So.Re.Sa.
Procedura per la conduzione delle verifiche di conformità ed adeguatezza delle misure preposte alla tutela dei dati personali

Autore/i:	Francesca Santaniello	EY Advisory S.p.A.
Rivisto Da	Francesco Daniele	EY Advisory S.p.A.
Approvato Da:	Nome e Cognome del Responsabile	Azienda di Riferimento
Accettato Da:	Nome e Cognome del Responsabile	Azienda di Riferimento

Storia del documento

Data	Versione	Descrizione modifiche	Autore
29/10/2020	1.0	Prima emissione	Francesco Daniele

Indice

Indice delle Tabelle

1 INTRODUZIONI GENERALI AL DOCUMENTO

1.2 SCOPO DEL DOCUMENTO

Il presente documento ha lo scopo di definire il processo per l'esecuzione delle attività di verifica attuate dalla Struttura Sanitaria, con lo scopo di valutare il grado di conformità e adeguatezza delle misure logiche, fisiche ed organizzative, preposte alla tutela dei dati personali ed al rispetto dei diritti degli interessati.

Le verifiche di adeguatezza e conformità costituiscono la fonte primaria che alimenta un processo di controllo sistematico e continuativo, attraverso il quale il Titolare dispone degli elementi decisionali utili all'attuazione delle azioni correttive/migliorative del sistema di gestione della privacy.

1.3 CAMPO DI APPLICAZIONE

Gli indirizzamenti definiti nel presente documento si applicano a tutte le UU.OO. della Struttura Sanitaria e sono da ritenersi estese anche ai fornitori o subfornitori esterni per i quali siano stati indicati i responsabili e gli eventuali sub-responsabili del trattamento di dati personali, nei modi e nei termini definiti nell'art. 28 del GDPR.

1.4 RIFERIMENTI

Interni

- Linee Guida per la conduzione delle verifiche di conformità ed adeguatezza delle misure preposte alla tutela dei dati personali

Esterni

- Regolamento UE 679/2016 (GDPR);
- Comitato europeo per la protezione dei dati (EDPB);
- D.Lgs 101/2018;
- Garante nazionale per la protezione dei dati personali.

1.5 DEFINIZIONI

Di seguito sono riportate le definizioni utilizzate nel documento:

Termine	Descrizione
Responsabile di Servizio	Colui che, in qualità di responsabile del soggetto esterno autorizzato / dipendente della Struttura Sanitaria, può richiedere la creazione dell'utenza a cui potranno corrispondere diversi privilegi in base alle esigenze lavorative. Allo stesso modo, il Responsabile di Servizio potrà richiedere la modifica dei privilegi o la disabilitazione dell'utenza.
DPO	Data Protection Officer

Termine	Descrizione
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
GDPR	Regolamento Generale per la Protezione dei Dati.

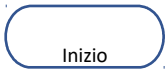
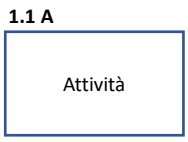
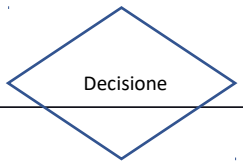
Tabella 1 – Definizioni

1.6 SIMBOLOGIA UTILIZZATA

Al fine di descrivere il processo, sono descritte le suddette attività tramite:

- una rappresentazione grafica dei flussi (flow-chart) che compongono il processo;
- una matrice che descrive analiticamente tale rappresentazione.

Di seguito sono illustrati i simboli utilizzati nel flowchart, con una breve descrizione degli stessi:

Simbolo	Denominazione	Descrizione
	Inizio	Rappresenta l'inizio del processo.
	Attività	Rappresenta l'operazione attuata, collocata all'interno del processo tramite: • il numero della fase di riferimento (1.1) • la lettera identificativa dell'attività (A)
	Decisione	Rappresenta un momento decisionale.
	Linee di flusso	Connette le attività fra di loro indicando il flusso delle informazioni.

Simbolo	Denominazione	Descrizione
	Fine	Rappresenta la conclusione del processo.

