periodicamente, ogni sei mesi, il contenuto dei suddetti archivi e a richiedere formalmente alla direzione aziendale l'autorizzazione alla cancellazione o distruzione dei dati il cui periodo di conservazione stabilito è terminato;
- provvedendo a tenere in cura l'archivio in maniera da poter assicurare l'esercizio dei diritti dell'interessato ed i conseguenti obblighi che il REG UE 679 2016 pone in capo all'azienda nella sua qualità di titolare, così come indicato nel precedente paragrafo DIRITTI DELL'INTERESSATO.

6. GESTIONE EVENTI ED INCIDENTI SULLA SICUREZZA PER LA PRIVACY E DATA BREACH

PROCEDURA DI NOTIFICAZIONE IN CASO DI INCIDENTE DI SICUREZZA

L'azienda ha implementato notevoli misure di sicurezza volte a proteggere adeguatamente i dati personali ed il loro trattamento.

Nel caso in cui, tuttavia, nonostante tali misure si sia verificata in azienda una violazione dei dati personali trattati, l'azienda assicura il rispetto degli obblighi di cui all'art 33 e 34 del REG UE 679/2016.

In particolare, qualsiasi soggetto che è autorizzato a trattare dati personali dell'azienda, ivi compresi i "Responsabili" e i soggetti "Incaricati al trattamento" dovrà, in caso di accertamento o anche semplice sospetto dell'accadimento di un incidente di sicurezza, comunicarlo prontamente e senza indugio all'organo amministrativo, anche tramite mail aziendale.

In ogni caso l'azienda notificherà la violazione all' Autorità Garante della Protezione dati personali competente entro 72 ore dal momento in cui l'azienda ha avuto conoscenza dell'accadimento. Se l'organo amministrativo non ritiene probabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche ne renderà opportuna documentazione anche con verbale di valutazione dell'accadimento datato e sottoscritto.

In caso di notifica all'autorità garante della protezione dei dati personali competente, la comunicazione dovrà contenere le prescrizioni di cui all'art 33 par 3 e, quindi dovrà almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Se la violazione dei dati personali avvenuta è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche l'azienda, ai sensi dell'art 34 REG UE 679/2016 e se l'azienda ritiene, in sede di analisi del data breach,

- di non aver messo in atto le misure tecniche e organizzative adeguate di protezione applicate ai dati personali oggetto della violazione;
- di non adottare misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- che la comunicazione richiederebbe sforzi sproporzionati;

comunicherà l'avvenuto data breach al soggetto interessato.

Nel caso in cui la comunicazione richiederebbe sforzi sproporzionati procederà ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati saranno informati con analoga efficacia.

SCOPO E CAMPO DI APPLICAZIONE

La presente procedura ha lo scopo di assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza all'interno dell'azienda a fornitori e clienti ed agli interessati in accordo al REG 679/2016 ed in particolare:

- definire cosa si intende per "Incidente di Sicurezza" e "data breach";
- definire le responsabilità delle persone incaricate di gestire gli incidenti di sicurezza;
- definire le modalità per permettere a tutta l'organizzazione di denunciare in modo tempestivo un "Incidente di Sicurezza";
- gestire in modo controllato gli "Incidenti di Sicurezza", in funzione della gravità dell'incidente ed intraprendere opportune azioni per la sua risoluzione;
- registrare gli incidenti in database aziendale che sia anche di riferimento come "lesson learned" per l'analisi dei futuri incidenti.

DEFINIZIONI E AMBITO DI APPLICAZIONE

Definizioni

- **Incidente di Sicurezza delle informazioni**: singolo evento o una serie di eventi indesiderati o inattesi relativi alla sicurezza delle informazioni che hanno una significativa probabilità di compromettere le operazioni di business e minacciare la sicurezza delle informazioni in termini di disponibilità, integrità o riservatezza. Rientra nell'ambito della definizione di incidente sulla sicurezza delle informazioni in modo particolare la *«violazione dei dati personali»* ovvero la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
- **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro dell'UE ai sensi dell'articolo 51 REG 679/2016;
- **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
  a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
  b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
  c) un reclamo è stato proposto a tale autorità di controllo;

Ambito di applicazione

Di seguito si forniscono indicazioni di ciò che può essere considerato un Incidente di Sicurezza. Queste non vogliono essere esaustive, ma hanno lo scopo di aiutare a comprendere il significato di Incidente di Sicurezza.

