Automotive

G.D.P.R.

GENERAL DATA PROTECTION REGULATION

ADEGUAMENTO NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

RELAZIONE DOCUMENTALE

VERIFICATA E PRODOTTA

martedì 8 marzo 2022

RAGIONE SOCIALE

KH Automotive s.r.l.

SEDE LEGALE

Zona Industriale Tito Scalo, 85050 Potenza (PZ)

C.F./P.IVA

01470450766

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

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 Anna Patrone e il DATA PROCESSOR Anna Patrone.

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
Anna Patrone	**Anna Patrone**

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 Anna Patrone e il Data Controller Anna Patrone 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 KH Automotive s.r.l. 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, antivirus centralizzato con mdm - mobile device management, antivirus centralizzato con dlp - data loss prevention

Firewall Installati
firewall hardware, firewall vpn/ids/ips

Crittografia in Essere
crittografia di file e cartelle

Dispositivi USB aziendali
penne usb con fingerprint

Sistemi di backup
Xopero Backup & Restore
Frequenza backup: Giornaliera
Modalità di ripristino: Tramite software Xopero

Tempi di ripristino: Tempo necessario al recovery da rete LAN
Tipo backup: sistema di backup locale commerciale

ServerAS400

Frequenza backup: Giornaliera
Modalità di ripristino: Immediata
Tempi di ripristino: Immediati
Tipo backup: sistema di backup locale commerciale
Backup con sistema a nastro interno

Protezione generica

Per quanto riguarda la parte delle risorse umane, KH Automotive s.r.l. 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**
- **registrazione accessi**

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 KH Automotive s.r.l. dichiara di aver predisposto la seguente protezione ambientale per il cartaceo:

- **armadi con chiave**
- **armadi blindati**
- **armadi ignifughi**
- **sistema di allarme**
- **distruggi documenti**
- **estintori**
- **sistema antincendio**

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 KH Automotive s.r.l. 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 KH Automotive s.r.l. dichiara di avere le seguenti sedi al cui interno sono presenti i seguenti uffici dove risiedono i dati sia digitali che cartacei.

KH Automotive s.r.l
Zona Industriale - 85050, Tito Scalo (Potenza)

- Uffici amministrativi
- Stanza di Patrone Anna
- Stanza di Cetani Gianni
- Stanza di Lafiosca Sandro
- Stanza di Patrone Nicola Maria
- Reception
- CED
- Stanza di Mongiello Michele
- Stanza di Patrone Paolo
- Stanza di Giordano Mario

DATA PROCESSOR ESTERNI

Nella suddetta sezione vengono nominati tutti i data processor esterni all'azienda KH Automotive s.r.l., 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

---

csimpresa
Troia Donato

Opera Soc. Coop.
Lovallo Anna & Tamburrino Gerardo Giuseppe

Data processor esterno CSIMPRESA

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
Gestione contabilità	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Gestione dati dei clienti e dei fornitori	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data processor esterno OPERA SOC. COOP.

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
Gestione contabilità	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Gestione dati dei clienti e dei fornitori	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

DATA HANDLER

Ai sensi dell'art. 4, n. 10, il Regolamento non esclude la presenza della **figura dell' "incaricato" al trattamento** (ex art. 30 Codice Privacy), in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".Infatti, seppur non sia prevista espressamente come figura autonoma, ciò non vieta al titolare (o al responsabile del trattamento) di definire volontariamente un'ulteriore responsabilizzazione di tali soggetti attraverso una specifica lettera di designazione come "Incaricati". Questo non esclude tutto quello che il Regolamento prevede espressamente per "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Tale modalità è da considerarsi una buona prassi volta a poter ulteriormente sostenere la dimostrabilità della compliance al GDPR. Tuttavia questa facoltà non deve essere intesa come un obbligo normativo, differentemente dalla nomina a incaricato prevista dall' art. 30 punto 2 del Codice Privacy, dove è previsto che la designazione dell'incaricato sia effettuata per iscritto e che nell'atto di nomina debba essere puntualmente individuato l'ambito del trattamento consentito.

