PROCEDURA AZIENDALE PER TESTARE, VERIFICARE E VALUTARE REGOLARMENTE L'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE IN MATERIA DI PRIVACY

ai sensi dell'art. 32 par.1 lett. d) del Regolamento UE 2016/679

2022

Versione del documento

Versione	Data	Delibera di adozione	Modifiche
1.0			**Prima stesura**

SOMMARIO

1. Scopo del documento

La presente procedura riporta le modalità di conduzione delle attività di test, verifica e valutazione dell'efficacia delle misure di sicurezza fisiche, logiche ed organizzative applicate dall'ASL di Bari e finalizzate alla tutela dei dati personali ed al rispetto dei diritti e delle libertà degli interessati.
Le verifiche di adeguatezza e conformità, configurandosi quali attività di *auditing* interno sono finalizzate ad alimentare un processo di controllo sistematico e continuativo che consenta di rilevare il recepimento dei requisiti normativi stabiliti:

- dal Regolamento UE 2016/679 (GDPR), ai sensi dell'art. 32 par.1 lett. d);
- dal Comitato europeo per la protezione dei dati (EDPB);
- dal D.Lgs 196/2003 (Codice Privacy), così come modificato dal D.Lgs 101/2018;
- dai Provvedimenti dell'Autorità Garante per la protezione dei dati personali.

2. Ambito di applicazione

La presente procedura trova applicazione in tutte le strutture aziendali dell'ASL di Bari ed è da ritenersi estesa anche ai fornitori o sub-fornitori esterni nominati Responsabili del trattamento dei dati, nonché agli eventuali sub-responsabili, nei modi e nei termini definiti nell'art. 28 del Regolamento UE 2016/679.

3. Responsabilità

Competente ad eseguire controlli di adeguatezza e conformità è il DPO, ai sensi di quanto previsto dall'art. 39 del Regolamento UE 2016/679, ovvero terzi opportunamente designati dal Titolare del trattamento per i controlli di conformità normativa.
Nello svolgimento delle attività di che trattasi il DPO o altro soggetto designato dal Titolare del trattamento, ha la facoltà di avvalersi della collaborazione di:

- Personale tecnico specialistico appartenente alle Unità Operative del Titolare del trattamento, avendo cura di evitare conflitti di ruolo che possano compromettere l'imparzialità delle verifiche e l'oggettività delle valutazioni;
- Consulenti esterni incaricati mediante specifici contratti di servizio;
- Servizi di terze parti, erogati da società operanti nel settore della privacy e/o della cybersecurity.

Tutti i soggetti (stakeholder), convolti a vario titolo nelle attività di verifica, sono tenuti a fornire al DPO o altro soggetto designato dal Titolare del trattamento, il supporto necessario alla raccolta delle informazioni utili alla formulazione delle valutazioni di conformità.
In particolare:

- il Direttore Sanitario assicura la piena collaborazione del personale preposto al trattamento di dati riconducibili allo stato di salute degli assistiti;
- il Direttore Amministrativo assicura la piena collaborazione del personale preposto al trattamento di dati amministrativi riconducibili a persone fisiche (es. assistiti, utenti, fornitori);
- il Direttore della UOC Sistemi informativi aziendali assicura la piena disponibilità del personale preposto alla gestione dei sistemi e delle reti informatiche che trattano dati personali direttamente o indirettamente riconducibili a persone fisiche;
- il Direttore della UOC Gestione Patrimonio e della UOC Gestione Tecnica assicurano la piena disponibilità del personale preposto alla gestione dei contratti e convenzioni da quali scaturiscono responsabilità di cui all'art. 28 del Regolamento UE 2016/679;
- il Direttore della UOC Risorse Umane assicura la piena disponibilità e collaborazione del personale preposto al trattamento dei dati riconducibili al personale dipendente;
- i Responsabili e i sub-responsabili di fornitori o sub-fornitori esterni assicurano la piena disponibilità a fornire le informazioni richieste, osservando i principi di trasparenza, tempestività, correttezza e completezza.

4. Programmazione degli audit

Entro il mese di dicembre di ciascun anno, il DPO, coadiuvato dal personale afferente all'UOS Privacy redige il "Programma annuale degli Audit per la conformità normativa al Reg. UE 2016/679" (modello esemplificativo in allegato) che costituisce il documento di pianificazione delle verifiche che si dovranno svolgere nel corso dell'anno solare successivo.
Nel programma devono essere indicate, per ciascuna sessione, al minimo le seguenti informazioni:

- Scopo della verifica;
- Unità operative interessate;
- Tipologia Audit (es. *Vulnerability assessment, Compliance Audit*);
- Calendario attività;

Il programma nella sua versione definitiva deve essere sottoposto alla preventiva approvazione del Titolare del trattamento.

