

Principi, Diritti e Misure Tecniche e Organizzative – Requisiti/Schede di Audit

Si indicano, in base alla loro applicabilità in relazione al servizio erogato per conto del Titolare, i principi di trattamento e i diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) unitamente alle misure di sicurezza previste.

Le indicazioni fornite nel presente allegato relative alle misure di sicurezza sono estrapolate dalle Linee Guida ENISA relative alla sicurezza dei trattamenti di dati personali: esse dovranno essere riportate all'interno del Registro dei Trattamenti del Responsabile.

Principi di Trattamento e Diritti degli Interessati

Req.	Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)
A.1	Art. 5.1.b – Misure per garantire la limitazione della finalità del trattamento (dati non utilizzati per altre finalità)
A.2	Art. 5.1.c – Misure per garantire la minimizzazione dei dati del trattamento
A.3	Art. 5.1.d – Misure per garantire la esattezza/qualità dei dati
A.4	Art. 5.1.e – Misure per garantire la limitazione della conservazione
A.5	Art. 15 – Misure per garantire il diritto di Accesso dell'interessato
A.6	Art. 16 – Misure per garantire il diritto di Rettifica
A.7	Art. 17 – Misure per garantire il diritto alla Cancellazione ("Oblio") – ove applicabile
A.8	Art. 18 – Misure per garantire il diritto alla Limitazione del Trattamento
A.9	Art. 19 – Misure per garantire l'obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento
A.10	Art. 20 – Misure per garantire il diritto alla portabilità dei dati – ove applicabile
A.11	Art. 21 – Misure per garantire il diritto di Opposizione
A.12	Art. 22 - Misure per garantire la sicurezza in caso di processo decisionale automatizzato relativo alle persone fisiche, compresa la <i>profilazione</i>

Misure di Sicurezza

Il perimetro di sicurezza definito come ambito di applicazione delle misure di sicurezza di seguito elencate è costituito dal servizio effettuato dal Responsabile per conto della ASL di Pescara; di conseguenza le seguenti misure sono applicabili all'organizzazione, alle informazioni/dati, agli strumenti HW, SW e di rete ed al personale coinvolti nell'erogazione del servizio contrattualizzato.

Le presenti misure di sicurezza verranno utilizzate quale riferimento per l'esecuzione degli audit previamente concordati.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Politiche di sicurezza e procedure per la protezione dei dati personali	1.1	Il Responsabile deve disporre di una propria regolamentazione (o politica di sicurezza) in materia di protezione dei dati personali conforme alla normativa vigente e che disciplini i servizi erogati per conto del Titolare.
	1.2	La regolamentazione di cui al punto precedente deve essere riesaminata e aggiornata almeno su base annuale.
	1.3	La regolamentazione deve essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.
	1.4	La regolamentazione deve disciplinare almeno i seguenti punti: ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili e sub-responsabili del trattamento dei dati e per le altre terze parti coinvolte nel trattamento dei dati personali.
Ruoli e responsabilità	2.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.
	2.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
	2.3	Deve essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
Riservatezza del personale	3.1	Il Responsabile deve garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di attivazione del Servizio/Contratto.
	3.2	Prima di assumere i propri compiti, il personale del Responsabile deve essere invitato a riesaminare e concordare la Regolamentazione di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
Formazione	4.1	Il Responsabile deve garantire che tutto il personale sia adeguatamente formato sui controlli di sicurezza previsti per il servizio e per gli eventuali sistemi informatici ad esso correlati. Il personale coinvolto nel trattamento dei dati personali deve inoltre essere adeguatamente informato e periodicamente aggiornato in merito ai requisiti in materia di protezione dei dati e agli obblighi previsti dalla normativa vigente attraverso regolari campagne di sensibilizzazione.
	4.2	Il Responsabile deve disporre programmi di formazione (relativi alla protezione dei dati personali e alla sicurezza delle informazioni) strutturati e regolari per il proprio personale, compresi programmi specifici per l'inserimento di eventuali nuovi arrivati (es.: job rotation, nuove assunzioni, ecc...).
Politica controllo accessi	5.1	Specifici diritti di accesso devono essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
	5.2	Deve essere definita una politica di controllo degli accessi. Nel documento l'organizzazione deve determinare le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.
	5.3	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata.
Controllo accessi e autenticazione	6.1	Ove fornita dall'Organizzazione, deve essere attuata la politica di controllo accessi applicabile a tutti gli utenti che accedono ai sistemi IT, con particolare riguardo agli aspetti relativi alla creazione, approvazione, riesame ed eliminazione degli account.
	6.2	L'uso di account generici (non personali) deve essere evitato. Nei casi in cui ciò sia necessario, l'utilizzo deve essere autorizzato dal referente dell'Organizzazione. Qualora tale autorizzazione fosse fornita, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
	6.3	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, deve essere presente un meccanismo di autenticazione che consenta l'accesso che sia in linea con la politica di controllo degli accessi ove fornita dall'Organizzazione. Come minimo deve essere utilizzata una combinazione di user-id e password.
	6.4	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, il sistema di controllo degli accessi deve essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano i criteri definiti al punto precedente.
	6.5	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio deve essere possibile configurare i seguenti parametri relativi alle password: complessità, maximum age, password history, lunghezza e il numero di tentativi di accesso non riusciti accettabili. I criteri dovranno essere concordati con il referente dell'Organizzazione (in base alla politica di controllo accessi).

