GENERAL DATA PRIVACY POLICY

(25/05/2018)

Consorzio MEBIC
Sede legale- Via Val Cannuta, 247 – Roma tel. 06.52252132
mebic@sanraffaele.it – mebic@legalmail.it

SOMMARIO

INTRODUZIONE

Scopo

Lo scopo del presente documento è quello di indicare la politica adottata dal Consorzio MEBIC (in seguito "Società") per regolare le modalità di trattamento dei dati personali.

Applicabilità

Il presente documento si applica alla Società ed è rivolta a tutti i dipendenti di tale Società e collaboratori esterni, intesi come Fornitori di servizi, Terze Parti, Outsourcers, Liberi Professionisti, che, a diverso titolo e per diversi scopi, collaborano con la Società, effettuando attività di trattamento di dati personali.

RIFERIMENTI

Riferimenti

[Rif. 1]

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[Rif. 2]

Provv. Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronicirelativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008) e successive modifiche ed integrazioni

ACRONIMI e DEFINIZIONI	DESCRIZIONE
IT	Information Technology, le tecnologie dell'informazione
Hardening	Procedure di securizzazione di un sistema, mirate al restringimento dei soli servizi necessari e alla modifica delle impostazioni di "default"
OS	Operating System (Sistema operativo)
DB	Data Base (Banca dati)
Pseudonimizzazione	Procedura volta al mascheramento di dati personali, in modo che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile
Data breach	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
DPIA	Data Protection Impact Assessment (Valutazione d'impatto sulla protezione dei dati). È una procedura di analisi che mira a valutare la necessità, la proporzionalità ed i rischi di un trattamento, allo scopo di approntare misure idonee ad affrontarli

PRINCIPI GENERALI

Nell'ambito della gestione dei processi di protezione dei dati e delle informazioni trattate, la Società garantisce il rispetto dei seguenti principi generali:

- **Privacy by design**: devono essere messe in atto, al momento di determinare i mezzi del trattamento ed all'atto del trattamento stesso, misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento [Rif.1] e tutelare i diritti degli interessati.
- **Privacy by default:** devono essere messe in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tali misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
- **Need to Know**: assegnazione dell'utenza di accesso ad un sistema/servizio informatico esclusivamente agli utenti che necessitano dell'accesso a tale sistema/servizio per lo svolgimento delle proprie attività lavorative.
- **Least Privilege**: assegnazione a ciascun utente di un set di privilegi minimo necessario per l'espletamento delle proprie attività lavorative.
- **Segregation of Duty**: scomposizione delle responsabilità, dei compiti e dei privilegi tra più utenti al fine di garantire che un dato processo non sia controllato interamente da un singolo soggetto e in modo da ridurre i rischi connessi ad abusi ed errori.
- **Defense in depth**: il principio stabilisce che devono essere previsti dei controlli di sicurezza in ognuno degli strati dell'architettura (i.e. network, application, OS e DB); lo sviluppo di controlli di sicurezza in tutti gli strati dell'architettura fa in modo che la compromissione della sicurezza in un singolo strato non sia sufficiente a compromettere l'intera architettura
- **Riservatezza**: solo gli utenti autorizzati possono decifrare l'informazione e nessun soggetto terzo può accedere al contenuto informativo, anche se in possesso dell'informazione cifrata.
- **Integrità**: il contenuto informativo non può essere alterato ed è possibile verificare l'integrità delle informazioni al fine di stabilire l'occorrenza di una qualunque alterazione.
- **Disponibilità**: il contenuto informativo deve essere sempre disponibile e fruibile quando viene richiesto.

RUOLI E RESPONSABILITA'

Al fine di gestire correttamente i processi di protezione dei dati e delle informazioni trattate è stato individuato e nominato il personale chiave per il trattamento di dati personali. In particolare, il Regolamento di cui al [Rif.1] individua specifici ruoli e responsabilità, di cui si riportano di seguito i principali:

- **Titolare del trattamento -** ha il compito di:
  - determinare le finalità e i mezzi del trattamento di dati personali;
  - mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento di cui al [Rif.1];
  - riesaminare e aggiornare, qualora necessario, le misure tecniche e organizzative adottate;
  - porre in essere le misure tecniche e organizzative per garantire la protezione dei dati fin dalla progettazione e per impostazione predefinita;
  - istruire il Responsabile del trattamento o chiunque agisca sotto la propria autorità e abbia accesso a dati personali.

