G.D.P.R.

GENERAL DATA PROTECTION REGULATION

ADEGUAMENTO NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

RELAZIONE DOCUMENTALE

VERIFICATA E PRODOTTA

martedì 18 maggio 2021

RAGIONE SOCIALE

PERTUR SRL

SEDE LEGALE

VIA G.PIZZI 45, 63074 S.BENEDETTO DEL TR. ()

C.F./P.IVA

01853400446

CONTATTI
+39 0735 594456
+39 0735 595419
+39 370 3328674
info@pertur.it
PEC: pertur@postcert.it

INDICE

1. PREMESSA
2. SISTEMI DI SICUREZZA PRESENTI IN AZIENDA
3. SEDI E UFFICI
4. DATA PROCESSOR ESTERNI
5. DATA HANDLER
6. NOMINE INCARICATI
7. SISTEMI DI ELABORAZIONE
8. REGISTRO DEI TRATTAMENTI
9. BANCHE DATI
10. PRIVACY IMPACT ASSESSMENT

CONTATTI
+39 0735 594456
+39 0735 595419
+39 370 3328674
info@pertur.it
PEC: pertur@postcert.it

PREMESSA

Ogni elemento contenuto in questo documento è stato elaborato, creato e predisposto in conformità alle nuove disposizioni in vigore al regolamento GDPR, ogni dato è stato misurato con il pieno rispetto della legittima realtà presente alla data di creazione del suddetto documento di comune accordo con il DATA CONTROLLER FRANCESCO MARONI e il DATA PROCESSOR VALENTINA CAPANNA.

Le valutazioni, i rimedi e le condizioni che emergono sono connessi al principio della buona fede e della diligenza nell'attuare tutti i processi utili che vengono e verranno predisposti per renderne minima la probabilità di accadimento di eventi negativi.

La conservazione ed il trattamento del dato creato ed evidenziato nelle relazioni sottostanti determinano il PIA aziendale (Privacy Impact Assessment = censimento degli impatti privacy), in cui si vuole valutare la rischiosità complessiva, le azioni intraprese e da intraprendersi creando un documento che fotografa la situazione corrente.

Il nostro PIA nasce con un piano interno in cui viene stabilito in quale modo verrà mitigato il singolo rischio, coloro che sono incaricati di operare in tal senso e la gestione utile prevista per l'attività.

La mitigazione del Rischio, la privacy by design e gli strumenti di sicurezza utilizzati per il trattamento del dato personale vogliono diventare per l'azienda un'importante base per l'approccio al Sistema Privacy.

Questo planning operativo è e sarà costantemente monitorato, avrà impatto sul Privacy Impact Assessment in cui andremo ad evidenziare i miglioramenti ottenuti e le eventuali ulteriori rischiosità subentrate nel corso dei periodi di esercizio.

Grazie ai nostri fornitori ci siamo dotati di un sistema informatico atto a censire, valutare, monitorare lo stato di rischio e implementando automaticamente il reporting necessario e le comunicazioni operative per le varie risorse.

Il nostro PIA è disegnato per raggiungere tre obiettivi:

- Garantire la conformità con le normative, e requisiti di politica legali applicabili per la privacy;
- Determinare i rischi e gli effetti che ne conseguono;
- Valutare le protezioni e eventuali processi alternativi per mitigare i potenziali rischi per la privacy.

Data Processor	Data Controller
VALENTINA CAPANNA	**FRANCESCO MARONI**

SISTEMI DI SICUREZZA PRESENTI IN AZIENDA

I Dati Aziendali sono un patrimonio fondamentale e vanno protetti con la massima attenzione e prevenzione. Solitamente riguardano informazioni di basilare importanza per il proprio business. Il danneggiamento o la perdita anche parziale di alcuni di essi (dovuta a guasti delle apparecchiature, virus, spam, errori umani, furti, od altri eventi) può rappresentare un evento disastroso per l'azienda ed un grosso danno economico.
Come noto la sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi. Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e l'elaborazione a distanza (informatica distribuita). In particolare non è da sottovalutare il rischio cui può andare incontro il trasferimento elettronico dei fondi tra banche oppure il trasferimento da uno Stato all'altro di intere basi di dati reso possibile dai moderni sistemi di trasmissione telematica.