5. Comunicazione degli audit

L'inizio delle attività di audit è concordato con i Responsabili delle strutture interessate, per consentire loro di predisporre tutte le risorse necessarie a supportare le attività dei verificatori. A tale scopo il DPO,

invia una comunicazione formale (avviso di audit) tramite il sistema informativo aziendale ed/o il sistema di gestione documentale.
La suddetta comunicazione ai Responsabili delle strutture interessate, deve contenere, al minimo, le seguenti informazioni:

- Data proposta per l'inizio delle attività;
- Finalità della verifica (es. audit di compliance, audit di sicurezza informatica);
- Oggetto della verifica, specificando a grandi linee il dominio di asset sui quali verranno svolte le verifiche (es. servizi, trattamenti, sistemi informatici, processi aziendali);
- Modalità di verifica (es. interviste al personale, riscontri documentali, test sui sistemi informatici);
- Durata approssimativa delle attività di verifica;

I Responsabili delle strutture interessate possono posticipare la data di inizio attività fino ad un massimo di dieci giorni lavorativi successivi alla data proposta dal DPO. Il calendario di verifica così concordato, viene confermato dal DPO e comunicato per conoscenza alla Direzione Generale.
Ciascuna sessione programmata e preventivamente comunicata nei termini sopra indicati, prevede una fase di pianificazione propedeutica all'esecuzione delle attività operative, che deve essere documentata attraverso uno specifico "Piano di verifica".
Il "Piano di verifica", così redatto dal DPO, con il supporto delle strutture interessate, deve essere inviato al Responsabile della UOS Privacy e al Titolare del trattamento. Nei casi in cui le verifiche riguardino trattamenti gestiti da fornitori esterni, le attività di pianificazione seguiranno le eventuali indicazioni stabilite contrattualmente ovvero saranno preventivamente condivise con i rispettivi responsabili/sub-responsabili interessati.

6. *Scope* degli audit

Lo *scope* degli audit o "dominio di verifica" individua l'insieme dei processi, dei servizi e delle infrastrutture sui quali il DPO, coadiuvato dal personale afferente alla UOS Privacy e dai Responsabili delle Strutture competenti per materia, ritiene opportuno svolgere le verifiche periodiche di conformità.
I domini di verifica sono individuati prima di redigere il "Programma annuale degli audit".
Ferma restando la piena discrezionalità decisionale del DPO, i criteri generali per la selezione dei domini di verifica possono essere fondati sulle seguenti considerazioni:

- Presenza di asset organizzativi, procedurali e tecnologici riconducibili a trattamenti sottoposti a rischi elevati per i diritti e le libertà degli interessati (es. cartella clinica elettronica, controlli da remoto per dispositivi impiantabili, videosorveglianza intelligente etc.);
- Presenza di asset organizzativi, procedurali e tecnologici riconducibili a nuove tipologie o nuove modalità di trattamento (es. servizi in cloud, telemedicina etc.);
- Presenza di specifici "Piani di sicurezza" che sottintendono l'implementazione di misure logiche, fisiche ed organizzative per la sicurezza dei dati personali e per la tutela dei diritti e delle libertà degli interessati.

7. Comunicazione dei risultati degli audit

Al termine delle attività di verifica, il DPO coadiuvato dal personale afferente alla UOS Privacy e con il supporto di eventuali terzi specializzati in materia, provvede alla stesura della seguente documentazione:

- Rapporto dettagliato di audit, nel quale sono documentati tutti i passi che hanno condotto alle valutazioni finali, inclusa tutta la documentazione delle evidenze raccolte (documentazione, screenshot, file di log, questionari di intervista);
- Rapporto di sintesi direzionale, limitatamente alle verifiche di conformità, nel quale sono riepilogati gli esiti dell'audit (giudizi di conformità) e le azioni correttive proposte, corredate da una scala di criticità utile per l'attribuzione delle priorità di intervento;
- Il Rapporto dettagliato di audit viene inviato, in modalità riservata, ai responsabili delle strutture, avendo cura di ripartire la documentazione secondo criteri di pertinenza e competenza, trasmettendo le liste dei rilievi e delle raccomandazioni esclusivamente ai Responsabili direttamente interessati.
- Il Rapporto di sintesi direzionale viene inviato al Titolare del trattamento (Direttore Generale), al termine del processo di validazione degli esiti di verifica, descritto al paragrafo successivo.