- **Responsabile del trattamento -** ha il compito di:
  - trattare dati personali per conto del Titolare del trattamento;
  - nominare formalmente le persone autorizzate al trattamento dei dati personali (c.d. incaricati) garantendo che si impegnino alla riservatezza;
  - supportare il Titolare del trattamento per l'adozione delle più ampie misure di sicurezza a protezione dei dati personali trattati;
  - supportare il Titolare del trattamento per la gestione di scenari di Data Breach;
  - cooperare e/o fornire supporto, ove richiesto dal Titolare del trattamento, nell'esecuzione delle attività di analisi dei rischi privacy "DPIA" per uno specifico trattamento;
  - comunicare al Titolare qualunque circostanza possa sollevare incertezze in merito al mantenimento dei requisiti di Legge.

- **Incaricato al trattamento -** ha il compito di:
  - effettuare operazioni di trattamento adottando le disposizioni ed istruzioni impartite dal Titolare o dal Responsabile del trattamento;
  - supportare il Titolare o il Responsabile del trattamento per il mantenimento dei più alti livelli di conformità a normative vigenti:
    - comunicando eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
    - segnalando ogni situazione sospetta di anomalia, di potenziale illecito o di evidente violazione di dati personali;
  - prestare la più ampia e completa collaborazione al Titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

- **Responsabile della protezione dei dati -** ha il compito di:
  - informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento in merito agli obblighi derivanti dal Regolamento di cui al [Rif. 1];
  - sorvegliare l'osservanza del Regolamento di cui al [Rif. 1];
  - cooperare e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento (i.e. Garante per la protezione dei dati personali).

POLICY GENERALE DI GESTIONE DEI DATI

I principi generali che devono essere recepiti, adottati e rispettati per la protezione dei dati e delle informazioni trattate, in conformità con il Regolamento di cui al [Rif. 1] sono:

- **Gestione organizzativa della sicurezza delle informazioni:**
  - garantire che, all'interno dell'organizzazione, siano identificate le figure chiave per la gestione e governo dei processi di Sicurezza delle informazioni. Per ciascuna figura devono essere assegnate specifiche responsabilità. Devono altresì essere disegnati ed adottati processi organizzativi a garanzia della corretta applicazione della presente Policy.

- **Gestione dei rischi di sicurezza delle informazioni**:
  - garantire che sia definito e documentato un processo che consenta l'adozione di criteri e metodologie per l'analisi, la determinazione e la valutazione dei Rischi sulla sicurezza delle informazioni e sul loro trattamento. Particolare attenzione e cura dovrà essere posta nell'esecuzione di attività di "DPIA" per la valutazione del livello di rischiosità di un trattamento di dati personali e l'individuazione delle più opportune misure di sicurezza a protezione dei dati.

- **Classificazione e protezione dei dati**:
  - garantire che sia definito e documentato un processo di classificazione e protezione dei dati, che definisca le responsabilità e le modalità di trattamento delle informazioni aziendali archiviate, elaborate o condivise all'interno e all'esterno dell'organizzazione, al fine di garantirne una protezione adeguata durante tutto il loro ciclo di vita;
  - assicurare che le misure di sicurezza da adottare per la protezione delle informazioni siano valutate in funzione dei seguenti criteri minimi di:
    - appetibilità, da valutare in funzione della tipologia del dato;
    - potenziale impatto in caso di perdita, distruzione, alterazione o diffusione del dato, da valutare in funzione della criticità del dato stesso.

- **Gestione accessi logici ai sistemi ed alle applicazioni:**
  - garantire che sia definito e documentato un processo di gestione degli accessi logici alle risorse informatiche aziendali, in grado di restringere gli accessi a tali risorse al solo personale autorizzato;
  - garantire che i privilegi di accesso ai sistemi ed alle applicazioni consentano di rispettare i principi di *Need to Know*, *Least Privilege*, *Privacy by default* e *Segregation of Duties*. Particolare attenzione e cura dovrà essere posta nell'affidamento dei privilegi di accesso "amministrativi", per consentire al personale preposto di gestire e governare i sistemi aziendali, secondo i regolamenti interni aziendali ed in conformità con il provvedimento di cui al [Rif. 2]. Le utenze di accesso devono essere di tipologia "nominale" e solo per

specifiche necessità sarà consentito l'uso di utenze di tipologia "non nominale" o "di servizio": in questi casi verrà assegnato ad ogni utenza uno specifico responsabile che risponderà circa l'utilizzo delle stesse;

- effettuare e documentare periodiche attività di revisione delle utenze presenti sui sistemi e sulle applicazioni, volte alla bonifica delle utenze attive ma inutilizzate, inattive o non conformi ai processi di gestione adottati dalla Società.