Riguardo l'aspetto "sicurezza" connesso alla rete telematica essa può essere considerata una disciplina mediante la quale ogni organizzazione che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati. Un bene può essere un'informazione, un servizio, una risorsa hardware o software e può avere diversi modi possibili di interazione con un soggetto (persona o processo). Se, ad esempio, il bene è un'informazione, ha senso considerare la lettura e la scrittura (intesa anche come modifica e cancellazione); se invece il bene è un servizio, l'interazione consiste nella fruizione delle funzioni offerte dal servizio stesso.

Nell'ottica del regolamento europeo n. 2016/679 (GDPR) questo concetto di sicurezza informatica ha assunto un significato più attuale alla luce anche dei sempre più numerosi attacchi ed incidenti di natura informatica che lasciano intuire una preoccupante tendenza alla crescita di tale fenomeno.

In particolare negli ultimi tempi si è assistito ad una rapida evoluzione della minaccia che possiamo definire "cibernetica" che è divenuta un bersaglio specifico per alcune tipologie di attaccanti particolarmente pericolosi.

I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi:
- il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si riflette sulla sofisticazione delle strategie e degli strumenti utilizzati;
- il secondo è rappresentato dal fatto che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti.

La combinazione di questi due fattori fa sì che, a prescindere dalle misure minime di sicurezza previste dal nostro codice in materia di protezione dei dati personali, (antivirus, firewall, difesa perimetrale, ecc.) bisogna fare particolare attenzione alle attività degli stessi utenti che devono rimanere sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto

della macchina attraverso una scalata ai privilegi.

Ciò ovviamente comprende anche misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il Data Processor VALENTINA CAPANNA e il Data Controller FRANCESCO MARONI devono valutare anche il rischio informatico che può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

Nel GDPR un chiaro riferimento alle misure di sicurezza già si trova nell'art. 24 quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability).

A questo riguardo PERTUR SRL in accordo con i propri consulenti IT ha delineato negli anni una protezione perimetrale che posa garantire standard adeguati di sicurezza e a tal proposito dichiara che il patrimonio aziendale relativo alla sicurezza è elencato qui sotto.

Antivirus Installati

antivirus commerciale, antivirus centralizzato, antivirus centralizzato con monitoraggio attività file, antivirus centralizzato con gestione delle patch di aggiornamento, antivirus centralizzato con modalità protetta per operazioni bancarie

Firewall Installati

firewall software

Crittografia in Essere

nessuna crittografia presente

Dispositivi USB aziendali

dispositivo usb semplice, penne usb con fingerprint

Sistemi di backup

HD Esterno

Frequenza backup: Settimanale
Modalità di ripristino: Copia e ripristino softwares e dati
Tempi di ripristino: 1 giorno

Tipo backup: sistema di backup locale commerciale
Ripristino gestionale, posta e dati da backup locale

Protezione generica

Per quanto riguarda la parte delle risorse umane, PERTUR SRL ha predisposto le seguenti misure per aumentare la consapevolezza dell'importanza dei dati:

- **consegna del mansionario**
- **formazione del personale**
- **nomina incaricato**
- **consegna delle policy**
- **autenticazione utenti**

Il Regolamento Generale sulla Protezione dei dati **si applicherà quindi sia ai dati detenuti in forma elettronica** (es. email e database) **che cartacea** (con poche eccezioni). Ciò significa che l'azienda è responsabile anche degli archivi cartacei che devono essere conservati in modo sicuro e, quando non più necessari, devono essere distrutti in sicurezza, grazie ad un distruggi documenti conforme alla nuova normativa. A questo proposito PERTUR SRL dichiara di aver predisposto la seguente protezione ambientale per il cartaceo:

- **armadi con chiave**
- **contenitori con chiave**
- **sistema di allarme**
- **distruggi documenti**
- **estintori**
- **pseudonimizzazione**

