FIDA
Finanza Dati Analisi

DATA PROTECTION PROGRAM

Misure di sicurezza

Settembre 2018 – Rev. 2.0

FINANZA DATI ANALISI Srl
P.IVA e Cod. Fisc. 06512970960 – Cap. Soc. 100.000 euro i.v. – R.E.A. TO 1104529
Via Cernaia, 31 – 10121 TORINO, Italia – Tel. +39 011.5813.777 Fax +39 011.5813.741
www.fidaonline.com

DATA PROTECTION PROGRAM

La finalità del presente documento è quella di fornire una sintesi delle misure tecniche e organizzative adottate ai sensi del regolamento UE 679/2016.
Per qualsiasi informazione, chiarimento o segnalazione è possibile inviare una e-mail all'indirizzo dataprotection@fida.financial

Localizzazione del Data Center

I server utilizzati da FIDA SRL per l'erogazione dei servizi oggetto del presente documento sono localizzati presso un nostro fornitore di servizi cloud presente sul territorio nazionale, nominato come Responsabile del Trattamento.

Accesso ai sistemi

L'autenticazione ai sistemi è gestita con l'inserimento di username e strong password, e l'accesso è consentito attraverso una VPN utilizzando client VPN preventivamente autenticato oppure in remote desktop ma con indirizzi IP specifici appartenenti ai client autorizzati.

L'accesso ai sistemi è consentito solo a personale autorizzato per le necessità strettamente attinenti all'erogazione dei servizi e per la manutenzione e l'aggiornamento degli stessi. Esiste una politica di change management che prevede l'esecuzione di aggiornamenti e/o manutenzioni preventivamente definiti in accordo con il nostro fornitore di servizi cloud.

Politiche di ridondanza e resilienza dei sistemi

I server sono localizzati presso il datacenter del nostro fornitore di servizi cloud (TIER IV) che soddisfa i requisiti della certificazione ISO 27001:2013 e adotta delle policy interne (verificate e aggiornate annualmente) che supportano la Business Continuity (Business Impact Analysis e Business Continuity Plan).
La policy include:

- Ruoli e Responsabilità coinvolti
- Criteri di attivazione
- Communication Plan
- Modalità e tempi di recovery (per ogni Business Unit)
- Contatti per l'emergenza
- RTO e RPO
- Procedure, periodicità e modalità dei test
- Siti di DR

La Business Continuity viene testata annualmente e viene effettuato un verbale di audit. In caso vengano rilevate non conformità viene predisposta un'azione correttiva.

Pseudonimizzazione e crittografia

Al momento la crittografia del dato non è implementata ma è in fase di valutazione la sua applicazione.

La pseudonimizzazione è già implementata evitando una associazione immediata dell'utente ai suoi dati.

Politiche di backup

I backup hanno frequenza giornaliera e sono schedulati alle 4.00, tutti i giorni quello incrementale e la domenica quello synthetic full; la retention dei dati è attualmente di 15 giorni

I backup sono memorizzati nel Backup Center del nostro fornitore di servizi cloud.

Politiche di sicurezza

Oltre ai dispositivi canonici di virus/malware detection e firewall sono implementati un servizio di Intrusion Protection e Next-Generation Firewall

Supporto durevole

In considerazione del fatto che sono state adottate misure organizzative e tecniche in relazione al grado di rischio rilevato, si esclude la possibilità di qualsiasi modifica del suo contenuto di provenienza esterna, quindi anche il sito internet può considerarsi un valido supporto duraturo.
Il personale di FIDA autorizzato al trattamento del dato in oggetto è preventivamente informato sugli aspetti relativi alla privacy (tipologia di dato personale) alla sicurezza ed alla riservatezza delle informazioni.