Si debbono denunziare come Incidenti di Sicurezza:

- la divulgazione di informazioni riservate a soggetti non autorizzati;
- la compromissione dell'integrità delle informazioni, corruzione di dati;
- l'indisponibilità momentanea o permanente delle informazioni necessarie durante le attività lavorative o legate all'erogazione di servizi;
- i comportamenti non conformi rispetto a politiche o linee guida sulla sicurezza delle informazioni;
- le violazioni di accesso ai sistemi (ad esempio: accessi logici non autorizzati);

- le violazioni di accesso alle soluzioni di sicurezza fisica (ad esempio: intrusione fisica da parte di personale non autorizzato);
- i malfunzionamenti di software o hardware (ad. es: Denial of Services, attacchi di virus, rallentamenti sospetti nelle attività di elaborazione delle informazioni, …);
- la perdita / il furto di dispositivi IT (pc, cellulari, …) o documenti cartacei;
- il danneggiamento dei sistemi IT, reti, risorse CED;
- la perdita / sottrazione di credenziali di accesso (ad esempio: perdita del badge);
- la messaggistica (sottrazione di e-mail, phishing, mail sospette…).

RESPONSABILITÀ

La Direzione ha designato per la corretta gestione degli incidenti di sicurezza delle informazioni le figure seguenti:

Incident Manager

Queste attività rientrano tra i compiti del Responsabile Protezione dei Dati (RPD) qualora nominato o in alternativa l'azienda identificherà la persona a cui affidare tale ruolo.

- L'"Incident Manager" è la persona preposta a:
  - raccogliere le segnalazioni di incidente;
  - valutare la loro gravità e se l'evento di sicurezza deve essere classificato come incidente per la sicurezza delle informazioni ed in particolare ai fini della privacy;
  - analizzare se un incidente presenta le caratteristiche di rischio elevato per i diritti e le libertà delle persone fisiche dialogando con il titolare del trattamento e con i responsabili del trattamento se necessario;
  - risolvere gli incidenti in tempi compatibili con i loro impatti sulla organizzazione attivando quando necessario lo '"Incident Response Team";
  - valutare l'efficacia delle azioni intraprese;
  - mantenere le registrazioni a documentazione delle attività fatte.
- L'" Incident Manager" ha la responsabilità della gestione del Team e di assicurare la gestione dell'incidente dalla presa in carico fino alla sua risoluzione.
- L'" Incident Manager" ha la responsabilità di comunicare tempestivamente incidenti classificati con gravità alta al titolare del trattamento.
- L'"Incident Manager" ha ancora la responsabilità di mantenere i contatti esterni alla Organizzazione nello interfacciare le autorità, gruppi di interesse esterni o forum che gestiscono questioni collegate agli incidenti relativi alla sicurezza delle informazioni.
- Effettua le sue attività in conformità a quanto previsto nel REG 679/2016 EU ed in particolare all'articolo 33, 34 e 55.

Incident Response Team - eventuale

Lo "Incident Response Team" è un team preposto a supportare lo "Incident Manager" nell'analisi e la risoluzione degli incidenti in relazione alle competenze dei partecipanti costituenti il team:

- Amministratore di Sistema – in relazione alle problematiche relative alla gestione degli assets di informatica individuale, CED e Reti e agli accessi logici;
- Responsabile di Sede o operativi – in relazione alle tematiche relative alle sedi e agli accessi fisici;

- Responsabile del Personale – in relazione alle tematiche relative alla gestione dei dipendenti e delle parti esterne (fornitori e outsourcers)
- Responsabili al trattamento dei dati – in relazioni a specifici eventi che possono riguardarli per l'identificazione delle cause o delle risoluzioni

MODALITÀ OPERATIVE

Segnalazione da parte di dipendenti e fornitori

Chiunque facente parte dell'Organizzazione o un fornitore che opera per conto della stessa si trovi in una delle circostanze indentificate o identificabili come incidente sulla sicurezza delle informazioni e della privacy, deve provvedere a riportare l'incidente allo "Incident Manager" in modo tempestivo, compilando il "Modulo Incidenti di Sicurezza" disponibile sul database aziendale nella parte "Segnalazione Incidente" e fornendo una descrizione accurata dell'incidente rilevato.