La corretta conservazione di tutto l'apparato informatico rappresenta la prima difesa a protezione dei dati digitale. Una cattiva o non adeguata manutenzione dei sistemi informativi è spesso la causa di intrusioni e/o danneggiamenti con conseguente perdita di dati. A questo proposito PERTUR SRL dichiara di aver predisposto per tutte le apparecchiature informatiche la seguente policy:

- **gruppi di continuità**
- **manutenzione spot apparecchiature**
- **manutenzione programmata apparecchiature**
- **aggiornamento interno dei software**

Cancellazione sicura

Nell'azienda, i dispositivi che vengono ELIMINATI subiscono una cancellazione sicura mediante distruzione preventiva delle memorie di massa.
Non si effettua la vendita dei dispositivi dismessi.
Non si effettua la rotazione dei dispositivi.

SEDI E UFFICI

L'azienda PERTUR SRL dichiara di avere le seguenti sedi al cui interno sono presenti i seguenti uffici dove risiedono i dati sia digitali che cartacei.

Pertur Viaggi
Via G. Pizzi 45 - 63074, San Benedetto del tronto (AP)

- Ufficio privato Direttore
- Ufficio e biglietteria al pubblico

DATA PROCESSOR ESTERNI

Nella suddetta sezione vengono nominati tutti i data processor esterni all'azienda PERTUR SRL, le figure presenti hanno ricevuto la documentazione di informazione all'adeguamento al GDPR, hanno firmato ed accettato le lettere di incarico e i mansionari e le relative policy di sicurezza

---

Studio Luciani

Consulente Commercialista

Consulente Commercialista, contabilità, buste paga e gestione fiscale dipendenti.

Data processor esterno STUDIO LUCIANI

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione

DATA HANDLER

La **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" in particolare, art. 4, n. 10, del regolamento. Quindi anche se il GDPR non prevede la figura autonoma dell'incaricato, questo non vieta che se il titolare o il responsabile del trattamento, oltre a fare tutto quello che il regolamento espressamente prevede per "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile", vogliono anche fare (su base volontaria) una ulteriore responsabilizzazione di queste persone attraverso una specifica lettera di attribuzione di incarico e identificare queste persone utilizzando il termine "Incaricato" lo possono fare. Questa modalità operativa potrebbe anche essere considerata una buona prassi volta a poter ulteriormente sostenere la dimostrabilità della compliance al GDPR. Ma questa facoltà non deve essere intesa come un obbligo normativo come lo è invece per il Codice Privacy la nomina a incaricato prevista dall' art. 30, che al punto 2 prevede che la designazione dell'incaricato sia effettuata per iscritto e che nell'atto di nomina si debba individuare puntualmente l'ambito del trattamento consentito.

L'azienda PERTUR SRL in accordo con quanto affermato dal Garante per la protezione dei dati italiano ha deciso di nominare le figure dei data Handler, ovvero coloro che gestiscono e trattano il dato per nome dell'azienda. Si premette che ogni singolo individuo persona fisica o giuridica ha firmato e ricevuto le lettere di incarico, i mansionari e la policy privacy.

Data handler VALENTINA CAPANNA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione

Data handler FRANCESCO MARONI

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione

NOMINE INCARICATI

L'azienda PERTUR SRL per essere totalmente compliant alle direttive del nuovo regolamento europeo della privacy ha deciso di fare le seguenti nomine delle figure aziendali previste dalla normativa:

Data controller
- FRANCESCO MARONI

Data processor
- VALENTINA CAPANNA

MOTIVAZIONI PER LA MANCATA NOMINA DEL D.P.O.:

Il Regolamento UE 2016/679 NON prevede l'
obbligo
di designazione
del
Data Protection Officer per piccole aziende come Pertur srl.

SISTEMI DI ELABORAZIONE

L'azienda PERTUR SRL identifica in questa sezione tutti i sistemi di elaborazione elettronici collegati e/o di proprietà dell'azienda, dichiarando che ogni strumento è conforme alla legge Europea e protetto con adeguati sistemi conformi alle direttive dettate dal GDPR.