8. Validazione audit

Entro e non oltre cinque giorni lavorativi dalla data di ricezione del rapporto di audit, i Responsabili delle strutture interessate possono rispondere ai rilievi fornendo ulteriore documentazione utile ad una possibile revisione dei giudizi valutativi. Le richieste di revisione devono essere corredate da evidenze (es. documenti, screenshot, file di log) che potrebbero incidere sui giudizi valutativi precedentemente assegnati dai verificatori. Sulla base delle nuove evidenze prodotte, il DPO ha la facoltà di rivedere i giudizi valutativi, comunicando ai Responsabili interessati le eventuali revisioni apportate al rapporto dettagliato di verifica. Il nuovo giudizio è da intendersi definitivo e non suscettibile di ulteriori revisioni.

In caso di mancato accoglimento da parte del DPO delle richieste di revisione restano validi i giudizi valutativi precedentemente formulati.
Indipendentemente dall'esito delle richieste di revisione, la nuova documentazione prodotta dalle Strutture interessate è comunque archiviata come allegato al rapporto dettagliato di verifica.

9. Piano di rientro

Entro sessanta giorni lavorativi decorrenti dalla data di ricezione del rapporto di audit, ogni Responsabile di struttura aziendale che ha ricevuto rilievi e raccomandazioni è tenuto a redigere un piano di rientro indicante, per ciascuna raccomandazione:

- Le iniziative che saranno poste in essere per ottemperare alla raccomandazione;
- Le date indicative per l'inizio delle attività di rientro;
- Le date indicative per il termine delle attività di rientro.

I piani di rientro, prodotti da ciascun Responsabile e comunicati al DPO o terzo designato, sono da intendersi puramente indicativi e subordinati ad eventuali approvazioni dei budget di spesa, ai contratti in essere e agli iter amministrativi di approvvigionamento. Indipendentemente da tali fattori, il DPO provvede ad inoltrarne copia al Direttore Generale.

10. Monitoraggio e follow-up

Il DPO effettua una costante attività di monitoraggio sui piani di rientro prodotti dalle strutture aziendali a seguito delle verifiche svolte. A tale proposito, i Responsabili informano periodicamente il DPO sull'andamento dell'iter di approvazione dei piani di rientro e in caso di approvazione, ne comunicano le date di inizio e fine lavori.
Le verifiche di *follow-up* sono finalizzate a constatare l'effettivo rientro da raccomandazioni pregresse. A tale scopo il DPO ha la facoltà di inserire nel programma annuale una o più sessioni di verifiche circostanziate riconducibili a raccomandazioni precedentemente formulate.

11. Archiviazione documentale

I report degli audit, il report di sintesi direzionale e tutti gli allegati a corredo sono archiviati, in formato elettronico pdf non modificabile, a cura del DPO o terzo designato che ne è responsabile della custodia per un arco temporale non inferiore a 10 anni.
La documentazione deve essere archiviata in maniera tale da essere sempre accessibile agevolmente, e sulla base almeno di uno o più dei seguenti criteri di selezione:

- Unità Operativa interessata;
- Tipologia delle verifiche (es. *Vulnerability Assessment, audit di compliance normativa*);
- Data di riferimento delle verifiche (giorno/mese/anno).

Qualora non sia disponibile un sistema documentale informatizzato, i documenti possono essere archiviati in cartelle e sottocartelle gerarchicamente strutturate, con idoneo sistema di autenticazione, autorizzazione e tracciabilità.

12. Conduzione audit

Gli audit hanno lo scopo di rilevare il grado di conformità dei trattamenti di dati ai requisiti imposti dalla vigente disciplina in materia di protezione dei dati personali ed alle prescrizioni impartite dal Titolare. A tale proposito le attività di verifica devono essere riconducibili a fonti autoritative documentali ben identificate, che a loro volta alimentano specifiche liste di controllo (*check list*), attraverso le quali il verificatore conduce le attività di riscontro sul campo e formula i giudizi valutativi di conformità.
Su disposizione del Titolare, questa tipologia di verifiche si applica obbligatoriamente ai trattamenti che utilizzano informazioni direttamente o indirettamente riconducibili allo stato di salute degli assistiti (dati sanitari, dati genetici).