- **Gestione della sicurezza fisica ed ambientale:**
  - definire perimetri di sicurezza per proteggere le aree che contengono le informazioni critiche;
  - definire opportune misure tecniche ed organizzative di sicurezza fisica ed ambientale atte alla protezione dei locali aziendali e dei dati ivi contenuti da minacce naturali, malfunzionamenti di sistemi ed impianti nonché abusi. Particolare attenzione e cura dovrà essere posta nella valutazione delle misure di sicurezza da implementare per la protezione dei locali tecnici e dei data center contenenti impianti di elaborazione;
  - definire opportune misure tecniche ed organizzative per garantire che l'accesso ai locali aziendali, siano essi uffici, depositi, data center, sale tecniche o qualunque altra tipologia di locale, sia limitato al solo personale interno autorizzato. L'accesso del personale esterno, come fornitori, terze parti, outsourcers e visitatori esterni, può avvenire in ragione di uno specifico contratto con la società esterna o il professionista. Le visite del personale esterno devono essere tracciate e monitorate ed il fornitore deve essere identificato con idonei supporti che devono essere esposti e ben visibili.

- **Gestione degli incidenti ed eventi critici:**
  - mettere in atto misure tecniche ed organizzative volte ad assicurare che i guasti, le anomalie e gli incidenti di sicurezza delle informazioni siano correttamente riconosciuti e gestiti;
  - Adottare efficaci sistemi e processi di prevenzione, comunicazione e risposta, al fine di consentire all'organizzazione di adempiere ad eventuali obblighi normativi (i.e. notifica al Garante di Data Breach, per gli incidenti relativi a dati personali) e allo scopo di minimizzare eventuali impatti sul business.

- **Gestione della continuità operativa aziendale:**
  - condurre con cadenza almeno annuale attività di analisi della continuità del business aziendale, finalizzate alla comprensione degli scenari di minaccia verso la continuità operativa aziendale, valutazione delle priorità del business aziendale ed implementazione di opportune misure a garanzia della continuità operativa;
  - mettere in atto misure tecniche ed organizzative in funzione dei requisiti raccolti in fase di analisi della continuità del business e finalizzate ad assicurare la continuità del business aziendale anche al verificarsi di scenari di guasti,

malfunzionamenti, eventi disastrosi o crisi. Particolare attenzione e cura dovrà essere posta nella valutazione delle misure di sicurezza da implementare per garantire la continuità dei sistemi informatici di elaborazione.

- **Gestione della compliance**:
  - garantire che sia definito e documentato un processo di gestione della compliance volto al mantenimento dei livelli di sicurezza necessari per l'adeguamento ai Regolamenti di cui al [Rif. 1] e [Rif. 2] ed ulteriori normative applicabili, regolamenti aziendali interni, standard organizzativi applicabili e standard internazionali adottati;

  - effettuare periodicamente verifiche interne finalizzate al mantenimento della conformità con le normative applicabili, documentandone e condividendone l'esito con il personale apicale chiave per la gestione e governo dei processi di compliance,. Le eventuali non conformità rilevate saranno gestite con uno specifico piano di intervento che indicherà le tempistiche e le modalità di rimedio individuate.

- **Gestione della formazione**:
  - garantire che sia definito e documentato un processo di formazione aziendale strutturato rivolto a tutto il personale interno che, a diverso titolo e con diversi incarichi, effettua operazioni di trattamento di dati personali, volto alla sensibilizzazione, istruzione, formazione e addestramento sui regolamenti normativi applicabili e sulle politiche e procedure interne dell'organizzazione di sicurezza e protezione dei dati personali.

- **Gestione della crittografia:**
  - garantire che sia definito e documentato un processo di gestione delle soluzioni crittografiche per la gestione degli scenari nei quali le informazioni, per un requisito normativo, di business o per scelta aziendale, necessitano di essere crittografate;
  - garantire che le informazioni critiche, oggetto di specifici requisiti normativi (i.e. i dati personali, particolari e giudiziari) o connesse a proprietà intellettuali della Società, archiviate, trasmesse o pubblicate su canali di comunicazione insicura, come la rete internet, siano oggetto di cifratura. Particolare attenzione e cura dovrà essere posta per i processi di trasmissione di tali informazioni al di fuori della rete aziendale, attraverso lo strumento di produttività della posta elettronica, in particolare devono essere sempre adottati i seguenti accorgimenti:
    - il contenuto informativo critico della trasmissione deve essere criptato;
    - lo scambio della chiave di decifratura, qualora si utilizzino tecniche di cifratura simmetrica, deve avvenire attraverso un canale separato dal canale di trasmissione;

        - la trasmissione deve essere circoscritta ai soli destinatari titolati alla ricezione di tali informazioni;
    - redigere e divulgare opportune istruzioni sulle modalità di utilizzo degli strumenti crittografici aziendali, al fine di rendere edotto tutto il personale e minimizzare potenziali utilizzi impropri dei suddetti strumenti ed i connessi rischi di sicurezza.