L'azienda KH Automotive s.r.l. in accordo con quanto affermato dal Garante italiano per la protezione dei dati personali 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 ricevuto e firmato le relative lettere di incarico, i mansionari e la policy privacy.

Data handler GIANNI CETANI

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
Gestione dati dei clienti e dei fornitori	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Gestione contabilità	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler ANNA PATRONE

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
Gestione dati dei clienti e dei fornitori	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Gestione contabilità	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler ANTONELLA SCAGLIONE

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distruzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
Gestione contabilità	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Gestione dati dei clienti e dei fornitori	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

NOMINE INCARICATI

L'azienda KH Automotive s.r.l. 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
- Anna Patrone

Data processor
- Anna Patrone

Sub data processor
- Gianni Cetani

Amministratore di sistema
- Anna Patrone

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

La KH Automotive s.r.l. non nomina un DPO in quanto non sussistono i requisiti di legge che prevedono l'obbligo di tale nomina; nello specifico, La KH Automotive s.r.l. non tratta dati sensibili (sanitari, biometrici e giudiziari) e non effettua trattamenti ne in modo sistematico ne in larga scala. Inoltre, La KH Automotive s.r.l. non è un ente pubblico o in partecipazione pubblica.

SISTEMI DI ELABORAZIONE

L'azienda KH Automotive s.r.l. 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.

PC Dell Optiplex 3050

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Patrone Anna
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: gennaio 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

PC Dell Optiplex 3080

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Cetani Gianni
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: settembre 2020

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

PC Dell Optiplex 3070

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Lafiosca Sandro
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: gennaio 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

PC Asus PRO

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Patrone Nicola Maria
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: dicembre 2016

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

PC Dell Vostro 3670

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Reception
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: settembre 2020

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

PC Dell Vostro 3470

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Uffici amministrativi
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: gennaio 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

Server HP Proliant G6

TIPOLOGIA: Server
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: CED
AMBIENTE: Windows Server 2008
DATA ACQUISTO: gennaio 2014

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

Server IBM AS400

TIPOLOGIA: Server
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: CED
AMBIENTE: AS400 v. 7.xx
DATA ACQUISTO: gennaio 2014

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

iphone 10X

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Patrone Anna
AMBIENTE: IOS
DATA ACQUISTO: giugno 2020

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

iphone 10X

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Cetani Gianni
AMBIENTE: IOS
DATA ACQUISTO: dicembre 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

iphone 12

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Lafiosca Sandro
AMBIENTE: IOS
DATA ACQUISTO: dicembre 2020

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

iphone 12

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Patrone Nicola Maria
AMBIENTE: IOS
DATA ACQUISTO: dicembre 2020

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

iphone 13

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Mongiello Michele
AMBIENTE: IOS
DATA ACQUISTO: ottobre 2021

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

iphone 10X

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Giordano Mario
AMBIENTE: IOS
DATA ACQUISTO: dicembre 2018

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:

Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

iphone 13

TIPOLOGIA: Smartphone
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Patrone Paolo
AMBIENTE: IOS
DATA ACQUISTO: ottobre 2021

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Aggiungere:
Aggiornamento interno dei software
Gruppi di continuità
Manutenzione programmata apparecchiature

PC Dell Optiplex 7060

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Mongiello Michele
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: gennaio 2021

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

PC Dell Optiplex 3070

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Patrone Paolo
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: dicembre 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

PC Dell Vostro

TIPOLOGIA: Client
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: Stanza di Giordano Mario
AMBIENTE: Windows 10 Professional
DATA ACQUISTO: gennaio 2019

VALUTAZIONE DEL SISTEMA DI ELABORAZIONE:
Obiettivo compliance raggiunto!

Datacenter Dell

TIPOLOGIA: Server
UBICAZIONE: SEDE: Trattamenti di superfice per il settore Automotive, UFFICIO: CED
AMBIENTE: AS400 v. 7.xx
DATA ACQUISTO: gennaio 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 KH Automotive s.r.l. 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.