Segnalazione in arrivo da parte degli interessati

Viene messa a disposizione la casella di posta elettronica: ladisa.ristorazione@legalmail.it al fine di permettere a tutti gli interessati di inviare eventuali segnalazioni di potenziali eventi o incidenti sulla sicurezza.

Presa in carico, valutazione e Comunicazione

L' "Incident Manager" ricevuta la segnalazione, esamina se quanto segnalato si configuri effettivamente come incidente e dopo una analisi preliminare, classifica l'incidente per livello di gravità in funzione dell'impatto che l'incidente potrebbe avere sulla Organizzazione, fornendone la motivazione:

- Alto: l'incidente impatta in modo critico le attività della azienda con possibilità di danni economici, di perdita di business, di rivendicazioni anche legali del cliente o delle parti interessate o la violazione di dati personali in accordo al REG 679/2016 UE;
- Medio: l'incidente potrebbe avere impatti significativi sulle attività della azienda o per il rispetto della normativa vigente;
- Basso: l'incidente dovrebbe avere impatti poco significativi sulle attività della azienda o sul rispetto della normativa vigente.

Riporta quindi l'Incidente sul "Registro degli incidenti" e decide se coinvolgere lo "Incident Response Team" per la risoluzione dello stesso e le figure necessarie.

Per "Registro degli incidenti" si intende un archivio digitale o cartaceo che archivi i moduli del registro degli incidenti o un documento equivalente.

Inoltre l'Incident Manager ha il compito di custodire il registro degli incidenti in modo sicuro ovvero consentirne l'accesso solo alle figure al fine di non consentire a terzi di utilizzare le informazioni su una vulnerabilità per esercitare possibili azioni negative.

Qualora l'incidente venga classificato come "Alto" in accordo al reg 679/2016 ovvero in materia di dati personali o particolari si dovrà:

- In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
- Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
- La notifica deve includere almeno:
  a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
  c) descrivere le probabili conseguenze della violazione dei dati personali;
  d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

  Così come riportato nella modulistica allegata alla presente procedura.

- Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
- Il titolare del trattamento o per suo conto l'incident Manager documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
- Il titolare del trattamento o per suo conto l'incident Manager comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di

cui all'articolo 33, paragrafo 3, lettere b), c) e d) del regolamento 679/2016. Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1 del reg 679/2016;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 del regolamento 679/2016 è soddisfatta.

- Le registrazioni documentate sugli incidenti classificati con gravità Alta consentono all'autorità di controllo di verificare il rispetto del regolamento 679/2016.

Risoluzione incidente

L'"Incident Manager" esamina gli incidenti secondo la priorità assegnata al singolo incidente e con l'eventuale supporto del "Incident Response Team" valuta le cause che hanno originato l'incidente, esamina se ci sono stati casi analoghi in precedenza mediante il "Registro degli incidenti" e decide azioni di correzione, interpellando eventualmente gruppi di interesse esterni o forum che gestiscono questioni collegate agli incidenti relativi alla sicurezza delle informazioni come ad esempio il sito del garante o linee guida in materia.

Il "Trattamento" (per la soluzione contingente della problematica) e/o "Azione correttiva pianificata" (per la risoluzione alla radice della problematica) sono riportati sul "Modulo Incidenti di sicurezza" e sul "Registro degli incidenti" assieme al responsabile della attuazione e la data di implementazione prevista.

Una volta portata a termine la correzione, questa viene registrata sul "Modulo Incidenti di sicurezza" e sul "Registro degli incidenti" assieme al responsabile che ha attuato l'azione e la data di attuazione.

È responsabilità dell' "Incident Mgr" verificare l'efficacia della azione correttiva dopo un tempo che ritiene congruo per il conseguimento del risultato previsto e riportare il risultato delle attività sul "Modulo Incidenti di Sicurezza" e sul "Registro degli incidenti" e quindi comunicare detti risultati al titolare del trattamento.

L'"Incident Mgr" ha la responsabilità di comunicare l'esistenza di ogni incidente relativo alla sicurezza delle informazioni o di qualsiasi dettaglio pertinente con esso ad altro personale interno ed esterno o ad organizzazioni che abbiano la necessità di sapere.