13. Liste di controllo

Le liste di controllo costituiscono lo strumento guida per la conduzione delle verifiche di conformità e devono pertanto essere strutturate in maniera tale che sia evidente la relazione gerarchica tra la fonte di riferimento (es. requisito di legge) e tutti gli altri elementi (attributi) che la compongono.
La parte dedicata ai questionari di intervista deve essere rappresenta in forma tabellare e contenere i seguenti campi:

- Codice Identificativo del requisito di riferimento, che identifica univocamente il campo successivo;
- Requisito, che descrive in forma discorsiva, chiara ed esauriente, il requisito da cui scaturiscono le analisi di conformità;
- Codice identificativo del controllo, che identifica in maniera univoca il campo successivo;
- Controllo, che descrive in maniera dettagliata le attività necessarie a rilevare le evidenze comprovanti il soddisfacimento del requisito;
- Osservazione, che descrive in maniera dettagliata gli elementi comprovanti il soddisfacimento del controllo;

- Giudizio di conformità, che descrive il grado di soddisfacimento del controllo, basato sulle osservazioni precedenti:
- Raccomandazione, che descrive in maniera sintetica le eventuali azioni correttive/migliorative per il completo soddisfacimento del controllo (campo da compilarsi solo nel caso in cui siano stati attribuito un giudizio di non conformità o parziale conformità;
- Nominativo del referente: che indica il nominativo della persona che ha fornito le informazioni utili per formulare l'osservazione ed il giudizio di conformità;
- Lista delle evidenze: che contiene la lista di eventuali documenti utili alla formulazione dell'osservazione e del giudizio di conformità;
- Suggerimenti migliorativi: che indica eventuali proposte formulate dal verificatore per migliorare il grado di adempienza ai controlli risultati comunque conformi;
- Note: nel quale sono indicate eventuali considerazioni a corredo di quanto rilevato da verificatore o dichiarato dal referente intervistato.

Le sessioni di verifica che prevedono l'impiego di liste di controllo, possono essere condotte dal verificatore sia attraverso interviste colloquiali con i referenti individuati delle strutture interessate, sia mediante autovalutazione da parte dei medesimi referenti di struttura.
Nel primo caso il valutatore formula le domande necessarie alla valutazione di conformità, annotando nella lista di controllo le risposte fornite al valutatore. Nel caso di autovalutazione il valutatore provvede a distribuire a ciascun referente interessato solo le parti della lista di controllo da compilare, costituite da tabelle contenenti i seguenti campi:

- Codice identificativo del controllo;
- Controllo;
- Osservazione;
- Nominativo del referente;
- Lista delle evidenze;
- Note.

Qualora il controllo sia strutturato in maniera tale da consentire risposte chiuse di tipo booleano (es. si/no; vero/falso) o risposte chiuse a scelta multipla, il campo "Osservazione" dovrà essere sostituito da uno o più campi opportunamente strutturati per accogliere le due tipologie di risposta.
Le risposte ai questionari di autovalutazione devono essere restituite al valutatore nei modi e nei termini prestabiliti nel "Piano di verifica".

14. Giudizi di conformità

A fronte delle risposte e delle evidenze raccolte, sia tramite intervista che tramite autocertificazione, il valutatore attribuisce i giudizi di conformità utilizzando la seguente nomenclatura standard:

- **Conforme**: giudizio che attesta il pieno soddisfacimento del controllo;
- **Parzialmente Conforme**: giudizio che evidenzia un soddisfacimento del controllo incompleto, integrato dal giudizio di parzialità;
- **Non Conforme**: giudizio che evidenzia la completa assenza di elementi comprovanti il soddisfacimento del controllo;
- **Non Applicabile**: giudizio che evidenzia la non applicabilità del controllo al contesto in esame.

In seguito all'attribuzione di un giudizio di conformità parziale, il valutatore ha la facoltà di aggiungere un ulteriore attributo complementare, denominato "stato di parzialità", che contribuisce a definire la natura delle carenze che motivano tale giudizio.
Lo stato di parzialità, qualora presente, può assumere i seguenti valori:

- "**Incompleto**" che sottintende una parzialità derivante da fattori quantitativi;
- "**Non pertinente**" che sottintende una parzialità derivante da fattori qualitativi;
- "**Inadeguato**" che sottintende una parzialità derivante sia da fattori quantitativi che qualitativi.

Qualora il giudizio di conformità indichi valori non soddisfacenti (es. "Non conforme" o "Parzialmente conforme"), il valutatore deve formulare una specifica raccomandazione, indicando puntualmente gli elementi correttivi/integrativi necessari al conseguimento della piena Conformità.
Qualunque sia il giudizio di conformità attribuito, il valutatore ha la facoltà di indicare eventuali suggerimenti migliorativi, utili ad accrescere qualitativamente il soddisfacimento del controllo.
Qualora il controllo risulti "Non conforme" o "Parzialmente conforme", i suggerimenti migliorativi non sostituiscono quanto formulato nella raccomandazione, il cui soddisfacimento costituisce la condizione minima necessaria per il conseguimento della conformità.

