T – VERIFICHE E CONTROLLI DELLE MISURE TECNICHE E ORGANIZZATIVE (TOM)

Org. di Cert.:
Richiedente:
Target of Evaluation:
Nome (Esperto):
Data:

I seguenti criteri sono volti a disciplinare le misure tecniche e organizzative messe in atto per garantire la sicurezza dei dati personali trattati. I "Mezzi di Verifica Suggeriti", unitamente alla documentazione di riferimento, dovranno essere esaminati alla luce di tali criteri sino al reperimento di evidenze adeguate a sancirne il soddisfacimento.

Ref ID	Richiedente	Specifico / Generico	Livello	TITOLO	CRITERI applicabili al Target of Evaluation (clausole prescrittive)	GUIDA ALL'ATTUAZIONE (clausole informative)	Mezzi di verifica suggeriti	GDPR
T.1			**A**	**Requisiti fondamentali di sicurezza** Il Richiedente deve adottare misure adeguate per proteggere i dati personali e garantirne la riservatezza, l'integrità e la disponibilità.				
T.1.1				**Limitazione dell'accesso ai dati**				
T.1.1.1	CP	G	A	Minimizzazione dei diritti di accesso (principio del minimo privilegio)	A) I diritti di accesso devono essere limitati e concessi solo in base alle necessità, in conformità con il principio del "Minimo privilegio".	I diritti di accesso ai dati devono essere minimizzati e limitati esclusivamente ai dipendenti che necessitano di accedere ai dati e solo alle informazioni necessarie per svolgere le loro mansioni. Inoltre, il Richiedente deve adottare delle misure di sicurezza aggiuntive per i profili con privilegi elevati, come gli amministratori di sistema.	Registro e regole sui diritti di accesso. Ispezione.	25, 32
T.1.1.2	CP	G	A	Aggiornamenti del registro dei diritti di accesso	A) Deve essere adottata una procedura o un meccanismo per adeguare sistematicamente i diritti di accesso nei casi in cui un dipendente lasci l'azienda o cambi mansione all'interno della stessa.	Registro e gestione dei diritti di accesso Le procedure per la concessione e la revoca dei diritti di accesso devono essere presentate.	Procedure e meccanismi Ispezione e analisi di test a campione Intervista ai DPO e ai dipendenti	32

T.1.1.3	CP	G	A	Password policy	A) Deve essere definita una Password Policy che specifichi la lunghezza minima, i requisiti di complessità e la frequenza di rinnovo delle password. E B) Ove applicabile, la Password Policy per l'accesso ai dati archiviati deve essere conforme alle leggi e normative nazionali.	Il Richiedente deve disporre di una Password Policy che richieda un livello di autenticazione sufficientemente robusto per l'accesso ai dati personali. La Password Policy può essere soggetta a normative, linee guida e obblighi nazionali. Organizzazioni come l'ENISA forniscono indicazioni utili sulla gestione delle password e sulle policy, che possono essere utilizzate come riferimento. La policy o il meccanismo adottato deve imporre l'uso di un metodo di autenticazione adeguato per l'accesso al server. Inoltre, deve essere prevista una policy che imponga la modifica delle password di accesso al server quando necessario.	Revisione della documentazione. Ispezione e dimostrazione. Verifica del meccanismo di controllo degli accessi.	32
T.1.1.4	CP	G	A	Restrizione dell'accesso fisico	A) L'accesso alle stanze in cui i dati personali sono archiviati sui server deve essere ristretto e protetto da meccanismi efficaci di controllo degli accessi.	I siti che ospitano dati personali devono essere situati in un ambiente fisicamente sicuro e dotato di un efficace controllo degli accessi.	Ispezione dei controlli di accesso fisico e delle regole di accesso fisico.	25, 32
T.1.1.5	CP	G	A	Bring Your Own Device Policy	A) Il Richiedente deve disporre di una policy scritta che: a.1) limiti l'uso dei dispositivi mobili personali; a.2) (E) sia conosciuta dai dipendenti che hanno accesso ai server.	Una policy deve essere applicata per controllare e limitare l'accesso ai server in cui sono archiviati i dati personali tramite dispositivi mobili, come smartphone, laptop e chiavette USB. Deve essere adottata una policy scritta in modo chiaro, conosciuta dai dipendenti che hanno accesso ai dati. Ove applicabile, devono essere eseguite ispezioni e le porte USB devono essere disabilitate.	Policy Ispezione Intervista ai dipendenti	32
T.1.1.6	CP	G	B	Logout automatico della sessione	A) L'accesso ai dati personali archiviati deve essere protetto da un meccanismo di disconnessione automatica della sessione.	Deve essere previsto un meccanismo che renda automatico il log-out e faccia terminare la sessione in caso di inattività dell'utente.	Ispezione e dimostrazione. Verifica del meccanismo di controllo degli accessi.	25, 32
T.1.1.7	CP	S	B	Autenticazione a più fattori	A) L'accesso ai dati archiviati da parte dei dipendenti e degli agenti del Richiedente deve richiedere l'autenticazione a più fattori.	L'accesso ai server che archiviano dati personali deve essere controllato tramite un meccanismo di autenticazione adeguato. Il meccanismo deve essere proporzionato al valore dell'asset protetto, con l'uso di password sufficientemente sicure per dati di basso valore e autenticazione a più fattori per dati di valore maggiormente elevato.	Ispezione e dimostrazione. Verifica del meccanismo di controllo degli accessi.	32