Server Easy e client

TIPOLOGIA: Server
UBICAZIONE: SEDE: Uffici servizi al pubblico e uffici privati, UFFICIO: Ufficio e biglietteria al pubblico
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: maggio 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

Postazione 1

TIPOLOGIA: Client
UBICAZIONE: SEDE: Uffici servizi al pubblico e uffici privati, UFFICIO: Ufficio e biglietteria al pubblico
AMBIENTE: Windows 10 Home
DATA ACQUISTO: marzo 2017

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

Postazione 2

TIPOLOGIA: Client
UBICAZIONE: SEDE: Uffici servizi al pubblico e uffici privati, UFFICIO: Ufficio e biglietteria al pubblico
AMBIENTE: Windows 10 Home
DATA ACQUISTO: aprile 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

PC Direttore

TIPOLOGIA: Client
UBICAZIONE: SEDE: Uffici servizi al pubblico e uffici privati, UFFICIO: Ufficio privato Direttore
AMBIENTE: Windows 10 Home
DATA ACQUISTO: febbraio 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

REGISTRO DEI TRATTAMENTI

Ai sensi dell'art. 30, par. 4. del **Regolamento europeo in materia di protezione dei dati personali** è previsto che "su richiesta, il Titolare del trattamento o il Responsabile del trattamento e, ove applicabile, il rappresentante del Titolare del trattamento o del Responsabile del trattamento, mettono il registro a disposizione dell'autorità di controllo."

L'obbligo di documentazione della conformità della propria organizzazione alle prescrizioni della legge. Obbligo che grava anche sul responsabile, per i trattamenti che questi svolga per conto di un titolare.

L'autorità di controllo (Garante) è, d'altro canto, l'ente pubblico che ha titolo per richiedere la disponibilità del registro, al fine di esaminarlo.

L'obbligo di redazione e adozione del registro non è, tuttavia, generale. Il par. 5 dell'art. 30 specifica che esso non compete "alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."

La società PERTUR SRL ha deciso tuttavia di attuare la redazione del registro come caldeggiato dal gruppo di lavoro Ex articolo 29 ispirandosi alle seguenti ulteriori finalità:

- rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;
- costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

CONTATTI
+39 0735 594456
+39 0735 595419
+39 370 3328674
info@pertur.it
PEC: pertur@postcert.it

Rubrica mail - Rubrica contatti mail

- **Queste le categorie interessati:**
  Clienti, Potenziali clienti, Personale dipendente, Agenti e rappresentanti e commerciali, Soci, associati ed iscritti, Fornitori

- **Queste le categorie destinatari:**
  Soci associati ed iscritti, Clienti, Fornitori, Potenziali clienti o fornitori

- **I dati sono trattati in queste modalità:**
  Elettronica

- **Le finalità del trattamento:**
  L'azienda PERTUR SRL, tramite il trattamento "Rubrica mail", tratta i sopraindicati dati per: **CONTATTARE ED INVIARE SERVIZI ED INFORMAZIONI RICHIESTE AI CLIENTI**

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "Rubrica mail" non vengono trattati dati riguardanti i minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "Rubrica mail" non vengono trattati dati sanitari, biometrici e giudiziari

- **Durata del trattamento:**
  Il trattamento "Rubrica mail" ha una durata indefinibile:
  L'azienda PERTUR SRL dichiara il trattamento "Rubrica mail" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno cancellati.

- **Profilazione:**
  Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**
  I dati non vengono trasferiti in paesi extra UE

Gestionale - Database Gestionale Easy ADV

- **Queste le categorie interessati:**
  Clienti, Potenziali clienti, Personale dipendente, Fornitori

- **Queste le categorie destinatari:**
  Consulenti e liberi professionisti in forma singola o associata, Altre amministrazioni pubbliche, Clienti, Fornitori, Potenziali clienti o fornitori

- **I dati sono trattati in queste modalità:**
  Elettronica e cartacea

- **Le finalità del trattamento:**
  L'azienda PERTUR SRL, tramite il trattamento "Gestionale", tratta i sopraindicati dati per: **GESTIONE DATI E DOCUMENTI FISCALI E PREVENTIVI, CLINETI E FORNITORI**

  Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "Gestionale" non vengono trattati dati riguardanti i minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "Gestionale" non vengono trattati dati sanitari, biometrici e giudiziari

- **Durata del trattamento:**
  Il trattamento "Gestionale" ha una durata indefinibile:
  L'azienda PERTUR SRL dichiara il trattamento "Gestionale" con data indefinita in quanto continuerà a tenerlo in vita per poter proseguire la propria attività.
  Il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta raggiunte le finalità del presente trattamento, i dati verranno cancellati.