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Gestione risorse e degli asset	7.1	Deve essere predisposto un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete), in funzione di quanto applicabile al servizio esternalizzato. Il compito di mantenere e aggiornare il registro deve essere esplicitamente assegnato.
	7.2	Le risorse IT all'interno del registro essere riesaminate e aggiornate regolarmente.
	7.3	I ruoli che hanno accesso alle risorse devono essere definiti e documentati. In particolare devono essere definite le responsabilità in relazione alle risorse.
Sicurezza fisica	8.1	Il perimetro fisico dei locali in cui è ospitata l'infrastruttura IT utilizzata a fini di erogazione del servizio o vengono effettuati trattamenti di dati personali del Titolare deve essere accessibile esclusivamente a personale esplicitamente autorizzato da parte del Responsabile.
	8.2	Il personale autorizzato all'accesso ai locali di trattamento o ai locali in cui è ospitata l'infrastruttura IT per l'erogazione del servizio deve essere dotato di strumenti di identificazione personali (es. badge identificativi, PIN personali).
	8.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Deve essere mantenuto e monitorato in modo sicuro un registro fisico o una traccia elettronica del controllo di tutti gli accessi.
	8.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.
	8.5	Dovrebbero essere predisposte barriere fisiche per impedire l'accesso fisico non autorizzato.
	8.6	Le aree dei locali non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate.
	8.7	Nella sala server devono essere predisposti opportuni sistemi antincendio automatici, sistemi dedicati di climatizzazione e gruppi di continuità (UPS) che garantiscano l'erogazione sicura del servizio secondo quanto stabilito contrattualmente.
	8.8	Il personale di supporto esterno deve avere accesso limitato alle aree protette.
Change management	9.1	L'organizzazione deve adottare un processo di cambiamento che consenta di assicurarsi che tutte le modifiche al sistema/servizio siano opportunamente registrate (anche con eventuali aggiornamenti dell'inventario delle risorse) e monitorate.
	9.2	Ogni Cambiamento al sistema/servizio deve essere previamente segnalato al referente interno dell'organizzazione (committente) e da questi autorizzato. Nella segnalazione devono essere documentati: gli estremi del cambiamento (es.: cambiamento di versione), le tempistiche, eventuali prescrizioni aggiuntive che prevedano azioni da adottare prima che il cambiamento sia operativo (es.: formazione utenti).
	9.3	Lo sviluppo del software deve essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali in produzione. Quando è necessario eseguire i test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, il fornitore deve predisporre specifiche procedure per la protezione dei dati personali utilizzati nei test.
Logging e monitoraggio	10.1	I log devono essere attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	10.2	I log devono essere registrati e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica fonte temporale di riferimento (server NTP).
	10.3	È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.
	10.4	Non deve essere possibile la cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio effettuato per la rilevazione di attività insolite.
	10.5	Deve essere configurato un sistema di monitoraggio per l'elaborazione dei log e la produzione di rapporti sullo stato del sistema e notifica di potenziali allarmi.
Protezione dal malware	12.1	Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
Backup	14.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità; devono essere definite e documentate le strategie di backup da applicare ai dati in maniera coerente con il livello di criticità (RPO) dei servizi a cui afferiscono
	14.2	Ai backup deve essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	14.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	14.4	Le strategie di backup definite devono essere completate regolarmente.
	14.5	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati.
	14.7	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.
	14.8	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare dei dati.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
Sicurezza Server e Database	15.1	I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	15.2	I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione.
	15.3	Nei sistemi utilizzati per l'erogazione del servizio, devono essere considerate soluzioni di crittografia per i dati at rest, in transit e in use. Qualora non ritenute applicabili, deve essere data adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati
	15.4	Nei sistemi utilizzati per l'erogazione del servizio, ove possibile, devono essere applicate tecniche di pseudonimizzazione attraverso la separazione dei dati dagli identificatori al fine di evitare il collegamento diretto con l'interessato. In caso non fosse possibile, deve essere fornita adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati.
Network/Communication security	16.1	Deve essere predisposta e monitorato il rispetto di una policy per la Sicurezza di Rete (Network Security Policy) e per la gestione delle Comunicazioni Sicure (Network Communication Security) che preveda l'adozione di misure di cifratura delle comunicazioni nell'ambito dei processi di trattamento effettuati (TLS/Https, VPN, SSH, ecc...).
Sicurezza desktop/laptop/mobile	17.1	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza.
	17.2	Le applicazioni anti-virus e le relative signatures devono essere configurate regolarmente in maniera continuativa.
	17.3	Gli utenti non devono avere i privilegi per installare applicazioni software non autorizzate o disattivare applicazioni autorizzate