15. Report audit finali

Il "Rapporto di verifica di conformità" costituisce il documento formale con il quale il DPO comunica ai soggetti designati interni, gli esiti della verifica.
Il "Rapporto di sintesi direzionale" è un documento formale, redatto dal DPO e destinato al Titolare del trattamento, nel quale sono riepilogati i risultati della verifica, integrati da ulteriori considerazioni

analitiche, utili a rappresentare lo stato di conformità conseguito e le criticità dei controlli che hanno portato a valutazioni di non conformità o parziale conformità.
A tale scopo il DPO attribuisce a ciascun rilievo un "indice di criticità" espresso mediante la seguente scala valutativa ordinale:

- **Criticità elevata**: giudizio attribuito alle non conformità o parziali conformità derivanti da inadempienze a requisiti cogenti sanzionabili a norma di legge;
- **Criticità media**: giudizio attribuito alle non conformità o parziali conformità derivanti da inadempienze alle disposizioni del Titolare (es. Politiche, Linee guida, procedure operative, clausole contrattuali) che possono essere sanzionabili nei casi in cui si verifichino violazioni della privacy imputabili a tali inadempienze;
- **Criticità bassa**: giudizio attribuito alle non conformità o parziali conformità derivanti da inadempienze che non comportano sanzioni ma solo possibili osservazioni/suggerimenti migliorativi da parte dell'Autorità Garante per la protezione dei dati.

I giudizi di criticità formulati dal DPO, costituiscono un elemento oggettivo di supporto decisionale, in base al quale il Titolare autorizza le attività correttive formulate nei Piani di rientro.

16. Test di efficacia delle misure di sicurezza

Le verifiche di adeguatezza, secondo quanto disposto dal Titolare nella presente procedura, sono finalizzate a testare il grado di efficacia, efficienza e robustezza delle misure di sicurezza applicabili ai servizi automatizzati, ai sistemi informatici ed alle infrastrutture ICT che supportano i trattamenti di dati personali, con particolare riferimento ai dati personali riconducibili allo stato di salute degli assistiti (dati sanitari).
Ai fini di una corretta e univoca interpretazione semantica dei termini utilizzati nel presente documento, si assume che:

- con il termine "**efficacia**" s'intende la capacità di una contromisura di sicurezza di contrastare o contenere il rischio, entro soglie accettabili;
- con il termine "**efficienza**" s'intende la capacità di una contromisura di sicurezza nel garantire tempi di reattività idonei a contrastare/contenere il rischio, con un dispendio di risorse ottimale;
- con il termine "**robustezza**" s'intende la capacità di una contromisura di sicurezza nel resistere ad attacchi intenzionali o involontari, che possano attenuarne il grado di efficacia e di efficienza.

Sulla base di tali assunzioni si stabilisce che:

- le verifiche di efficacia ed efficienza sono condotte mediante attività di "*ethical hacking*" dette "*Penetration Test*", condotte da personale tecnico specializzato con lo scopo di rilevare la possibilità di eludere o neutralizzare le misure di sicurezza informatica preposte a tutela della privacy (Riservatezza, Integrità e Disponibilità dei dati personali);
- le verifiche di robustezza sono condotte mediante sessioni analitiche dette "*Vulnerability Assessment*", svolte esclusivamente con l'ausilio di strumenti automatici dedicati al rilevamento delle vulnerabilità di sicurezza riconducibili ad una errata configurazione o ad una mancata installazione delle patch fornite dal produttore.
- le verifiche di robustezza effettuate mediante sessioni di *Vulnerability Assessment*, basate esclusivamente su scansioni automatizzate effettuate sui sistemi target, devono essere programmate con l'obiettivo di verificare, entro un arco temporale di 12 mesi, perlomeno tutti i sistemi/apparati ICT che supportano il trattamento dei dati sanitari relativi agli assistiti.
- le verifiche di adeguatezza effettuate mediante attività di *Penetration Test* dovrebbero preferibilmente riguardare sistemi/infrastrutture ICT già sottoposti a *Vulnerability Assessment*, a seguito dei quali sono già state implementate le azioni di rientro dalle vulnerabilità rilevate. Il Titolare del trattamento deve prevedere almeno una sessione di *Penetretion Test* nell'arco di dodici mesi.