Tabella 2 – Legenda

Di seguito viene riportata un esempio di tabella che descrive analiticamente la rappresentazione dei flowchart:

ID	Attività	Descrizione	Responsabile
1.1 A	Attività 1	Descrizione dell'attività 1 che viene effettuata dal corrispondente responsabile	Responsabile 1
1.1 B	Attività 2	Descrizione dell'attività 2 che viene effettuata dal corrispondente responsabile	Responsabile 2
1.1 C	…		…
1.2 C	…		…

2 CONDUZIONE DELLE VERIFICHE

2.1 ATTIVITÀ DI VERIFICA

Il processo da seguire per la conduzione delle verifiche di adeguatezza e conformità del sistema di gestione della privacy si articola con diverse fasi e rientrano nell'ambito delle competenze istituzionali conferite al DPO.

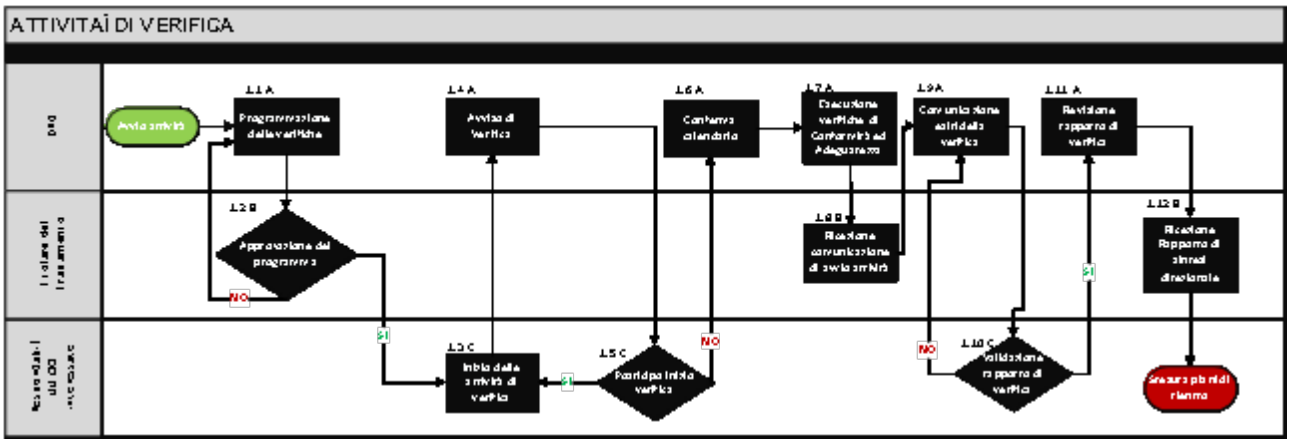
Le fasi possono essere racchiuse come di seguito:

- Programmazione delle verifiche
- Approvazione del programma
- Inizio delle attività di verifica
- Avviso di Verifica
- Posticipo inizio verifica
- Conferma calendario
- Ricezione comunicazione di avvio attività
- Comunicazione esiti della verifica
- Validazione rapporto di verifica
- Revisione rapporto di verifica
- Ricezione Rapporto di sintesi direzionale
- Stesura piani di rientro

Nei successivi paragrafi verranno descritte, nel dettaglio, le fasi suddette ed i principali deliverables prodotti nelle suddette fasi.

2.2.1 WORKFLOW DELLE ATTIVITÀ DI VERIFICA

Di seguito saranno descritte, in forma di flow chart, le fasi seguite nell'ambito della conduzione delle verifiche:



2.2.2 MATRICE DELLE ATTIVITÀ DI VERIFICA

ID	Attività	Descrizione	Responsabilità
1.1.A	Programmazione delle verifiche	Entro la fine di ogni anno solare, il DPO redige il "Programma annuale delle verifiche privacy" 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, come minimo le seguenti informazioni: • Scopo della verifica; • UU.OO. interessate; • Tipologia di verifica (es. Vulnerability assessment, Compliance Audit); • Data presunta di inizio verifica	DPO
1.2.B	Approvazione del programma	Il programma nella sua versione definitiva deve essere sottoposto all'approvazione del Titolare.	Titolare del trattamento
1.3.C	Inizio delle attività di verifica	L'inizio delle attività di verifica deve essere concordato con i responsabili delle UU.OO. interessate, per consentire loro di predisporre tutte le risorse necessarie a supportare le attività dei verificatori.	Responsabili UU.OO. interessate
1.4.A	Avviso di Verifica	Il DPO invia una comunicazione formale (avviso di verifica) tramite la posta elettronica interna. La comunicazione inviata ai Responsabili delle	DPO

