G.D.P.R.

GENERAL DATA PROTECTION REGULATION

Adeguamento nuovo regolamento Europeo sulla privacy

RELAZIONE DOCUMENTALE

VERIFICATA E PRODOTTA IL 27/12/2019

AGGIORNATA IL 03/01/2022

RAGIONE SOCIALE

ALES MARKET RESEARCH S.R.L.

SEDE LEGALE

VIA PRINCIPE AMEDEO 152 70122 BARI

P.IVA

05429820722

INDICE

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 (**TOMMASO PRONUNZIO**) e il DATA PROCESSOR (**LUIGI PAOLO CIMBASSO**). 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. **Ales Market Research** implementa le procedure atta a censire, valutare, monitorare lo stato di rischio e implementando 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

Luigi Paolo Cimbasso

Data Controller

Tommaso Pronunzio

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 **LUIGI PAOLO CIMBASSO** e il Data Controller **TOMMASO PRONUNZIO** deve 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. 22 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 Ales Market Research 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 sulle postazioni CLIENT e sui server WINDOWS

- antivirus commerciale MalwareBytes Pro, sottoscrizione annuale, costantemente aggiornato
- antivirus Windows Defender, costantemente aggiornato

Antivirus installati sui NAS

- Antivirus Essential, gratuito, costantemente aggiornato

Firewall Installati

- firewall software integrato al sistema operativo
- firewall hardware perimetrale

Crittografia in Essere

- nessuna crittografia

Dispositivi USB aziendali

- chiavette e hard disk usb privi di crittografia

Sistemi di backup BACKUP dei dati aziendali

- Frequenza backup: Oraria
- Tipo backup: sistema di backup on site e offsite, con versioning

BACKUP SU HARD DISK ESTERNO VIA USB (per BARE METAL RESTORE)

- Frequenza backup: Giornaliera
- Dispositivi interessati: Mail Server, Domain Controller

Protezione generica

Per quanto riguarda la parte delle risorse umane, ALES MARKET RESEARCH 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

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 ALES MARKET RESEARCH S.R.L. dichiara di aver predisposto la seguente protezione ambientale per il cartaceo:

- armadi con chiave
- armadi blindati
- armadi senza chiave
- scaffalature a vista
- sistema di allarme

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 ALES MARKET RESEARCH S.R.L. dichiara di aver predisposto per tutte le apparecchiature informatiche (stampanti escluse) la seguente policy:

- gruppi di continuità
- manutenzione programmata apparecchiature

SEDI E UFFICI

Ales Market Research 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.

Ales Market Research S.r.l.

SEDE CENTRALE Via Valtellina, 20 - 20159 Milano

SEDE LEGALE Via Principe Amedeo, Bari

DATA PROCESSOR ESTERNI

Nella suddetta sezione vengono nominati tutti i data processor esterni ad Ales Market Research 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 privacy

Dati di contatto del Responsabile della Protezione dei Dati Personali (DPO):

- Nome: Luigi Paolo Cimbasso
- Indirizzo: Via G. Bernini, 8 - 70010 Casamassima (BA)
- P.IVA / Codice Fiscale: 08022190725 / CMBLPL77L20A662V
- Telefono: +39 366 3688625
- Domicilio digitale (PEC): luigipaolo.cimbasso@postecert.it

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.

Ales Market Research S.r.l. 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 MARIA ALESSANDRA MASTROLONARDO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distribuzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA CONTABILITA'	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler ALESSANDRA COLLINI

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distribuzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA CONTABILITA'	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Data handler TOMMASO PRONUNZIO

Permessi relativi ai trattamenti aziendali elettronici/cartacei:

Trattamento	Raccolta	Inserimento	Registrazione	Modifica	Cancellazione	Distribuzione	Lettura	Consultazione	Creazione	Stampa	Comunicazione
AREA CONTABILITA'	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
AREA RETRIBUZIONI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

NOMINE INCARICATI

Ales Market Research per essere totalmente compliance alle direttive del nuovo regolamento europeo della privacy ha deciso di fare le seguenti nomine delle figure aziendali previste dalla normativa:

Data controller

TOMMASO PRONUNZIO

Data processor

LUIGI PAOLO CIMBASSO

Amministratore di sistema

LUIGI PAOLO CIMBASSO

D.P.O.