7. RESPONSABILE PROTEZIONE DATI PERSONALI - DPO

7.1 CONSIDERAZIONI INIZIALI

Il Responsabile della Protezione dei dati è una nuova figura definita dal REG UE 679/2016 che deve necessariamente essere nominato dal titolare del trattamento o dal responsabile in presenza di determinati presupposti. In base all'articolo 37, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
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; oppure
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.

Il Gruppo di lavoro articolo 29 (WP29) ha fornito indicazioni rispetto ai criteri e alle formulazioni utilizzati nell'articolo 37, paragrafo 1.

7.2 VALUTAZIONE SULLE NECESSITÀ DI NOMINARE UN DPO

Di seguito sono riportate le valutazioni e analisi sulla necessità di nominare un responsabile protezione dati (RPD o DPO):

1. **Analisi obbligo punto a**: l'azienda non è un'autorità pubblica o da un organismo pubblico, per tanto non rientra in questa casistica.
2. **Analisi obbligo punto b**: le attività principali dell'azienda sono quelle indicate nel proprio oggetto sociale ed in particolare nel paragrafo 4 del presente manuale per tanto:

   2.1. *L'attività principale dell'azienda consta nel trattamento di dati personali* necessarie al raggiungimento degli obiettivi perseguiti dal titolare, le operazioni di trattamento dei dati sono una componente inscindibile delle attività svolta dal titolare/responsabile. Nel caso della erogazione di un servizio di pasti per una mensa scolastica l'attività principale è l'erogazione del servizio mensa che è connessa inscindibilmente con il trattamento dei dati degli utenti a cui il servizio è offerto.

   2.2. Per quanto concerne il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "monitoraggio del comportamento di detti interessati" ricomprendendovi senza dubbio tutte le forme di

tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati. L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29:

2.2.1. che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;

2.2.2. ricorrente o ripetuto a intervalli costanti;

2.2.3. che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

L'azienda eroga i propri servizi in modo continuo e quotidiano e questi trattamenti sono predeterminati, organizzati secondo procedure e sistemi ad esempio, per il servizio di fornire pasti alla popolazione scolastica e questo richiede un monitoraggio dei dati degli utenti ad esempio, in relazione ai pagamenti o in relazione alla definizione delle diete personalizzate:

- è "regolare" perché avviene ad intervalli periodici (ad esempio, con la sottoscrizione di eventuali moduli all'inizio dell'anno scolastico, o alla ricezione giornaliera delle diete);
- è "sistematico" in quanto avviene per sistema, in base ai dati raccolti e gestiti in diverse forme, quali ad esempio cartacee e digitali, al fine della gestione del servizio attraverso i diversi sistemi informativi; il tutto inoltre risulta regolato da diverse procedure ed istruzioni operative.

2.3. Per quanto riguarda il trattamento su "larga scala" In base all'articolo 37, paragrafo 1, lettere b) e c) del GDPR, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un DPO. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito. In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. A ogni

modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

2.3.1. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

2.3.2. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

2.3.3. la durata, ovvero la persistenza, dell'attività di trattamento;

2.3.4. la portata geografica dell'attività di trattamento.

Relativamente queste raccomandazioni, in termini assoluti in riferimento al servizio di mensa scolastica, in quanto i soggetti interessati del trattamento rappresentano l'intera popolazione scolastica che aderisce al servizio. *Per tanto, si ritiene, anche in via cautelativa, che il trattamento effettuato dall'azienda avvenga o possa avvenire su larga scala.*

Tutto ciò premesso l'azienda ritiene di essere tenuta al rispetto di questo obbligo **e quindi, in applicazione dell'art. 37 GDPR,** l'azienda ha nominato un Responsabile della Protezione dei dati personali.

Tuttavia, queste considerazioni saranno sottoposte ad aggiornamento e verifica al sopraggiungere di un cambiamento significativo nella attività dell'organizzazione.