Nel caso di attività di *ethical hacking*, riconducibili a sessioni di *Penetration Test*, il Titolare del trattamento deve autorizzare nominalmente e per iscritto ciascun verificatore, allegando nella lettera di incarico anche eventuali vincoli e limitazioni nell'esecuzione dei test.
Nei casi in cui le verifiche riguardino trattamenti gestiti da fornitori esterni, le attività di pianificazione seguiranno le eventuali indicazioni stabilite contrattualmente ovvero saranno preventivamente condivise con i rispettivi Responsabili/sub-responsabili interessati.

17. Penetration test

Il successo dei *Penetration Test*, in termini di affidabilità dei risultati ottenuti, è strettamente correlato alle effettive capacità dei verificatori, che devono quindi possedere specifiche competenze tecniche nella conduzione di queste tipologie di attività. Per tale motivo questa tipologia di test può essere affidata a personale esterno, previa verifica dei curricula e degli attestati (es. certificazioni internazionali) posseduti da ciascun soggetto del gruppo di verifica.
È buona prassi dichiarare gli obiettivi dei test che saranno effettuati sui sistemi target preventivamente individuati come ad esempio:

- Test inferenziali volti ad acquisire privilegi di amministratore che attestino la possibilità di modificare i parametri di configurazione del software di base e/o dei DBMS e/o di accedere ai dati personali;
- Test inferenziali volti a dimostrare la possibilità di rilasciare ed eseguire comandi o programmi malevoli in grado di compromettere la sicurezza dei sistemi target e dei dati personali trattati;
- Test inferenziali in grado di dimostrare la possibilità di analizzare il traffico di rete per rilevare informazioni riservate (es. password personali, dati personali).

Nell'esecuzione dei test inferenziali la selezione degli strumenti e delle tecniche di attacco è lasciata alla discrezionalità del verificatore, nel rispetto dei vincoli e dei limiti impartiti nella lettera di autorizzazione rilasciata dal Titolare del trattamento.
Le attività di esecuzione dei test devono essere supervisionate direttamente dal DPO affinché non vengano violati i vincoli e le limitazioni impartite dal Titolare (es. divieto di utilizzo di software malevolo non verificato, divieto di esecuzione di attacchi invasivi in grado di causare disservizi, divieto di accesso ai dati personali ecc.). Tutte le attività svolte dai verificatori sui sistemi target devono essere tracciate ed allegate alla documentazione rilasciata al termine della sessione di verifica.

Il "Rapporto di verifica di robustezza" costituisce il documento formale con il quale il DPO o terzo designato comunica ai soggetti interessati gli esiti della verifica, fornendo le informazioni dettagliate necessarie a:

- conoscere la tipologia, la natura e la severità delle vulnerabilità rilevate;
- consentire alle strutture interessate di predisporre i piani di rientro per l'eliminazione delle vulnerabilità rilevate.

A tale scopo il documento deve riportare le seguenti informazioni:

- Finalità e obiettivi della verifica, così come dichiarati nel "Piano di verifica";
- Strumento utilizzato per l'esecuzione delle scansioni;
- *Vulnerability report*, nel formato di origine generato dal tool di scansione;
- Tabella riepilogativa delle vulnerabilità rilevate, contenete per ciascuna di esse:
  - una codifica/descrizione comprensibile, tale che sia riconoscibile la sua natura o tipologia;
  - l'ambito entro il quale è stata rilevata;
  - un giudizio di severità in termini di incidenza sul rischio di compromissione della sicurezza del sistema target;

- le azioni correttive necessarie ad eliminarla.

Qualora le verifiche abbiano interessato centri di responsabilità differenti, dovranno essere prodotti altrettanti report di verifica, ognuno recante solo le informazioni riconducibili al rispettivo centro di responsabilità.

18. Vulnerability assessment

I test di verifica di robustezza effettuati in maniera automatizzata devono essere condotti con strumenti preventivamente approvati dal Responsabile dei Sistemi informativi o suo delegato sentito il DPO. Tali strumenti, che possono anche essere di tipo "*open source*", devono fornire ampie garanzie di affidabilità, in termini di:

- adeguatezza del *tool* di scansione nell'analizzare e rilevare le vulnerabilità dei sistemi target, tenendo conto delle loro peculiarità hardware e software;
- aggiornamento, delle basi di conoscenza che guidano le scansioni automatizzate;
- completezza dei test effettuati durante le scansioni, che devono essere in grado di rilevare sia vulnerabilità derivanti da errate configurazioni, sia vulnerabilità derivanti dalla mancata installazione degli aggiornamenti (patch) distribuiti dal produttore;
- esaustività dei report prodotti in maniera automatica che devono documentare, per ogni vulnerabilità rilevata, come minimo:

  - una codifica/descrizione comprensibile, tale che sia riconoscibile la sua natura o tipologia;
  - l'ambito entro il quale è stata rilevata;
  - la severità in termini di incidenza sul rischio di compromissione della sicurezza del sistema target;
  - le azioni correttive necessarie ad eliminarla.

