Policy sulla sicurezza delle informazioni

Rev. 1.0

Sommario

1. Introduzione

1.1 Finalità

La presente policy regola gli accorgimenti di sicurezza adottati da Meccanio S.r.l. (d'ora in poi "Meccanio") per proteggere l'integrità, la riservatezza e la disponibilità dei dati personali, nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 (General Data Protection Regulation, d'ora in poi "GDPR") in particolare all'art. 32.

1.2 Ambito di applicazione e definizioni

La presente Procedura si applica ad ogni *Utente* e per ogni sede aziendale.
Per *Utente* si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.
Per *Azienda* si intende, invece, la società Meccanio S.r.l. e i suoi marchi, titolare dei beni e delle risorse informatiche ivi disciplinate, la quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

1.3 Responsabilità personale dell'utente

Ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Azienda, è tenuto al rispetto di questa policy ed è personalmente responsabile del suo mancato rispetto in caso di negligenza o dolo.

2. Organizzazione della Sicurezza delle Informazioni

La cultura della protezione dei dati personali è supportata dal management aziendale. Meccanio si assicura di diffondere tale cultura al suo personale.

Le misure adottate comprendono:

a) Identificazione e attivazione di una serie di misure di sicurezza per il trattamento dei dati personali
b) La definizione della presente politica per sicurezza delle informazioni, approvata dal Top Management e diffusa a tutto il personale.
c) La politica di sicurezza Meccanio è rivista almeno annualmente e aggiornata in caso di necessità.
d) Tutto il Personale Meccanio incaricato di trattare dati personali ha firmato accordi di riservatezza che si applicano durante e successivamente al rapporto di lavoro.

e) La superficialità o l'intenzionalità del personale nel seguire le politiche di sicurezza delle informazioni può essere trattata come una questione disciplinare e portare a sanzioni.
f) A tutto il Personale Meccanio è stata data formazione dei fondamentali di sicurezza delle informazioni e della privacy.
g) Meccanio si impegna per il miglioramento continuo della propria sicurezza.
h) Tutti i soggetti che conferiscono a Meccanio i propri dati personali ricevono un'informativa secondo le prescrizioni del GDPR
i) Tutti i fornitori che dovessero trattare i dati personali di cui Meccanio è titolare ricevono un incarico come Responsabile del trattamento con delle specifiche prescrizioni in materia di privacy e sicurezza delle informazioni

3. Sistema di Gestione della Sicurezza delle Informazioni

Il Sistema di Gestione per la Sicurezza per le Informazioni di Meccanio definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei seguenti requisiti di sicurezza di base:

- Riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- Integrità: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- Disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
- Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
- Autenticità: garantire una provenienza affidabile dell'informazione.
- Privacy: garantire la protezione ed il controllo dei dati personali.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, tramite l'adozione di regole, procedure e tecnologie, la conservazione dei documenti, informatici o cartacei, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

4. Accesso fisico

L'accesso fisico ai dati personali è protetto. L'accesso ai locali è sempre presidiato da personale Meccanio, inoltre i dati personali sono custoditi sotto chiave e/o in ambienti riservati e non accessibili al pubblico.

Misure adottate:

a) Meccanio gestisce in autonomia il sito WEB www.meccanio.it e quelli dei suoi marchi www.generazionesolare.it e www.crunchy.it, così come tutto il parco applicativo. Solo personale autorizzato ha accesso ai locali dove sono i computer. Eventuali visitatori sono sempre accompagnati.
b) I personal computer sono protetti da interruzioni di e sono mantenuti da personale di possesso di adeguate competenze tecniche.
c) Apparecchiature o supporti di memoria contenenti dati personali (compresi i casi di difettosità o di dismissione) vengono cancellati in modo sicuro prima della rimozione e l'affidamento allo smaltimento rifiuti.
d) Quando i dati personali vengono copiati elettronicamente su sopporti di memoria portatili, viene mantenuto un adeguato livello di sicurezza fisica e, in ogni caso, i dati vengono cifrati.