7.3 CONOSCENZE E COMPETENZE DPO

In base all'articolo 37, paragrafo 5 DEL REGOLAMENTO, il DPO "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39". Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

3. Conoscenze specialistiche: Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il DPO avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del DPO, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

4. Qualità professionali: L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un DPO; tuttavia, sono pertinenti al riguardo la conoscenza da parte del DPO della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del Reg. UE 679/2019. Proficua anche la promozione di una formazione adeguata e continua rivolta ai DPO da parte delle Autorità di controllo. E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare; inoltre, il DPO dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.
5. Capacità di assolvere i propri compiti: Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del DPO, sia quanto dipende dalla posizione del DPO all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il DPO dovrebbe perseguire in via primaria l'osservanza delle disposizioni del GDPR. Il DPO svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.
6. DPO sulla base di un contratto di servizi: La funzione di DPO può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del GDPR; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal GDPR: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto DPO, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di DPO. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.

Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team DPO, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team DPO e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

L'azienda si è data i seguenti criteri relativi alla figura del DPO:

1) Utilizzare un:
    a. DPO esterno, nominato attraverso un contratto di servizio
    b. DPO interno, nominato attraverso atto di nomina

    In entrambi i casi dovranno essere garantiti i criteri di imparzialità, indipendenza e prevenire possibili conflitti d'interesse;

2) La figura della persona fisica che ricopre questo ruolo dovrà almeno:
    a. Avere un'esperienza lavorativa comprovata di 3 anni in settori affini a quello in cui opera l'azienda;
    b. Essere in possesso di una laurea triennale o equivalente nel settore ingegneristico o legale.
    c. Non trovarsi in conflitto di interessi con l'azienda;
3) Inoltre il DPO deve impegnarsi ad intraprendere un percorso formativo di crescita ed aggiornamento continuo del quale darà evidenza all'azienda su base annuale.

8. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA

8.1 CONSIDERAZIONI INIZIALI

Il REG. UE 679/2016 prevede che nel caso in cui vi sia un trattamento che comporti, in particolare l'uso di nuove tecnologie, e che, considerando la natura, l'oggetto, il contesto e le finalità del trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, sia necessario, prima di procedere al suddetto trattamento, compiere una valutazione di impatto dei trattamenti previsti sulla protezione dei dati personali ai sensi degli art 35 e ss.

Non è emersa l'obbligatorietà per l'azienda di procedere con la implementazione di una Valutazione di Impatto sulla Protezione dei Dati in accordo all'art 35 GDPR poiché non vi è stata evidenza del fatto che l'azienda operi un trattamento di dati che prevede l'uso di nuove tecnologie che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Infatti da quanto emerso l'azienda non effettua un trattamento che comporti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 del regolamento, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del regolamento; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

8.2 TRATTAMENTI EFFETTUATI DALL'AZIENDA E NECESSITÀ DI PROCEDERE AD UNA VALUTAZIONE DI IMPATTO

Riportata nei documenti:

- Metodologia per la conduzione valutazione di impatto sulla protezione dei dati
- Relazione relativa alla valutazione di impatto sulla protezione dei dati

9. VIDEOSORVEGLIANZA E RAPPORTO DI LAVORO

Vedi policy aziendale sui sistemi di videosorveglianza ed informativa ai dipendenti.

10. UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

La presente procedura disciplina l'utilizzo di sistemi e funzionalità di intelligenza artificiale (IA) nell'ambito delle attività aziendali, al fine di garantire un utilizzo corretto, controllato e trasparente delle tecnologie adottate, nel rispetto della normativa applicabile in materia di protezione dei dati personali e di intelligenza artificiale.

Allo stato attuale, l'intelligenza artificiale non viene utilizzata per assumere decisioni automatizzate relative a utenti, dipendenti, collaboratori, fornitori o altri soggetti interessati, né per determinare autonomamente l'accesso ai servizi aziendali o altri effetti giuridicamente rilevanti sulle persone.

L'unico utilizzo di IA attualmente individuato riguarda una funzionalità integrata nell'applicazione aziendale, attivata in occasione del primo accesso da parte dell'utente.

La procedura stabilisce pertanto le regole per la verifica, la gestione e il controllo di tale funzionalità, definisce le misure da adottare qualora l'utilizzo dell'intelligenza artificiale venga esteso ad altri ambiti aziendali e riguarda esclusivamente gli utilizzi di intelligenza artificiale connessi alle attività aziendali e non costituisce un'autorizzazione generale all'introduzione di ulteriori sistemi di IA.