T.1.2				**Crittografia dei dati**				
T.1.2.1	CP	G	A	Comunicazione crittografata su reti pubbliche	A) Il Richiedente deve disporre di regole, policy o meccanismi per garantire che l'accesso remoto ai dati personali sia crittografato quando transita attraverso reti pubbliche, come Internet.	Il Richiedente deve garantire che le regole, le policy o i meccanismi adottati prevedano la crittografia nella trasmissione dei dati personali su reti pubbliche, inclusa quella tra il cliente e una pagina web.	Revisione della documentazione. Ispezione del sito web. Test a campione. Analisi e verifiche dei flussi di dati. Intervista al CISO.	25, 32, Re-cita le 83
T.1.2.2	CP	G	B	Crittografia dei backup	A) I file di backup devono essere crittografati.	La crittografia dello storage del sistema operativo del server deve essere attivata e la configurazione deve essere documentata nella policy di gestione della crittografia.	Ispezione e dimostrazione. Analisi a campione.	25, 32
T.1.2.3	CP	G	B	Crittografia dei log utente	A) I log degli accessi degli interessati, inclusi i log dei siti web, devono essere crittografati.	I log di accesso web del servizio utilizzato per raccogliere dati personali devono essere crittografati.	Ispezione e dimostrazione. Analisi a campione.	25, 32
T.1.2.4	CP	S	B	Crittografia dei dati a riposo	A) I dati personali archiviati devono essere crittografati.	I dati a riposo (dati archiviati) sui server e sui dispositivi hardware mobili devono essere crittografati e/o protetti da password. La crittografia dello storage del sistema operativo client deve essere attivata e la sua configurazione deve essere documentata nella policy di gestione della crittografia.	Ispezione e dimostrazione. Analisi a campione.	25, 32

T.1.3				Altre misure di sicurezza				
T.1.3.1	CP	G	A	Test di ripristino del backup	A) Deve essere prevista una procedura per eseguire un test di ripristino dei dati almeno una volta all'anno. B) L'ultimo test di ripristino del backup deve essere stato eseguito da meno di 12 mesi. C) Qualora i test di ripristino individuino problemi da risolvere, il Richiedente deve aver adottato le opportune misure correttive.	Il sistema di ripristino dei dati basato sui file di backup deve essere stato testato con successo negli ultimi 12 mesi. I requisiti del test di ripristino devono tenere conto dei rischi specifici per gli interessati. Ad esempio, se i dati personali sono conservati da un ospedale, il tempo di ripristino deve essere ridotto al minimo, poiché il rischio per gli interessati è più elevato, mentre il ripristino di un elenco clienti di una panetteria ha un impatto minore. Per impostazione predefinita, un test di ripristino del backup è considerato riuscito se è in grado di ripristinare oltre il 99% dei dati entro un massimo di 48 ore. La frequenza dei test deve essere adeguata e aumentata in caso di trattamento di dati ad alto rischio. Inoltre, deve essere considerato l'utilizzo di backup offline geograficamente separati, in particolare quando il trattamento riguarda dati critici.	Report del test di ripristino del backup. Intervista al CISO.	32
T.1.3.2	CP	G	A	Aggiornamenti regolari del server	A) Deve essere prevista una procedura, una configurazione o un meccanismo per garantire che i server vengano aggiornati regolarmente e ogni volta che è necessaria una patch di sicurezza critica. E B) I server devono essere aggiornati e corretti con le patch di sicurezza in modo efficace e con regolarità, secondo le necessità.	È necessario produrre una documentazione relativa a questi test e applicare metriche di copertura. Il Richiedente dovrebbe considerare l'esecuzione di regression tests nel caso in cui un aggiornamento, sia esso di sicurezza o generale, possa influire sull'ambiente di produzione e quindi sulla disponibilità dei dati. Ciò potrebbe comportare un rischio elevato per gli interessati, a seconda del tipo di trattamento effettuato.	Regole e procedure. Report dei test. Ispezione e analisi di test a campione. Intervista ai DPO e ai dipendenti.	32
T.1.3.3	CP	G	B	Mitigazione degli attacchi Denial of Service (DoS)	SE i dati personali sono destinati ad essere accessibili online dagli Interessati, ALLORA: A) Devono essere adottate misure per mitigare il rischio di attacchi Denial of Service (DoS).	Devono essere adottate misure, come firewall, load balancer o soluzioni equivalenti, per mitigare l'impatto degli attacchi Denial of Service (DoS).	Mitigazione degli attacchi Denial of Service (DoS).	32
T.1.3.4	CP	G	B	Protezione da incendi e allagamenti	A) Devono essere adottate misure di protezione per proteggere i server in cui sono archiviati i dati personali da: a.1) incendi; a.2) (E) allagamenti.	I server che contengono dati personali devono essere collocati in una stanza protetta contro incendi e allagamenti. Devono essere installati rilevatori di fumo e incendio.	Ispezione delle misure di protezione contro incendi e allagamenti.	32