Gestione dati dei clienti e dei fornitori - Dati commerciali dei clienti e dei fornitori

- **Queste le categorie interessati:**
  Clienti, Consulenti e liberi professionisti, anche in forma associata, Fornitori

- **Queste le categorie destinatari:**
  Società e imprese, Clienti

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

- **Le finalità del trattamento:**
  L'azienda KH Automotive s.r.l., tramite il trattamento "Gestione dati dei clienti e dei fornitori", tratta i sopraindicati dati.

  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 risultino nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultino eccedenti al trattamento dichiarato.

- **Il trattamento segue i seguenti criteri di liceità:**
  Adempimento obblighi contrattuali, L'interessato ha espresso il consenso al trattamento.
  Per le seguenti motivazioni:
  Adampimento obblighi contrattuali e consenso espresso da parte dell'interessato del trattamento.

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "Gestione dati dei clienti e dei fornitori" non vengono trattati dati riguardanti i minori

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "Gestione dati dei clienti e dei fornitori" non vengono trattati dati sanitari, biometrici e giudiziari

- **Durata del trattamento:**
  Il trattamento "Gestione dati dei clienti e dei fornitori" ha una durata indefinibile:
  L'azienda KH Automotive s.r.l. mantiene il trattamento "Gestione dati dei clienti e dei fornitori" fino a data indefinita in quanto continuerà a tenerlo in vita per alimentare i fatturati, offrendo ai propri clienti tutte le nuove offerte su richiesta.
  L'azienda si impegna, comunque, a cancellare i dati necessari per il presente trattamento una volta venute meno le condizioni sopra descritte.

- **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

Gestione contabilità - Gestione contabilità

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

- **Queste le categorie destinatari:**
  Consulenti e liberi professionisti in forma singola o associata, Banche e istituti di credito, Enti previdenziali ed assistenziali, Altre amministrazioni pubbliche, Clienti

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

- **Le finalità del trattamento:**
  L'azienda KH Automotive s.r.l., tramite il trattamento "Gestione contabilità", tratta i dati dei dipendenti per fini amministrativi e fiscali con lo scopo di archiviare i cedolini paghe e ROL e le fatturazioni ciclo attivo e passivo.

  Il Data Processor e il Data Controller vigilano per garantire che i suddetti dati siano 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 risultino nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultino eccedenti al trattamento dichiarato.

- **Articolo 8 (dati riguardanti i minori):**
  Nel trattamento "Gestione contabilità" vengono trattati dati riguardanti i minori:
  L'azienda KH Automotive s.r.l., trattando dati di minori tramite il trattamento "Gestione contabilità", in osservanza dell'articolo 8 del GDPR si impegna a chiedere il consenso a chi ne esercita la responsabilità genitoriale garantendo l'immediatezza nel comunicare eventuali modifiche al trattamento.

- **Articolo 9 (dati sanitari, biometrici e giudiziari):**
  Nel trattamento "Gestione contabilità" vengono trattati dati sanitari, biometrici e giudiziari per le seguenti motivazioni:
  Il trattamento è necessario per assolvere gli obblighi di legge ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.
  Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità.
  L'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche.

- **Durata del trattamento:**
  Il trattamento "Gestione contabilità" ha una durata indefinibile:
  il Data controller e il Data processor vigileranno affinché si possa garantire agli interessati che, una volta

raggiunte le finalità del presente trattamento e decorsi i termini di legge, i suddetti 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 KH Automotive s.r.l. 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 "Gestione contabilità"

Server di dominio - (sistema di backup: Xopero Backup & Restore)

Dati anagrafici (Altre categorie particolari di dati personali) - Dati personali (Dati personali)

Trattamento "Gestione dati dei clienti e dei fornitori"

Gestionale Aziendale Youcubes_1 - (sistema di backup: Xopero Backup & Restore)

Dati commerciali (Altre categorie particolari di dati personali) - Dati contabili (Altre categorie particolari di dati personali) - Dati fiscali (Altre categorie particolari di dati personali)

Gestionale Aziendale Youcubes_2 - (sistema di backup: Xopero Backup & Restore)

Dati commerciali (Altre categorie particolari di dati personali) - Dati contabili (Altre categorie particolari di dati personali) - Dati fiscali (Altre categorie particolari di dati personali)

Gestionale Aziendale Youcubes_3 - (sistema di backup: Xopero Backup & Restore)

Dati commerciali (Altre categorie particolari di dati personali) - Dati contabili (Altre categorie particolari di dati personali) - Dati fiscali (Altre categorie particolari di dati personali)

PRIVACY IMPACT ASSESSMENT

L'azienda KH Automotive s.r.l. espone qui di seguito le valutazioni di impatto sulla privacy dei trattamenti sopra elencati.