In nessun caso sono ammesse azioni automatiche, volte ad eleminare la vulnerabilità a "*run time*", durante l'esecuzione del tool di scansione. I tool utilizzati per l'esecuzione delle verifiche automatiche devono essere opportunamente configurati in maniera tale che non vengano effettuati test soggetti a vincoli/limitazioni preventivamente stabilite dal Titolare (es. ricerca di password banali, test che prevedono un consumo elevato di risorse tali da compromettere l'efficienza del servizio).

Il "Rapporto di verifica di adeguatezza" costituisce il documento formale con il quale il DPO, comunica agli stakeholder gli esiti delle attività di *Penetration Test*, fornendo le informazioni dettagliate necessarie a:

- conoscere le circostanze, le tecniche e le modalità che hanno consentito di violare/aggirare le misure di sicurezza;
- individuare i fattori che hanno causato la perdita di efficacia e/o efficienza delle contromisure logiche preposte alla sicurezza dei dati personali trattati dai sistemi target;
- conoscere le eventuali azioni correttive/migliorative che possano ricondurre il grado di efficacia/efficienza delle misure di sicurezza entro i parametri qualitativi attesi.

A tale scopo il documento deve riportare le seguenti informazioni:

- finalità e obiettivi della verifica, così come dichiarati nel "Piano di verifica";
- tecniche di attacco e strumenti utilizzati (es. *host spoofing, SQL injection, packet sniffer, key logger*);
- conseguenze degli attacchi o delle simulazioni di attacco portati a termine (es. acquisizione dei privilegi di amministratore, accessi non autorizzati; interruzione di servizio ecc.);
- giudizio di severità delle vulnerabilità rilevate;
- suggerimenti sulle possibili azioni correttive/migliorative.

La documentazione così strutturata deve essere inviata ai Responsabili delle Strutture interessate, affinché vengano predisposti adeguati piani di rientro per l'eliminazione delle vulnerabilità rilevate. Data la loro particolare criticità, i rapporti di verifica di adeguatezza sono da considerarsi riservati ed accessibili, salvo deroghe, ai seguenti soggetti:

- Titolare del trattamento, qualora ritenga opportuno visionare questo report tecnico di dettaglio;
- Responsabile delle UOS Privacy e personale di supporto da questi incaricato;
- Responsabile dei Sistemi informativi aziendali o suo delegato.

19. Piano audit straordinario

Il Titolare del trattamento ha la facoltà di incaricare il DPO o il Responsabile della UOS Privacy dell'esecuzione di verifiche non previste nel Calendario annuale, a seguito del verificarsi di una o più delle seguenti circostanze contingenti:

- constatazione di violazioni privacy "*data breach*" soggette a comunicazione obbligatoria all'Autorità Garante per la protezione dei dati;
- rilievi formulati dall'Autorità Garante per la protezione dei dati a seguito di verifiche ispettive.

Le attività commissionate potranno riguardare sia l'esecuzione di verifiche di conformità sia l'esecuzione di verifiche di adeguatezza, che dovranno svolgersi nei modi e nei termini definiti nel presente documento.

20. Allegato

Modello esemplificativo Programma e Piano degli Audit per la conformità dei trattamenti dei dati personali al Regolamento UE 2016/679.

Programma e Piano degli Audit di conformità al Regolamento UE 2016/679

(Modello a titolo esemplificativo)

PROGRAMMA DEGLI AUDIT IN MATERIA DI PROTEZIONE DEI DATI PERSONALI: TRATTAMENTI DATI XXXXX	
Committente	*Titolare o Responsabile*
Scopo dell'Audit	Verifica della conformità dei trattamenti di dati personali al Reg. UE 2016/679
Responsabile del programma di Audit	*DPO o Responsabile UOS Privacy o soggetto designato dal Titolare del trattamento*
Obiettivi dell'Audit	**Valutazione della conformità normativa Privacy (Reg. UE 2016/679).** - valutazione elementi di accountability (regolamenti, nomine, registro delle attività di trattamento, etc.) - valutazione misure adeguate (log, profilazione, etc.) - valutazione dei rischi per l'organizzazione e gli utenti - valutazione del processo e delle responsabilità - identificazione di aree di potenziale miglioramento del sistema di gestione e le azioni e i mezzi necessari perprevenire il verificarsi di non conformità - valutazione dell'efficacia delle azioni correttive/preventive intraprese (feedback di controllo in audit successivi)