- **Gestione delle terze parti**:
    - garantire che sia definito e documentato un processo di gestione delle terze parti atto alla definizione dei requisiti di sicurezza delle informazioni volti a mitigare i rischi associati all'accesso agli asset aziendali da parte dei fornitori, terze parti, outsourcers e visitatori esterni;
    - assicurare che i contratti con i fornitori contengano opportuni requisiti di sicurezza per i processi di elaborazione, archiviazione e trasmissione, volti alla tutela del patrimonio informativo della Società;
    - effettuare verifiche periodiche sulle forniture volte a monitorare la conformità dell'erogazione dei servizi concordati.

- **Gestione dello sviluppo ed acquisizione dei sistemi informativi**:
    - garantire che sia definito e documentato un processo di gestione dello sviluppo ed acquisizione dei sistemi informativi mirato a garantire che siano presenti ed implementati, sin dalla progettazione o acquisizione di un nuovo sistema informativo, specifici principi di sicurezza delle informazioni volti alla protezione dei dati, in accordo con il principio *Privacy by design*;
    - definire specifici processi per il controllo ed il tracciamento dei cambiamenti ai sistemi informativi, mirati a garantire che le modifiche siano correttamente testate in ambienti distinti dall'ambiente di operatività reale o "di produzione", approvate dal personale chiave responsabile della gestione dei sistemi informativi e documentate, prima della loro applicazione.

- **Gestione delle vulnerabilità**:
    - garantire che sia definito e documentato un processo di gestione delle vulnerabilità e del codice malevolo volto alla rilevazione, valutazione e gestione delle vulnerabilità di sicurezza e di eventuali malware che affliggono i sistemi e le applicazioni;
    - garantire che il processo di rilevazione delle vulnerabilità sia eseguito con cadenza almeno annuale, mediante l'esecuzione di specifiche attività meglio note come "*Vulnerability Assessment*"documentandone gli esiti. Tale processo dovrà essere in ogni caso attivato a fronte di eventuali cambiamenti dei sistemi informativi o delle applicazioni ed all'acquisizione o sviluppo di nuovi sistemi;
    - garantire che i sistemi e le applicazioni siano sempre aggiornati con i più recenti aggiornamenti di sicurezza rilasciati dai fornitori di servizi informatici (i.e. "Vendor") in modo da garantire i più elevati livelli di protezione contro le minacce informatiche.

- **Gestione delle risorse tecnologiche aziendali:**
  - garantire che sia definito e documentato un processo di gestione delle risorse tecnologiche aziendali, in grado di creare e mantenere costantemente un inventario di tali risorse, volto al mantenimento dei più elevati livelli di sicurezza fisica e logica a protezione di tali asset.

- **Gestione e monitoraggio della rete:**
  - mettere in atto misure tecniche ed organizzative volte ad assicurare un adeguato funzionamento dei sistemi e degli apparati di rete ed un continuo controllo su tutte le componenti dei sistemi;
  - garantire il monitoraggio dello stato della rete per garantire che, a fronte di eventuali malfunzionamenti dei sistemi che possono rallentare o bloccare l'operatività aziendale, sia attivato un intervento tempestivo.

- **Gestione della sicurezza della rete e delle infrastrutture**:
  - garantire che sia definito e documentato un processo di gestione disicurezza della rete e delle infrastrutture volto al mantenimento dei più elevati livelli di sicurezza e che garantisca i più elevati livelli di continuità operativa, in accordo con il principio *Defense in depth*;
  - garantire che i servizi infrastrutturali siano stati oggetto di attività di hardening, mirate al restringimento dei soli servizi necessari e alla modifica delle impostazioni di "default", sia a livello di settaggi di sicurezza che di utenze per l'accesso logico;

  - applicare le best practices di sicurezza per la segmentazione delle reti aziendali interne, in modo da realizzare "zone" di sicurezza con diversi livelli di protezione;
  - garantire che i servizi esposti su rete pubblica e sulle reti aziendali interne siano adeguatamente protetti da strumenti di rilevazione e protezione contro attacchi informatici.

Per il Consorzio MEBIC

Il Legale Rappresentante