LUIGI PAOLO CIMBASSO

REGISTRO DEI TRATTAMENTI

L'Art. 30 del Regolamento europeo in materia di protezione dei dati personali nello specifico il par. 4 dell'art. 30, per il quale "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 Ales Market Research 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.

AREA CONTABILITA' - GESTIONE ANAGRAFICA FORNITORI E DIPENDENTI

Queste le categorie interessate:

Personale dipendente,Fornitori

Queste le categorie destinatari:

Consulenti e liberi professionisti in forma singola o associata,Istituti, scuole e università,Enti previdenziali ed assistenziali,Fornitori

I dati sono trattati in queste modalità:

Elettronica e cartacea

Le finalità del trattamento:

Ales Market Research, tramite il trattamento "AREA CONTABILITA", tratta i sopraindicati dati per: LA GESTIONE DEGLI INCASSI E DEL CICLO PASSIVO DAGLI ORDINI AL PAGAMENTO DELLE FATTURE E PAGAMENTO COMPENSI AD ESPERTI ESTERNI, PERSONALE INTERNO E VERSAMENTO RITENUTE FISCALI E PREVIDENZIALI AGLI ENTI PREPOSTI.

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.

Il trattamento segue i seguenti criteri di liceità:

Adempimento obblighi contrattuali, Obblighi di legge cui è soggetto il titolare, L'interessato ha espresso il consenso al trattamento.

Articolo 8 (dati riguardanti i minori):

Nel trattamento "AREA CONTABILITA" non vengono trattati dei minori

Articolo 9 (dati sanitari, biometrici e giudiziari):

Nel trattamento "AREA CONTABILITA" non vengono trattati dati sanitari, biometrici e giudiziari

Durata del trattamento:

Il trattamento "AREA CONTABILITA" ha durata indefinita: Ales Market Research dichiara il trattamento "AREA CONTABILITA" 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 archiviati.

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

AREA PERSONALE/ RETRIBUZIONI - GESTIONE DATI ANAGRAFICI E FASCICOLO PERSONALE DEI DIPENDENTI

Queste le categorie interessate:

Personale dipendente

Queste le categorie destinatari:

Dipendenti, Enti previdenziali ed assistenziali

I dati sono trattati in queste modalità:

Elettronica e cartacea

Le finalità del trattamento: Ales Market Research S.r.l., tramite il trattamento "AREA PERSONALE", tratta i sopraindicati dati per: LA GESTIONE DEGLI ATTI AMMINISTRATIVI DEL PERSONALE DIPENDENTE RIFERITI ALLA CARRIERA, ASSENZE, FORMAZIONE, VERSAMENTO RITENUTE PREVIDENZIALI E FISCALI AGLI ENTI INTERESSATI, DICHIARAZIONI CONTRIBUTIVE E FISCALI CORRELATE

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.

Il trattamento segue i seguenti criteri di liceità:

Adempimento obblighi contrattuali, Obblighi di legge cui è soggetto il titolare, L'interessato ha espresso il consenso al trattamento.

Articolo 8 (dati riguardanti i minori):

Nel trattamento "AREA PERSONALE/RETRIBUZIONI" non vengono trattati dei minori

Articolo 9 (dati sanitari, biometrici e giudiziari):

Nel trattamento "AREA PERSONALE/ RETRIBUZIONI" vengono trattati dati sanitari, biometrici e giudiziari per le seguenti motivazioni:

Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Durata del trattamento:

Il trattamento "AREA PERSONALE/RETRIBUZIONI" ha durata indefinita:

Ales Market Research dichiara il trattamento "AREA PERSONALE" 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 archiviati.

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