Livello di approfondimento	**Ambito di pertinenza** - completezza di applicazione (tutti i requisiti richiesti dal sistema informativo aziendale) - estensione del modello (declinazione dei requisiti in tutti gli aspetti organizzativi pertinenti) - documentazione e comprensione degli addetti (esplicitazione delle modalità gestionali e operative inerenti gli aspettiapplicativi dei requisiti richiesti dal modello) - sistematicità e diffusione (applicazione sistematica di quanto stabilito, laddove stabilito) - verifica gruppo di lavoro per sviluppo e servizio In particolare, il livello di approfondimento dovrà permettere di: - controllare che il sistema di trattamento sia conforme alle norme di riferimento del GDPR - controllare che il sistema informativo sia correttamente e completamente messo in atto, conformemente a quanto stabilito dai documenti di riferimento (manuale, procedure gestionali, procedure operative, ecc.) sempre nell'ottica degli adempimenti privacy;

PIANO DI AUDIT: TRATTAMENTI DATI	
Criteri per lo svolgimento dell'Audit	- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Applicazione delle misure di sicurezza tecniche ed organizzative previste dal Regolamento aziendale di attuazione del GDPR
Oggetto dell'Audit	Rispetto dei principi del Privacy by Design e Privacy by Default delle funzionalità sviluppate all'interno del sistema informativo in uso considerando: - Processo di sviluppo e di manutenzione del sistema informativo - Processo di trattamento dei dati - Processo di assistenza (autenticazione, trattamento, tracciabilità, etc.) - Processo rilascio credenziali e gestione dei profili di accesso
Estensione dell'Audit	Strutture organizzative coinvolte:
Documenti di riferimento	Regolamento (UE) 2016/679 del Parlamento europeo Accordi contrattuali Documenti di progetto: architettura, analisi dei rischi, requisiti, organizzazione del servizio, misure di sicurezza, dati di assistenza, accordi di servizio, etc. Documenti di processo: rilascio credenziali, organizzazione del servizio, piano di gestione del servizio
Calendario attività Data d'inizio e fine dell'audit	Previsione di attuazione dal GG/MM/AAAA al GG/MM/AAAA
Unità Operative interessate	*In riferimento all'Organizzazione*

Composizione dei "Gruppi di Audit"	- Auditor interno - Auditor esterno

PIANO DELL'AUDIT		
Ora e luogo	**Attività**	**Referenti dell'organizzazione di cui è richiesta la presenza**
giorno: *ora:* *sede*:	**Svolgimento della riunione di apertura** - Presentazione del programma di audit - Scopo, obiettivo ed estensione della verifica - Conferma piano di verifica e modalità operative - Individuazione dei referenti di interfaccia - Indicazione nominativa da parte dei Responsabili degli interlocutori ed eventuali accompagnatori per le fasi successive	Tutti
giorno: *ora:* *sede*:	**Verifica sul campo** esame della documentazione, osservazioni sul campo ed incontri con gli operatori per rilevare l'effettiva applicazione e valutazione dei requisiti previsti norma. - Assegnazione compiti e funzioni (nomine formali SATD/SAT/Amministratori di Sistema, Responsabili del trattamento) - Gestione delle credenziali per l'accesso ai sistemi e applicazioni - Misure di sicurezza e Analisi dei rischi sui trattamenti in corso - Procedure per data breach e per garantire l'esercizio dei diritti - Aderenza funzionale requisiti normativi	Governo Account Gruppo di Audit

giorno: *ora:* *sede*:	**Verifica sul campo** esame della documentazione, osservazioni sul campo ed incontri con gli operatori per rilevare l'effettiva applicazione e valutazione dei requisiti previsti norma. - Processo di manutenzione e sviluppo - Misure di sicurezza - Processo di Assistenza - Gestione Fornitori	Governo Sviluppo Assistenza Gruppo di Audit
giorno: *ora:* *sede*:	**Riunione del Gruppo di Verifica** per la stesura del "Rapporto di Verifica"	Gruppo di Audit
giorno: *ora:* *sede*:	**Riunione di chiusura** - presentazione rapporto e verbale di verifica - definizione programma di monitoraggio sugli eventuali piani di miglioramento - discussione	Tutti

ARTICOLAZIONE DELL'AUDIT	
Auditati	- ……. - ……. - ……. - …….