5. Sistema di accesso

I sistemi di elaborazione dati Meccanio vengono utilizzati solo da utenti autorizzati e autenticati sulla rete aziendale.

Misure adottate:

a) L'accesso ai sistemi interni Meccanio è concesso solo dal personale Meccanio e/o ai dipendenti autorizzati dei subappaltatori con modalità di accesso strettamente limitato alla funzione assegnata.
b) Tutti gli utenti accedono ai sistemi Meccanio con un identificatore univoco (ID utente) e una password.
c) Meccanio ha stabilito una politica delle password che ne vieta la condivisione e che richiede la modifica ad intervalli periodici nonché impedisce la permanenza di password di default.
d) Tutte le password devono soddisfare i requisiti minimi definiti e sono memorizzati in forma criptata. Ogni computer ha uno screensaver protetto da password.
e) Meccanio ha una procedura per disattivare gli utenti e il loro accesso quando un dipendente lascia l'azienda.
f) Opportuni software di sicurezza attiva prevengono potenziali accessi non autorizzati.

6. Accesso ai dati

Le persone incaricate di effettuare trattamento di dati personali hanno accesso solo ai dati per i quali sono autorizzati.

Misure adottate:

a) Limitazione dell'accesso del personale ai dati a ai sistemi informativi in base alla stretta necessità in virtù delle proprie funzioni operative.
b) La formazione del personale comprende i diritti di accesso e gli orientamenti generali sulla definizione e l'uso dei dati personali.
c) Se del caso, Meccanio impiega tecniche di minimizzazione e di pseudonimizzazione dei dati personali per ridurre la probabilità di accessi non autorizzati.
d) Meccanio utilizza software anti-virus e anti-malware aggiornati su tutti i computer e i server identificati come appropriati.
e) Meccanio utilizza firewall adeguatamente configurati per i servizi del sito WEB.
f) Meccanio si assicura di essere in condizione di ricevere avvisi e notifiche dai fornitori di software di sistema e altre fonti di avvisi di sicurezza e di installare regolarmente e in modo efficiente le patch software di sistema.

7. La trasmissione dei dati

Meccanio impedisce che i dati personali possano essere letti, copiati, modificati o cancellati da persone non autorizzate durante le trasmissioni.

Misure adottate:

a) L'accesso degli utenti ai servizi WEB Meccanio è protetto da SSL.
b) Impiego di crittografia forte per tutte le altre trasmissioni di dati personali al di fuori della rete dati Meccanio (VPN).
c) Tutti i dati personali memorizzati al di fuori della rete dati Meccanio sono protetti da crittografia forte.

Il Cliente è responsabile per la sicurezza dei dati personali una volta che questi gli siano stati trasmessi da Meccanio al Cliente, compresa la circostanza in cui i suddetti dati siano scaricati dagli utenti dei Clienti.

8. Riservatezza e integrità dei dati personali

I Dati Personali rimangono confidenziali, intatti, completi e aggiornati durante il trattamento.

Misure adottate:

a) Meccanio impiega personale adeguatamente formato in tema di sicurezza delle informazioni.
b) Tutte le modifiche al software, laddove sviluppato ad hoc, vengono effettuate attraverso un meccanismo di approvazione formale che tenga traccia delle richieste di modifica e delle relative approvazioni prima della realizzazione.

c) Tutti le funzioni di crittografia utilizzate all'interno delle applicazioni Meccanio utilizzando gli standard del settore.

9. Disponibilità

I dati personali sono protetti dalla distruzione o perdita accidentale e vi è la possibilità del ripristino tempestivo della loro disponibilità in caso di incidente.

Misure adottate:

a) Meccanio utilizza un elevato livello di ridondanza sui dati di produzione in modo che il guasto o la mancanza di disponibilità di un unico sistema o componente non influisca sulla disponibilità generale delle informazioni.
b) Il server principale dispone di più fonti di alimentazione, generatori on-site con batterie di back-up per salvaguardare la disponibilità di alimentazione elettrica.
c) Meccanio utilizza sforzi ragionevoli per creare copie di back-up dei dati personali criptate e conservarli in una posizione geograficamente separata.
d) Meccanio esegue test di ripristino da tali backup con periodicità almeno trimestrale.