PRIVACY IMPACT ASSESSMENT TRATTAMENTO **Gestione dati dei clienti e dei fornitori**

L'azienda KH Automotive s.r.l. con sede in Zona Industriale Tito Scalo, 85050 - Potenza (PZ), nell'ottica di assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

KH Automotive s.r.l. effettua il seguente trattamento: **Gestione dati dei clienti e dei fornitori** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L'azienda KH Automotive s.r.l., tramite il trattamento "Gestione dati dei clienti e dei fornitori", tratta i sopraindicati dati.

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 risultino nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultino eccedenti al trattamento dichiarato.

Adampimento obblighi contrattuali e consenso espresso da parte dell'interessato del trattamento.

Dopo attenta valutazione di comune accordo con il Data Controller Anna Patrone e il Data Processor Anna Patrone; KH Automotive s.r.l. 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 **Gestionale Aziendale Youcubes_1, Gestionale Aziendale Youcubes_2, Gestionale Aziendale Youcubes_3,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

KH Automotive s.r.l., 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
Registrazione accessi
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
Antivirus centralizzato con MDM - Mobile Device Management
Antivirus centralizzato con DLP - Data Loss Prevention
Penne USB con fingerprint
Gruppi di continuità
Antivirus centralizzato
Manutenzione spot apparecchiature

Tali mitigazioni danno al trattamento **Gestione dati dei clienti e dei fornitori** 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.

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 Anna Patrone e il Data Processor Anna Patrone 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

Potenza, li 07/03/2022

Il Data Controller Anna Patrone .....

Il Data Processor Anna Patrone .....

PRIVACY IMPACT ASSESSMENT TRATTAMENTO **Gestione contabilità**

L'azienda KH Automotive s.r.l. con sede in Zona Industriale Tito Scalo, 85050 - Potenza (PZ), nell'ottica di assolvimento dell'obbligo del Privacy Impact Assessment ovvero dell'articolo 35 della GDPR dichiara quanto segue:

KH Automotive s.r.l. effettua il seguente trattamento: **Gestione contabilità** meglio descritto nel registro dei trattamenti

Lo scopo è quello di:
L'azienda KH Automotive s.r.l., tramite il trattamento "Gestione contabilità", tratta i dati dei dipendenti per fini amministrativi e fiscali con lo scopo di archiviare i cedolini paghe e ROL e le fatturazioni ciclo attivo e passivo.

Il Data Processor e il Data Controller vigilano per garantire che i suddetti dati siano 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 risultino nel frattempo diversi dagli originali, a tenerli sempre aggiornati e a cancellare tutti quei dati che risultino eccedenti al trattamento dichiarato.

Dopo attenta valutazione di comune accordo con il Data Controller Anna Patrone e il Data Processor Anna Patrone; KH Automotive s.r.l. 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 **Server di dominio,** cancellando tutti i dati che non sono strettamente necessari al trattamento dichiarato.

KH Automotive s.r.l., 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
Registrazione accessi
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
Antivirus centralizzato con MDM - Mobile Device Management
Antivirus centralizzato con DLP - Data Loss Prevention
Penne USB con fingerprint
Gruppi di continuità
Antivirus centralizzato
Manutenzione spot apparecchiature

Tali mitigazioni danno al trattamento **Gestione contabilità** una compliance alla sicurezza del **80%**

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.

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 Anna Patrone e il Data Processor Anna Patrone 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

Potenza, li 07/03/2022

Il Data Controller Anna Patrone .....

Il Data Processor Anna Patrone .....