- **Profilazione:**
  Il trattamento non riguarda processi automatizzati o di profilazione

- **Trasferimento dei dati di questo trattamento:**
  I dati non vengono trasferiti in paesi extra UE

BANCHE DATI

L'azienda PERTUR SRL identifica in questa sezione tutte le banche dati, i campi che le compongono e la tipologia di questi ultimi. Tali banche dati vengono utilizzate nei trattamenti secondo le direttive dettate dal GDPR.

Trattamento "Gestionale"

Easy ADV - (sistema di backup: HD Esterno)

Gestione Contabile (Dati personali)

Trattamento "Rubrica mail"

Rubrica mail - (sistema di backup: HD Esterno)

Rubrica mail (Dati personali)

PRIVACY IMPACT ASSESSMENT

L'azienda PERTUR SRL espone qui di seguito le valutazioni di impatto sulla privacy dei trattamenti sopra elencati.

PRIVACY IMPACT ASSESSMENT TRATTAMENTO **Gestionale**

L'azienda PERTUR SRL con sede in VIA G.PIZZI 45, 63074 - S.BENEDETTO DEL TR., nell'ottica di assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

PERTUR SRL effettua il seguente trattamento: **Gestionale** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L'azienda PERTUR SRL, tramite il trattamento "Gestionale", tratta i sopraindicati dati per: **GESTIONE DATI E DOCUMENTI FISCALI E PREVENTIVI, CLINETI E FORNITORI**

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Dopo attenta valutazione di comune accordo con il Data Controller FRANCESCO MARONI e il Data Processor VALENTINA CAPANNA; PERTUR SRL considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **Easy ADV,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

PERTUR SRL, per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria

Comunicazione illegale dei dati e dei documenti
Copia abusiva
Degrado dei supporti e delle apparecchiature
Cortocircuito elettrico
Distruzione di apparecchiature o di supporti
Fenomeni meteorologici
Furto Apparecchiature
Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software
Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo
Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:
Aggiornamento interno dei software
Autenticazione utenti
Antivirus centralizzato con gestione delle patch di aggiornamento
Antivirus centralizzato con monitoraggio attività file
Manutenzione programmata apparecchiature
Antivirus centralizzato con modalità protetta per operazioni bancarie
Antivirus commerciale
Penne USB con fingerprint
Gruppi di continuità
Antivirus centralizzato
Manutenzione spot apparecchiature

Tali mitigazioni danno al trattamento **Gestionale** una compliance alla sicurezza del **77%**

La sua valutazione ci porta ad affermare che per fatturato aziendale, importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice

L'azienda PERTUR SRL,individuate tali vulnerabilità le cui performances di mitigazione sono considerate migliorabili, predispone i seguenti interventi atti a incrementare la compliance alla sicurezza:
maggio 2021: Server Easy e client (da attuare)

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una policy di sicurezza la cui visione è disponibile nella sezione policy di sicurezza.
Il Data Controller FRANCESCO MARONI e il Data Processor VALENTINA CAPANNA dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

S.BENEDETTO DEL TR., li 18/05/2021

Il Data Controller FRANCESCO MARONI .....

Il Data Processor VALENTINA CAPANNA .....

PRIVACY IMPACT ASSESSMENT TRATTAMENTO **Rubrica mail**

L'azienda PERTUR SRL con sede in VIA G.PIZZI 45, 63074 - S.BENEDETTO DEL TR., nell'ottica di assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

PERTUR SRL effettua il seguente trattamento: **Rubrica mail** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L'azienda PERTUR SRL, tramite il trattamento "Rubrica mail", tratta i sopraindicati dati per: **CONTATTARE ED INVIARE SERVIZI ED INFORMAZIONI RICHIESTE AI CLIENTI**

Il Data Processor e il Data Controller vigilano per garantire agli interessati che i dati saranno trattati solo per la finalità dichiarata e solo per la parte strettamente necessaria al trattamento. Si impegnano inoltre, entro i limiti della ragionevolezza, a modificare e correggere tutti i dati che risultano nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultano eccedenti al trattamento dichiarato.