	17.4	I sistemi utilizzati per l'erogazione del servizio, devono disporre di un timeout di sessione nel caso in cui l'utente non sia stato attivo per un determinato periodo di tempo (max 10 min).
	17.5	Gli aggiornamenti critici di sicurezza rilasciati dalle case produttrici di software di sistema devono essere installati regolarmente.
	17.6	Non è consentito il trasferimento di dati personali dai Database dei sistemi aziendali alle workstation utilizzate a fini di assistenza tecnica, se non previa esplicita autorizzazione del Responsabile dei Sistemi Informativi. I dati temporaneamente memorizzati devono essere cancellati alla fine della sessione di lavoro.
	17.7	Non deve essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	17.8	Deve essere abilitata la crittografia dei dischi delle postazioni di lavoro/laptop/device mobili utilizzate nell'ambito dell'erogazione del servizio
Dispositivi portatili	18.1	Le procedure di gestione dei dispositivi mobili e portatili devono essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	18.2	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati: non è consentito l'utilizzo di dispositivi personali, salvo eventuali specifiche autorizzazioni.
	18.3	I dispositivi mobili devono essere soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali (client).
	18.4	Il Responsabile deve individuare e comunicare al Titolare un proprio referente a cui attribuire la responsabilità della gestione dei dispositivi mobili e portatili utilizzati nell'ambito dell'erogazione del servizio.
	18.5	Il Responsabile deve essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso, nel caso in cui questo sia utilizzato nell'ambito dell'erogazione del servizio.
	18.6	In caso di utilizzo promiscuo dei dispositivi mobili (fini di erogazione del servizio al titolare e fini privati) deve essere prevista, mediante opportuni software containers sicuri, la separazione dell'uso privato dall'uso aziendale del dispositivo.
	18.7	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
Sicurezza del ciclo di vita delle applicazioni	19.1	Lo sviluppo degli applicativi deve essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID.
Sub-responsabile del trattamento	20.1	Il Responsabile ed i suoi sub-responsabili adottano le linee guida e le procedure relative al trattamento dei dati personali contenute nell'atto di designazione e nei suoi allegati (tra cui il presente documento).
	20.2	Il Responsabile del Trattamento deve osservare le indicazioni fornite nell'atto di designazione in caso di violazione di dati personali e nelle presenti misure di sicurezza.
	20.3	Il Responsabile deve sottoscrivere l'atto di designazione in cui sono contenuti requisiti formali e obblighi. Il Responsabile del trattamento deve, in risposta, fornire prove documentate sufficienti di conformità (es.: certificazioni di sicurezza, schede tecniche relative alle misure di sicurezza adottate per il servizio/sistema): in caso alternativo, verrà adottata una specifica politica di auditing.
	20.4	Il Responsabile dovrebbe verificare regolarmente la conformità del sub-responsabile al livello concordato di requisiti e obblighi.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	20.5	Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione.
Gestione degli incidenti / Violazione dei dati personali	21.1	Il Responsabile deve predisporre un proprio piano di risposta agli incidenti con procedure dettagliate che preveda la comunicazione al titolare (committente), secondo le indicazioni fornite nell'atto di designazione, al fine di garantire una risposta efficace e ordinata agli incidenti e violazioni relativi ai dati personali.
	21.2	Le violazioni dei dati personali, di competenza del Titolare, devono essere segnalate immediatamente alla Direzione. In qualità di Responsabile devono essere adottate specifiche procedure di supporto al Titolare per la notifica e la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
	21.3	La procedura di gestione delle violazioni di cui al punto precedente, deve essere documentata: essa deve includere un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.
	21.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.
Business Continuity	22.1	Il Responsabile deve predisporre un proprio Piano di Continuità Operativa (BCP - Business Continuity Plan) in relazione all'erogazione del servizio, in linea con quanto previsto dall'Organizzazione (Committente). Tale Piano deve stabilire procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del servizio (ad es.: in caso di incidente / violazione dei dati personali o interruzione del servizio).
	22.2	Il Piano di Continuità Operativa indicato al punto precedente deve includere azioni chiare e assegnazione di ruoli.
	22.3	Il Piano di Continuità Operativa deve essere in linea con il livello di qualità del servizio da garantire all'Organizzazione (Committente), con particolare riguardo alla sicurezza dei dati personali dei processi fondamentali di erogazione.
Cancellazione/eliminazione dei dati	23.1	I supporti di memorizzazione da dismettere devono essere distrutti fisicamente; in caso in cui ciò non sia possibile (es.: per indicazioni contrattuali relative all'assistenza dei dispositivi), prima della loro eliminazione (o riconsegna al fornitore) devono essere sottoposti a tecniche di distruzione dei dati (es.: ripetute operazioni di sovrascrittura con tecniche di clearing/purging).
	23.2	La distruzione di documenti deve avvenire mediante opportuni dispositivi di triturazione.
	23.3	Se sono utilizzati servizi di terzi per eliminare in modo sicuro i supporti di memorizzazione o documenti cartacei, è necessario stipulare uno specifico contratto di servizio e produrre un formale attestato di distruzione.