RIFERIMENTI NORMATIVI

La procedura è predisposta tenendo conto dei seguenti riferimenti:

- Regolamento (UE) 2016/679 (GDPR), con particolare riferimento agli articoli 5, 6, 12, 13, 25, 28, 30, 32 e, ove applicabile, 35;
- D.Lgs. 30 giugno 2003, n. 196, e successive modificazioni;
- Regolamento (UE) 2024/1689, relativo all'intelligenza artificiale (AI Act), nelle disposizioni applicabili;
- eventuali ulteriori disposizioni nazionali ed europee applicabili al servizio erogato e ai rapporti contrattuali con le Pubbliche Amministrazioni.

L'azienda applica i principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, limitazione della conservazione, integrità e riservatezza.

DESCRIZIONE DELL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

L'azienda utilizza una funzionalità di intelligenza artificiale integrata nell'applicazione “Ladisa Ristorazione”, che interviene esclusivamente nella fase di primo accesso dell'utente.

La funzionalità è destinata a fornire assistenza iniziale e guidare l'utente nella configurazione dell'applicazione e non assume decisioni automatizzate, anche con la sola finalità di profilare l'utente.

In Ladisa S.r.l., l'IA non è mai impiegata per:

- assumere decisioni automatizzate riguardanti gli utenti o il personale;
- valutare le prestazioni dei dipendenti o dei collaboratori;
- selezionare o profilare lavoratori, utenti, fornitori o altri soggetti;
- determinare autonomamente l'ammissione o l'esclusione dai servizi di mensa;
- assumere decisioni in materia di assunzioni, organizzazione del lavoro, gestione del personale o affidamento di contratti;
- sostituire le valutazioni e le responsabilità decisionali della Direzione o del personale incaricato.

PRINCIPI GENERALI DI UTILIZZO

L'utilizzo dell'intelligenza artificiale deve rispettare i seguenti principi:

- Necessità e limitazione delle finalità: La funzionalità di IA deve essere impiegata esclusivamente per la finalità connessa al primo accesso dell'utente, evitando utilizzi ulteriori non preventivamente valutati e autorizzati.

- Minimizzazione dei dati: Devono essere trattati esclusivamente i dati personali necessari al funzionamento della funzionalità; devono essere evitati la raccolta e l'inserimento di dati eccedenti rispetto alla finalità prevista.

- Trasparenza: quando la funzionalità interagisce direttamente con una persona fisica e ricorrono i presupposti previsti dalla normativa applicabile, l'utente deve essere informato della natura artificiale dell'interazione.

- Supervisione e controllo: La Direzione aziendale mantiene il controllo sull'utilizzo della funzionalità e assicura che eventuali anomalie, reclami o utilizzi non conformi siano segnalati e gestiti.

- Sicurezza e riservatezza: l'accesso ai dati e alle funzioni amministrative dell'applicazione deve essere limitato ai soggetti autorizzati. Devono essere adottate misure tecniche e organizzative adeguate ai rischi del trattamento.

GESTIONE DELLA FUNZIONALITÀ DI IA NELL'APP

Prima dell'attivazione e durante l'utilizzo della funzionalità, l'azienda, con il supporto del fornitore dell'applicazione ove necessario, verifica che:

- sia documentata la finalità della funzionalità e sia chiaro in quale momento del primo accesso essa interviene;
- siano individuati i dati eventualmente raccolti, trasmessi, elaborati o conservati;
- sia verificato se i dati personali vengano comunicati a fornitori terzi o trasferiti al di fuori dello Spazio economico europeo;
- siano definite, per quanto di competenza dell'azienda, le modalità di conservazione e cancellazione dei dati;
- siano disponibili informazioni sufficienti sul funzionamento della funzionalità, sui limiti del sistema e sulle misure di sicurezza adottate;
- siano verificati i ruoli privacy del fornitore e l'eventuale necessità di un accordo ai sensi dell'articolo 28 GDPR;
- sia verificata la coerenza tra il funzionamento effettivo della funzionalità, l'informativa privacy e gli eventuali accordi con le Pubbliche Amministrazioni committenti.

L'azienda non autorizza l'utilizzo della funzionalità per trattamenti ulteriori rispetto a quelli verificati e approvati.

Qualora la funzionalità consenta agli utenti di inserire liberamente testi, documenti o altre informazioni, devono essere valutati i rischi di inserimento di dati personali non necessari, con particolare attenzione a dati relativi alla salute, alle esigenze alimentari individuali o ad altre informazioni appartenenti a categorie particolari di dati.