		UU.OO. interessati, deve contenente come 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.	
1.5.C	Posticipo inizio verifica	I responsabili delle UU.OO. interessate possono posticipare la data di inizio attività fino ad un massimo di dieci giorni lavorativi successivi alla data proposta dal DPO.	Responsabili UU.OO. interessate
1.6.A	Conferma calendario	Il calendario di verifica così concordato, viene confermato dal DPO.	DPO
1.7.A	Esecuzione verifiche di Conformità ed Adeguatezza	Per le attività di verifica di Conformità ed Adeguatezza si rimanda ai paragrafi 3 e 4.	DPO
1.8.B	Ricezione comunicazione di avvio attività	Il calendario di verifica viene comunicato per conoscenza al Titolare del trattamento.	Titolare del trattamento
1.9.A	Comunicazione esiti della verifica	Al termine delle attività di verifica il DPO o il personale da questi incaricato, provvede alla stesura della seguente documentazione: • Rapporto dettagliato di verifica, 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 della verifica (giudizi di conformità) e le azioni correttive proposte, corredate da una scala di criticità utile per l'attribuzione delle priorità di intervento.	DPO
1.10.C	Validazione rapporto di verifica	Entro e non oltre cinque giorni lavorativi dalla data di ricezione del rapporto dettagliato di	Responsabili UU.OO. interessate

		verifica, i Responsabili delle UU.OO. interessate possono rispondere ai rilievi fornendo ulteriore documentazione utile ad una possibile revisione dei giudizi valutativi.	
1.11.A	Revisione rapporto di verifica	Sulla base delle nuove evidenze prodotte, il DPO ha la facoltà di rivedere i giudizi valutativi, comunicando ai Responsabili UU.OO. interessati le eventuali revisioni apportate nel rapporto dettagliato di verifica. Il nuovo giudizio, formulato dal DPO, è da intendersi definitivo e non suscettibile di ulteriori revisioni. In assenza di comunicazioni da parte del DPO, le richieste di revisione sono da intendersi non accolte, restando validi i giudizi valutativi precedentemente formulati. Indipendentemente dall'esito delle richieste di revisione, la nuova documentazione prodotta dalle UU.OO. interessate è comunque archiviata come allegato al rapporto dettagliato di verifica.	DPO
1.12.B	Ricezione Rapporto di sintesi direzionale	Il Rapporto di sintesi direzionale viene inviato al Titolare del trattamento, al termine del processo di validazione degli esiti di verifica.	Titolare del trattamento

2.2.3 DELIVERABLE: PIANI DI RIENTRO

Entro quarantacinque giorni lavorativi a partire dalla data di ricezione del rapporto dettagliato di verifica, ogni Responsabile delle UU.OO. che ha ricevuto rilievi e raccomandazioni è tenuto a redigere un piano di rientro indicante, per ciascuna raccomandazione:

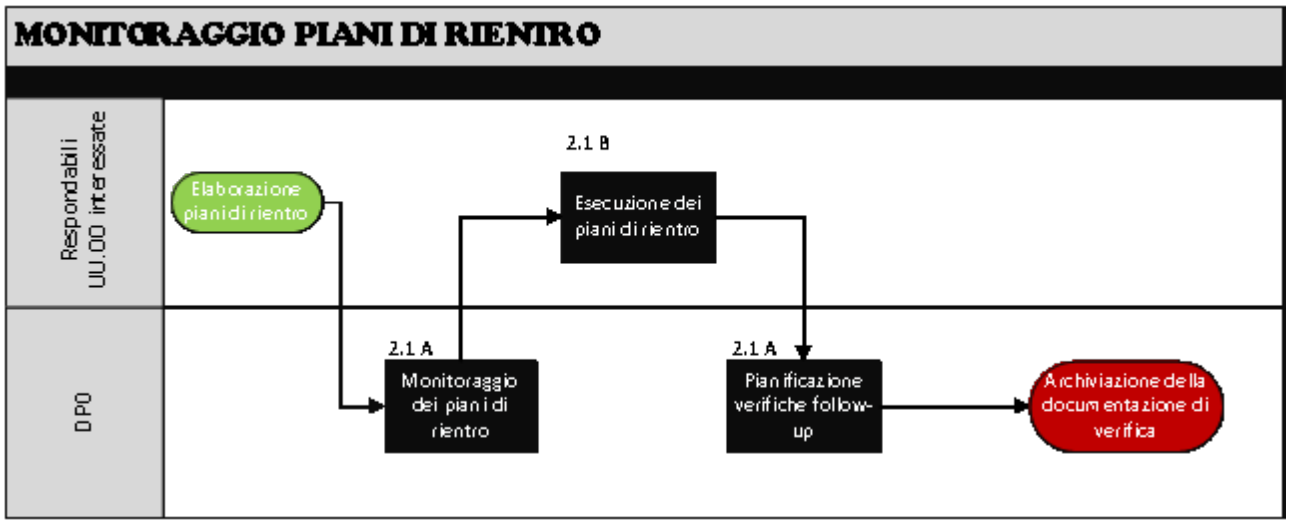
- Le iniziative che saranno poste in essere per ottemperare alla raccomandazione;
- Le date indicative per l'inizio delle attività di rientro;
- Le date indicative per il termine delle attività di rientro.

I piani di rientro, prodotti da ciascuna UU.OO. interessata e comunicati al DPO, sono da intendersi puramente indicativi e subordinati alle 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 Titolare.

2.3 MONITORAGGIO DEI PIANI DI RIENTRO

Il DPO effettua una costante attività di monitoraggio sui piani di rientro prodotti dalle UU.OO. a seguito delle verifiche svolte ed esegue periodicamente verifiche di follow-up finalizzate a constatare l'effettivo rientro da raccomandazioni pregresse.

2.3.1 WORKFLOW PER IL MONITORAGGIO DEI PIANI DI RIENTRO



1.2.1 MATRICE PER IL MONITORAGGIO DEI PIANI DI RIENTRO

ID	Attività	Descrizione	Responsabilità
2.1.A	Monitoraggio dei piani di rientro	Il DPO effettua una costante attività di monitoraggio sui piani di rientro prodotti dalle UU.OO. a seguito delle verifiche svolte.	DPO
2.1.B	Esecuzione dei piani di rientro	I Responsabili delle UU.OO. interessate informano periodicamente il DPO sull'andamento dell'iter di approvazione dei progetti di rientro e in caso di approvazione, ne comunicano le date di inizio e fine lavori.	Responsabili UU.OO. interessate
2.1.A	Pianificazione verifiche follow-up	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.	DPO

2.3.2 ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI VERIFICA

I report dettagliati di verifica, il report di sintesi direzionale e tutti gli allegati a corredo sono archiviati, in formato elettronico pdf non modificabile, a cura del DPO che ne è responsabile della custodia per un arco temporale non inferiore a trentasei mesi.
La documentazione deve essere archiviata in maniera tale che sia sempre possibile accedervi agevolmente, come minimo sulla base di uno o più dei seguenti criteri di selezione:

- Unità Operativa interessata;

- Tipologia delle verifiche (es. Vulnerability assessment, GDPR Compliance);
- 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 MS-Windows gerarchicamente strutturate.

Ad integrazione dei flussi descritti precedentemente, nei paragrafi successivi sono descritte le attività che regolamentano:

- Verifiche di conformità
- Verifiche di adeguatezza
- Verifiche straordinarie

3 VERIFICHE DI CONFORMITÀ

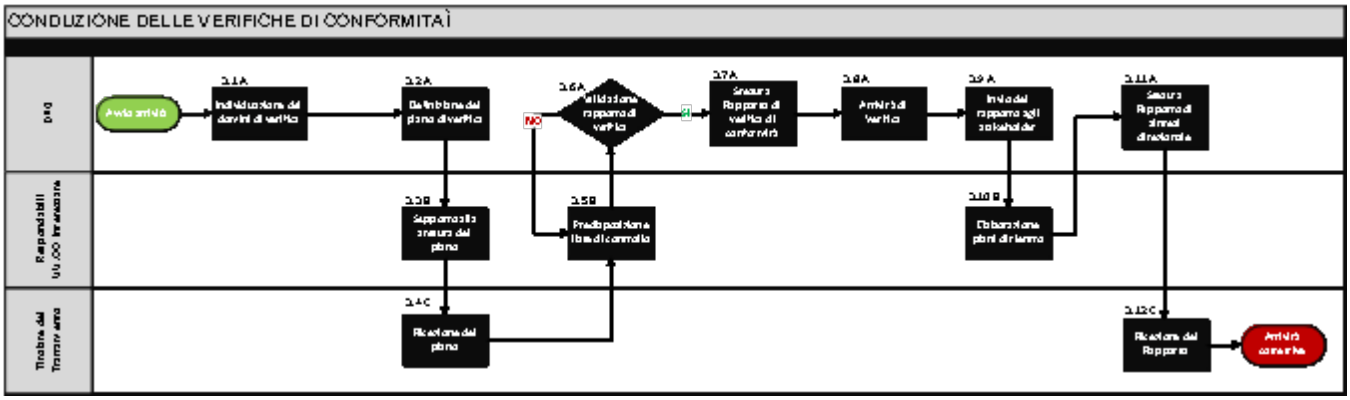
Le verifiche di conformità hanno lo scopo di rilevare il grado di adempienza ai requisiti indirizzati dalle normative di legge in materia di privacy ed alle prescrizioni impartite dal Titolare.

3.2 ATTIVITÀ DI VERIFICHE DI CONFORMITÀ

Il processo da seguire per la conduzione delle verifiche di conformità del sistema di gestione della privacy si articola con diverse fasi che possono essere racchiuse come di seguito:

- Individuazione dei domini di verifica
- Definizione del piano di verifica
- Supporto alla stesura del piano
- Ricezione del piano
- Predisposizione delle liste di controllo
- Validazione del rapporto di verifica
- Stesura del rapporto di verifica di conformità
- Invio del rapporto agli stakeholder
- Elaborazione dei piani di rientro
- Stesura del rapporto di sintesi direzionale
- Ricezione del rapporto

3.2.1 WORKFLOW PER LA CONDUZIONE DELLE VERIFICHE DI CONFORMITÀ



3.2.2 MATRICE PER LA CONDUZIONE DELLE VERIFICHE DI CONFORMITÀ

ID	Attività	Descrizione	Responsabilità
3.1.A	Individuazione dei domini di verifica	Un dominio di verifica o "scope" individua l'insieme dei processi, dei servizi e delle infrastrutture sui quali il DPO ritiene opportuno svolgere le verifiche periodiche di conformità. 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 di violazione delle libertà individuali degli interessati (es. trattamento di dati sanitari); • Presenza di asset organizzativi, procedurali e tecnologici riconducibili a nuove tipologie o nuove modalità di trattamento (es. introduzione di nuovi servizi automatizzati); • 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 degli interessati.	DPO
3.2.A	Definizione del piano di verifica	• Il piano di verifica è propedeutico all'esecuzione delle attività operative, e deve essere documentato attraverso uno specifico "Piano di verifica" nel quale sono dettagliate le seguenti informazioni: • Finalità e obiettivi della verifica (in	DPO

		conformità a quanto definito nel "Programma annuale delle verifiche privacy" nei casi applicabili); • Elenco delle norme di legge e/o delle politiche/procedure operative interne e/o delle clausole contrattuali, utilizzati come riferimento per le verifiche di conformità; • Cronoprogramma generale delle attività di verifica; • Elenco delle Unità Operative interessate; • Indicazione del "Lead auditor", referente interno alla struttura sanitaria nominato dal DPO, incaricato del coordinamento delle attività operative; • Calendario dettagliato delle interviste • Elenco delle check list e degli strumenti utilizzati per il rilevamento delle informazioni necessarie alle valutazioni di conformità.	
3.3.B	Supporto alla stesura del piano	Il "Piano di verifica" è redatto dal DPO con il supporto delle UU.OO interessate.	Responsabili UU.OO. interessate
3.4.C	Ricezione del piano	Il "Piano di verifica" deve essere inviato al Titolare del trattamento.	Titolare del trattamento
3.5.B	Predisposizione 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. • Ogni lista di controllo deve essere corredata da un frontespizio recante perlomeno le seguenti informazioni: • Titolo, che individua la specifica lista di controllo; • Sessione di verifica, che identifica la sessione di verifica nella quale è utilizzata la lista di controllo, utilizzando la medesima nomenclatura definita nel Piano di verifica; • Data di compilazione, che indica la data alla quale è stata compilata la lista di verifica; • Verificatore, che indica il nominativo della	Responsabili UU.OO. interessate