T.1.3.5	CP	G	B	Implementazione di firewall con policy di accesso alle porte basata sul principio del minimo privilegio.	A) Deve essere implementato e configurato un firewall per proteggere i server accessibili da remoto che archiviano dati personali. E B) La configurazione del firewall deve bloccare tutte le porte che non sono necessarie.	Un sistema di firewalling deve essere implementato per proteggere l'infrastruttura ICT relativa ai dati personali del Titolare del trattamento (o del Responsabile del trattamento).	Configurazione del firewalling. Test. Intervista al CISO.	25, 32
T.1.3.6	CP	G	B	Antivirus aggiornato	A) Deve essere implementata una soluzione di sicurezza, che includa almeno un'applicazione antivirus, per proteggere i server e i dispositivi terminali sotto il controllo del Richiedente utilizzati per il trattamento nel Target of Evaluation. E B) Deve essere prevista una policy, una procedura o un meccanismo per garantire che la soluzione di sicurezza venga mantenuta aggiornata.	Devono essere implementate soluzioni antivirus e anti-spyware per proteggere l'infrastruttura ICT relativa ai dati personali del Titolare del trattamento.	Ispezione. Data dell'ultimo aggiornamento antivirus.	32

T.2			**B**	**Requisiti di sicurezza avanzati** **SE il Target of Evaluation include un trattamento di dati ad alto rischio, come specificato nello Schema di Certificazione (2.4.2), ALLORA:**				
T.2.1				**Verifiche di connettività per l'accesso a Internet** Condizione: SE il Target of Evaluation include l'accesso a Internet, ALLORA:				
T.2.1.1	CP	G	B	HTTPS abilitato	A) L'HTTPS deve essere abilitato di default per l'accesso all'interfaccia web.	La conformità dell'interfaccia web deve essere dimostrata e testata.	Ispezione e test	32
T.2.1.2	CP	G	B	SDNS abilitato	A) Il Secure DNS (SDNS) deve essere abilitato per la risoluzione dei nomi di dominio pubblici.	La conformità dell'interfaccia web deve essere dimostrata e verificata attraverso test.	Ispezione e test	32
T.2.1.3	CP	G	B	SSL	A) NON deve essere utilizzato un SSL non sicuro.	. L'uso di SSL 2.0 è proibito e SSL 3.0 non è sicuro. Questa restrizione deve essere riflessa nella policy degli strumenti crittografici e, ove applicabile, deve essere oggetto di test.	Ispezione e test	32
T.2.1.4	CP	G	B	TLS	A) NON deve essere utilizzato un TLS non sicuro.	TLS 1.1 non è sicuro. Versioni superiori di TLS possono essere utilizzate se considerate sufficientemente sicure. Il protocollo di sicurezza della rete deve essere configurato correttamente. Questa configurazione deve essere riflessa nella policy degli strumenti crittografici e, ove applicabile, deve essere oggetto di test.	Ispezione e test	32
T.2.1.5	CP	G	B	SSH	A) NON deve essere utilizzato un SSH non sicuro.	SSH-1 non è sicuro, mentre SSH-2 è accettabile. Questa distinzione deve essere riflessa nella policy degli strumenti crittografici. L'uso di SSH non sicuro deve essere evitato. Ove applicabile, deve essere oggetto di test	Ispezione e test	32
T.2.1.6	CP	G	B	Incompatibilità retroattiva	A) La compatibilità retroattiva con versioni non sicure di SSL o TLS deve essere disabilitata.	Deve essere eseguito un test del protocollo per dimostrare che i client legacy vengono rifiutati.	Ispezione e test	32
T.2.1.7	CP	G	B	WiFi	SE il Target of Evaluation tratta dati personali tramite WiFi, ALLORA: A) L'accesso WiFi deve essere configurato per utilizzare: a.1) WPA2 o superiore; a.2) WPA2-PSK o superiore; a.3) una soluzione sicura almeno quanto WPA2. E B) La rete WiFi accessibile ai visitatori deve essere separata dalla rete WiFi utilizzata per scopi interni.	I punti di accesso WiFi rappresentano punti di ingresso vulnerabili alla rete per gli hacker e devono essere adeguatamente protetti.	Ispezione e test	32
T.2.2				**Gestione della crittografia**				