RAPPORTI CON I FORNITORI DEL SERVIZIO DI IA

Qualora la funzionalità di IA sia sviluppata o gestita da un fornitore esterno, l'azienda verifica, in relazione al ruolo effettivamente svolto dalle parti:

- l'identità del fornitore e le caratteristiche del servizio;
- le condizioni contrattuali di utilizzo;
- le misure di sicurezza applicate;
- le modalità di trattamento e conservazione dei dati;
- l'eventuale utilizzo dei dati per addestrare o migliorare modelli di IA;
- le condizioni per la cancellazione o restituzione dei dati;
- l'eventuale ricorso a subfornitori e i trasferimenti internazionali;
- le responsabilità delle parti in materia di protezione dei dati personali.

Quando il fornitore tratta dati personali per conto dell'azienda, è formalizzato, ove necessario, il rapporto ai sensi dell'articolo 28 GDPR.

L'azienda richiede al fornitore informazioni adeguate a consentire la verifica della conformità del servizio alle finalità autorizzate e agli obblighi applicabili.

VALUTAZIONE DEI RISCHI E MISURE DI SICUREZZA

L'azienda valuta i rischi connessi all'utilizzo dell'applicazione, considerando la natura dei dati trattati, le modalità di interazione con gli utenti, i soggetti coinvolti e le caratteristiche del servizio.

In particolare, Ladisa S.r.l. verifica:

- la possibilità di accessi non autorizzati o divulgazione dei dati;
- la presenza di dati personali eccedenti rispetto alla finalità;
- la conservazione non necessaria di conversazioni o registrazioni;
- l'eventuale riutilizzo dei dati da parte del fornitore;
- l'eventuale presenza di dati appartenenti a categorie particolari;
- le conseguenze di errori o risposte non corrette della funzionalità.

Qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, viene valutata la necessità di effettuare una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 GDPR.

Le misure di sicurezza sono individuate in modo proporzionato ai rischi effettivamente rilevati e sono riesaminate in occasione di modifiche significative del servizio.

GESTIONE DI ANOMALIE E INCIDENTI

Qualsiasi soggetto che rilevi un malfunzionamento della funzionalità di IA, un utilizzo non autorizzato, una divulgazione di dati o un possibile incidente di sicurezza deve darne tempestiva comunicazione al referente aziendale competente, nonché al DPO.

Il referente incaricato provvede a:

- registrare la segnalazione;
- coinvolgere il fornitore, se necessario;
- valutare la natura e la gravità dell'evento;
- adottare le misure correttive e di contenimento appropriate;
- informare il titolare del trattamento e il DPO, secondo le rispettive competenze;

- valutare gli eventuali obblighi di notifica al Garante e di comunicazione agli interessati, nei casi e nei termini previsti dal GDPR.

Le attività svolte e le misure adottate sono documentate secondo le procedure aziendali applicabili alla gestione degli incidenti e delle violazioni dei dati personali.

DIVIETO DI ESTENSIONE NON AUTORIZZATA

L'eventuale introduzione di nuove funzionalità di IA, o l'estensione di quelle esistenti ad altri processi aziendali, deve essere preventivamente sottoposta alla Direzione e alla funzione incaricata della privacy.

Prima dell'attivazione devono essere valutati, secondo necessità:

- la finalità e le modalità di utilizzo;
- i dati personali coinvolti;
- la base giuridica del trattamento;
- le informazioni da fornire agli interessati;
- i rischi per i diritti e le libertà delle persone;
- gli eventuali obblighi derivanti dall'AI Act;
- gli accordi con fornitori e committenti;
- le misure di sicurezza e le responsabilità interne.

Nessuna nuova funzionalità può essere introdotta sulla sola base della disponibilità tecnica del servizio o di una richiesta informale del personale.

11. INFORMAZIONI SULLA SOCIETÀ

Ladisa S.R.L.

Via Guglielmo Lindemann 5/3 – 5/4 Bari (BA)

Versione	Data approvazione	Principali modifiche dalla versione precedente	A cura di:
0	30/07/2018	Prima emissione	Consulenti esterni
01	26.10.2026	Seconda emissione	Consulenti esterni