10. Controllo dei trattamenti

I dati personali trattati per conto di un utente vengo elaborati esclusivamente in conformità con le finalità dichiarate e nel rispetto della vigente normativa.

Misure adottate laddove Meccanio agisca come responsabile del trattamento dei dati personali:

a) Meccanio memorizza ed elabora i dati personali, al fine di effettuare i trattamenti sotto le istruzioni dell'utente e per le finalità da lui stabilite.
b) Meccanio non accede ai Dati Personali degli utenti, eccezion fatta per le finalità necessarie per lo svolgimento del suo servizio, su richiesta del Titolare o dell'interessato, per ragioni di sicurezza o per ogni altro adempimento di legge.
c) Meccanio impiega un numero limitato di fornitori, che incarica come responsabili del trattamento. Essi sono vincolati al rispetto della riservatezza dei Dati Personali e a seguire le sue procedure e policy di sicurezza delle informazioni. Un elenco è disponibile su richiesta.
d) Meccanio ha adottato procedure e policy che la rendono compliant con il Regolamento Europeo 2016/679 (General Data Protection Regulation - GDPR)

11. Separazione dei dati

Dati personali raccolti per scopi diversi vengono trattati separatamente.

Misure adottate:

a) Meccanio realizza la separazione logica dei dati personali provenienti da più utenti.
b) I quadri e le aziende iscritte hanno accesso solo ai dati personali di propria competenza.

12. Gestione degli incidenti di privacy

In caso di violazione della sicurezza dei dati personali, l'effetto della violazione è ridotto al minimo. Le Autorità e/o gli interessati vengono informati secondo le prescrizioni del regolamento.

Esiste un'apposita procedura di Data Breach alla quale si rimanda per la descrizione delle azioni adottate.

Viene tenuto un apposito registro dei Data Breach, sul quale vengono annotati gli incidenti di privacy, anche quelli il cui esito non comporta, a norma di legge, la notifica al Garante e/o agli interessati.

13. Compliance

Meccanio verifica continuamente l'efficacia di queste misure tecniche e organizzative.

Misure adottate:

a) Meccanio conduce regolarmente verifiche interne attraverso la periodica valutazione d'impatto sulla protezione dei dati.
b) Meccanio prende misure ragionevoli per assicurare che il personale sia a conoscenza e rispetti le misure tecniche e organizzative di cui al presente documento. In particolare l'azienda fornisce la formazione necessaria e continui aggiornamenti in merito alla normativa e agli accorgimenti comportamentali in tema di data protection.

14. Documentazione di riferimento

ID	TITOLO	DATA EMISSIONE
1	Regolamento Europeo 2016/679 – General Data Protection (GDPR)	Ottobre 2016
2	Linee guida in materia di notifica delle violazioni di dati personali (Data Breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 Versione emendata e adottata il 6 febbraio 2018	Febbraio 2018
3	Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali http://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili	

15. Definizioni

TERMINE	DEFINIZIONE
Dato personale	Dato atto ad individuare univocamente una persona fisica
Dato sensibile - categorie particolari di dati personali	Nella pratica operativa si possono considerare le seguenti tipologie: o I dati idonei a rivelare le origini razziali ed etniche. o I dati idonei a rivelare le convinzioni religiose o filosofiche o l'appartenenza sindacale o I dati idonei a rivelare lo stato di salute o alla vita sessuale o I dati idonei a rivelare le convinzioni politiche o Dati di carattere giudiziario o Dati biometrici intesi a identificare in modo univoco una persona fisica o Dati genetici

16. Approvazione della Policy

La presente Procedura è stata approvata dal Legale Rapresentante ing. Paolo Ciuffo in data 18/05/2018.

Si chiarisce che l'Azienda si riserva di effettuare eventuali variazioni al presente regolamento o al suo allegato, e che le stesse verranno comunicate agli Utenti.

Roma, 18 maggio 2018