T.2.2.1	CP	G	B	Policy di gestione degli strumenti di protezione	A) Deve esistere una policy scritta che inquadri l'introduzione, la manutenzione e la graduale eliminazione degli strumenti di protezione.	La policy è esplicita, specifica e completa. Deve compilare un elenco di tutti gli strumenti utilizzati.	Policy. Ispezione. Intervista ai dipendenti.	32
T.2.2.2	CP	G	B	Policy crittografica	A) Il Richiedente deve disporre di una policy crittografica che specifichi: a.1) gli algoritmi crittografici da utilizzare; a.2) (E) la generazione, l'aggiornamento, la conservazione in escrow e la revoca (distruzione) delle chiavi; a.3) (E) i requisiti adeguati di lunghezza delle chiavi; a.4) (E) il periodo di tempo dopo il quale le chiavi devono essere sostituite.	La policy deve essere esplicita, specifica e completa. Deve includere un elenco di tutti gli algoritmi utilizzati.	Policy crittografica.	32
T.2.2.3	CP	G	B	Lunghezza della chiave	A) La lunghezza delle chiavi deve essere adeguata agli standard attuali, garantendo un livello di sicurezza simmetrico per i dati transazionali di almeno: a.1) 80 bit per dati archiviati per meno di 5 anni; a.2) 128 bit per dati destinati a essere archiviati per un periodo di 5 anni o più.	I requisiti minimi attuali per la lunghezza delle chiavi devono essere equivalenti a un livello di sicurezza simmetrico di: 1. 80 bit per i dati transazionali; 2. 128 bit per i dati con un requisito di riservatezza fino a 5-10 anni.	Ispezione Test a campione	32
T.2.2.4	CP	G	B	Aggiornamento delle chiavi	A) Le chiavi devono essere aggiornate tempestivamente in conformità con la policy di gestione delle chiavi.	La policy deve specificare l'intervallo di tempo o le condizioni in base alle quali le chiavi devono essere sostituite.	Ispezione Test a campione	32
T.2.2.5	CP	G	B	Revoca delle chiavi	A) Le chiavi compromesse devono essere revocate in modo efficace.	La policy di gestione delle chiavi deve specificare come vengono revocate le chiavi.	Ispezione Test a campione	32

T.2.3				**Penetration Test e monitoraggio**				
T.2.3.1	CP	G	B	PEN Test	A) Il Richiedente deve eseguire penetration tests: a.1) su base annuale e dopo variazioni significative che possono incidere sulla sicurezza; a.2) (E) l'ultimo Penetration test deve risalire a meno di 12 mesi prima; a.3) (E) deve esistere una procedura per assicurare che i risultati dei PEN Tests siano presi in considerazione.	I Penetration test devono essere eseguiti su sistemi che conservano informazioni che appartengono a categorie particolari di dati personali. Gli attacchi da considerare includono: SQL injection, script, Crosssite scripting, buffer overflow, Man in the Middle, replay, ecc.	Penetration Test	*32*
T.2.3.2	CP	G	B	Rilevamento degli accessi non autorizzati	A) Il Richiedente deve disporre di regole, procedure o meccanismi per rilevare e segnalare gli accessi non autorizzati.	Il monitoraggio degli accessi non autorizzati e degli attacchi è un elemento fondamentale per garantire la sicurezza.	Ispezione Penetration Test	*32*