MrDisk | Forensic & Data Recovery

DOCUMENTO INFORMATIVO PER IL CLIENTE E IL SUO LEGALE

Linee guida per la valutazione giuridica e l’eventuale conferimento di incarico tecnico

Oggetto: valutazione della possibilità di accesso e recupero dei dati da un iPhone appartenuto a persona maggiorenne deceduta circa diciotto mesi fa, con eventuale analisi di ulteriori dispositivi e archivi digitali.

Il presente documento ha finalità esclusivamente informative e tecniche. Non costituisce un parere legale, né un’autorizzazione a effettuare operazioni sul dispositivo. Il legale incaricato dovrà verificare la legittimazione del richiedente e individuare gli atti necessari prima dell’avvio delle attività.

1. Presupposti giuridici e tutela dei dati

L’accesso ai dati personali di una persona deceduta può richiedere una valutazione ai sensi dell’art. 2-terdecies del D.Lgs. 196/2003, oltre all’esame di eventuali limitazioni, diritti di terzi, condizioni dei fornitori dei servizi e altre norme applicabili. La qualità di genitore o familiare non comporta automaticamente un diritto illimitato di accesso all’intero contenuto del telefono o degli account.

Si richiede pertanto al legale di verificare la legittimazione del soggetto richiedente, le finalità concrete del recupero e il perimetro dei dati ai quali sia consentito accedere, nonché l’eventuale necessità di ulteriori consensi, autorizzazioni o provvedimenti.

2. Limiti tecnici dello sblocco di un iPhone

Non tutti i codici di sblocco degli iPhone possono essere recuperati o sottoposti a tentativi tecnici efficaci. Le possibilità dipendono dal modello, dalla versione di iOS, dalle protezioni crittografiche, dallo stato del dispositivo e dagli strumenti concretamente disponibili.

Alcune procedure di acquisizione richiedono uno stato operativo detto After First Unlock (AFU): il telefono deve essere stato sbloccato almeno una volta dopo l’ultima accensione. In questo stato possono rimanere disponibili determinate chiavi crittografiche e condizioni di accessibilità; un riavvio o spegnimento può farle perdere. Ciò non implica che il PIN corretto sia memorizzato in chiaro nella cache o sia direttamente estraibile.

Dato il tempo trascorso dal decesso, è possibile che l’iPhone sia stato spento, riavviato o abbia esaurito la batteria: in tali circostanze alcune tecniche potrebbero non essere applicabili. Il solo trascorrere del tempo, tuttavia, non dimostra quale sia l’attuale stato crittografico del dispositivo.

3. Percorsi alternativi: account, credenziali e backup

Oltre all’accesso diretto al telefono, può essere utile verificare la presenza di backup locali o cloud e di informazioni relative ad Apple Account (già Apple ID), indirizzi email, numeri telefonici, dispositivi associati, chiavi di recupero e altri account digitali.

Il recupero dell’Apple Account non elimina automaticamente il codice di accesso dell’iPhone. Potrebbe però consentire, quando giuridicamente e tecnicamente possibile, di recuperare alcuni dati sincronizzati o presenti in copie di sicurezza, anche mediante procedure ufficiali dei fornitori.

4. Eventuale estensione ad altri dispositivi e supporti

Con specifica autorizzazione e nel rispetto della legittimazione accertata, potrebbe essere opportuno analizzare computer, notebook, tablet, iPad, precedenti smartphone, chiavette USB, dischi esterni, schede di memoria e archivi di backup appartenuti al defunto.Questi supporti potrebbero contenere annotazioni di codici, password salvate, portachiavi digitali, database applicativi, file di configurazione o backup. Le informazioni possono essere in chiaro oppure cifrate; l’eventuale recuperabilità delle credenziali cifrate deve essere verificata caso per caso. Non è possibile presumere che il codice dell’iPhone sia

effettivamente presente altrove.

5. OSINT e ricostruzione degli identificativi digitali

Un’eventuale attività OSINT può essere finalizzata a individuare informazioni legittimamente accessibili utili a ricostruire account, identificativi e servizi utilizzati dal defunto. Devono essere esclusi accessi abusivi, impersonificazioni, acquisizioni ingannevoli di credenziali e attività su account di terzi non autorizzate.

6. Contenuto consigliato dell’incarico formale • Identificazione del richiedente, titolo di legittimazione e documentazione a supporto (incluso certificato di morte, ove necessario).

• Identificazione puntuale dell’iPhone e degli eventuali ulteriori dispositivi o supporti da esaminare.

• Indicazione delle finalità, delle categorie di dati ricercate e dei limiti dell’accesso, con particolare riguardo alle comunicazioni di terzi.

• Autorizzazione distinta per la valutazione tecnica preliminare e, solo successivamente, per le specifiche operazioni di acquisizione, tentativo di accesso e recupero dati.

• Eventuale autorizzazione separata per analisi di backup, credenziali, account e attività OSINT lecite.

• Istruzioni per trattamento, conservazione, protezione, restituzione o cancellazione dei dati, nonché per la documentazione delle operazioni e i destinatari dei risultati.

7. Procedura operativa e fattibilità

MrDisk propone una prima fase di valutazione documentale e tecnica, preferibilmente non invasiva, prima di concordare qualsiasi intervento successivo e i relativi costi. È opportuno preservare lo stato attuale dell’iPhone, evitando riavvii, aggiornamenti, ripristini e tentativi ripetuti di codice non concordati con il laboratorio.

Non viene garantito lo sblocco del dispositivo né il recupero totale o parziale dei dati. Il laboratorio potrà accettare l’incarico soltanto dopo la verifica della documentazione e delle condizioni tecniche e giuridiche necessarie.

Richiesta al legale Si invita il professionista incaricato a valutare i presupposti giuridici dell’intervento e, se ritenuto ammissibile, a predisporre un mandato tecnico scritto con autorizzazioni specifiche, perimetro operativo e adeguate tutele per tutti i soggetti interessati. Il legale potrà interfacciarsi direttamente con MrDisk per definire le attività tecniche concretamente ipotizzabili.