Dopo attenta valutazione di comune accordo con il Data Controller FRANCESCO MARONI e il Data Processor VALENTINA CAPANNA; PERTUR SRL considera questo trattamento essenziale e indispensabile per il corretto perseguimento dell'oggetto sociale cosi come la sua proporzionalità e non eccedenza. A tale proposito è stato effettuato un ridimensionamento delle banche dati **Rubrica mail,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

PERTUR SRL, per garantire una sempre maggiore libertà dei diritti e sicurezza dei dati agli interessati si sforza continuamente di trovare le migliori mitigazioni a tutti i rischi ai quali i dati in nostro possesso possono andare incontro.

in particolare segnaliamo di aver individuato i seguenti rischi:
Accessi esterni non autorizzati
Allagamento
Alterazione dolosa o colposa dati avvenuta internamente
Attacco Ransomware
Azione di virus informatici o di codici malefici
Carenza di consapevolezza, disattenzione o incuria
Comunicazione illegale dei dati e dei documenti
Copia abusiva
Degrado dei supporti e delle apparecchiature
Cortocircuito elettrico
Distruzione di apparecchiature o di supporti
Fenomeni meteorologici
Furto Apparecchiature
Incendio
Ingressi non autorizzati a locali/aree ad accesso ristretto
Malfunzionamento hardware o software
Mancanza di continuità di alimentazione elettrica
Mancata manutenzione del sistema informativo

Perdita credenziali
Polvere, corrosione o gelo
Possibile rottura dell'hard disk o altri componenti hardware/software
Accessi tramite dispositivi mobili non autorizzati
Errato utilizzo doloso o colposo del software
Mancata distruzione o restituzione dei supporti raggiunta la finalità

Dei sopraelencati rischi, in accordo con i consulenti IT abbiamo posto in essere le seguenti mitigazioni:
Aggiornamento interno dei software
Autenticazione utenti
Antivirus centralizzato con gestione delle patch di aggiornamento
Antivirus centralizzato con monitoraggio attività file
Manutenzione programmata apparecchiature
Antivirus centralizzato con modalità protetta per operazioni bancarie
Antivirus commerciale
Penne USB con fingerprint
Gruppi di continuità
Antivirus centralizzato
Manutenzione spot apparecchiature

Tali mitigazioni danno al trattamento **Rubrica mail** una compliance alla sicurezza del **74%**

La sua valutazione ci porta ad affermare che per fatturato aziendale, importanza dei dati di questo trattamento e principio di proporzionalità il trattamento stesso ha una valutazione di impatto più che accettabile.
Tuttavia segnaliamo anche che sono stati individuate alcune criticità che possono mettere a rischio i dati anche se in misura minimale. A questo proposito segnaliamo:
Dispositivo USB semplice

L'azienda PERTUR SRL,individuate tali vulnerabilità le cui performances di mitigazione sono considerate migliorabili, predispone i seguenti interventi atti a incrementare la compliance alla sicurezza:
maggio 2021: USB finger print (da attuare)

Infine, per sensibilizzare tutti i dipendenti incaricati al trattamento ad una sempre maggiore attenzione alla protezione dei dati abbiamo realizzato e consegnato a ciascuno una policy di sicurezza la cui visione è disponibile nella sezione policy di sicurezza.
Il Data Controller FRANCESCO MARONI e il Data Processor VALENTINA CAPANNA dichiarano di aver ottemperato a quanto richiesto dal GDPR in base al principio di proporzionalità, all'importanza e la quantità dei dati in loro possesso e ai fatturati aziendali

S.BENEDETTO DEL TR., li 18/05/2021

Il Data Controller FRANCESCO MARONI .....

Il Data Processor VALENTINA CAPANNA .....