		persona che ha condotto la verifica.	
3.6.A	Validazione rapporto di verifica	Ogni lista di controllo così predisposta, deve essere sottoposta all'approvazione preventiva del DPO, che ne attesta l'idoneità al perseguimento degli scopi della verifica. La mancata approvazione preventiva da parte del DPO preclude l'impiego della lista di controllo nella sessione di verifica.	DPO
3.7.A	Stesura Rapporto di verifica di conformità	Il "Rapporto di verifica di conformità" costituisce il documento formale con il quale i DPO comunica gli esiti della verifica.	DPO
3.8.A	Attività di Verifica	Le attività di verifica sono contenute nel documento "Linee guida per la conduzione delle verifiche di conformità e adeguatezza delle misure preposte alla tutela dei dati personali" al paragrafo 3.4 *Regole per la compilazione delle liste di controllo.*	DPO
3.9.A	Invio del rapporto agli stakeholder	Il "Rapporto di verifica di conformità viene inviato agli stakeholder.	DPO
3.10.B	Elaborazione piani di rientro	La documentazione così strutturata deve essere inviata al/i Responsabile/i della/e UO affinché vengano predisposti adeguati piani di rientro per il conseguimento della piena conformità.	Responsabili UU.OO. interessate
3.11.A	Stesura Rapporto di sintesi direzionale	Il "Rapporto di sintesi direzionale" è un documento formale, nel quale sono riepilogati i risultati della verifica, integrati da ulteriori considerazioni analitiche, utili a rappresentare lo stato di conformità conseguito e la criticità dei controlli che hanno portato a valutazioni di non conformità o parziale conformità.	DPO
3.12.C	Ricezione dei Rapporti	Il "Piano di verifica" deve essere inviato al Titolare del trattamento, in base al quale autorizza le attività correttive formulate nei piani di rientro.	Titolare del trattamento

3.2.3 DELIVERABLE: I RAPPORTI

Al termine di questa fase vengono prodotti due rapporti di verifica:
Rapporto di verifica di conformità costituisce il documento formale con il quale i DPO comunica agli stakeholder gli esiti della verifica, fornendo le informazioni dettagliate necessarie a:

- Comunicare alle UU.OO. interessate gli esiti della verifica, pubblicando per ciascun controllo, le osservazioni, i giudizi di conformità e le raccomandazioni formulate dal valutatore;

- Consentire alle UU.OO. interessate di formulare un piano di rientro per il conseguimento della piena conformità ai requisiti di legge e/o alle disposizioni del Titolare.
- A tale scopo il documento deve riportare le seguenti informazioni:
  - Finalità e obiettivi della verifica, così come dichiarati nel "Piano di verifica";
  - Elenco delle norme di legge e/o delle politiche/procedure operative interne e/o delle clausole contrattuali, utilizzati come riferimento per le verifiche di conformità, sempre secondo quanto dichiarato nel "Piano di verifica";
  - Check list dei controlli, complete delle relative osservazioni, giudizi di conformità e raccomandazioni formulate dal valutatore;
  - Elenco delle evidenze documentali raccolte in sede di verifica e utilizzate in sede di valutazione.
- 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.

Rapporto di sintesi direzionale è un documento formale nel quale sono riepilogati i risultati della verifica, integrati da ulteriori considerazioni analitiche, utili a rappresentare lo stato di conformità conseguito e la 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 del Garante nazionale.
-

4 VERIFICHE DI ADEGUATEZZA

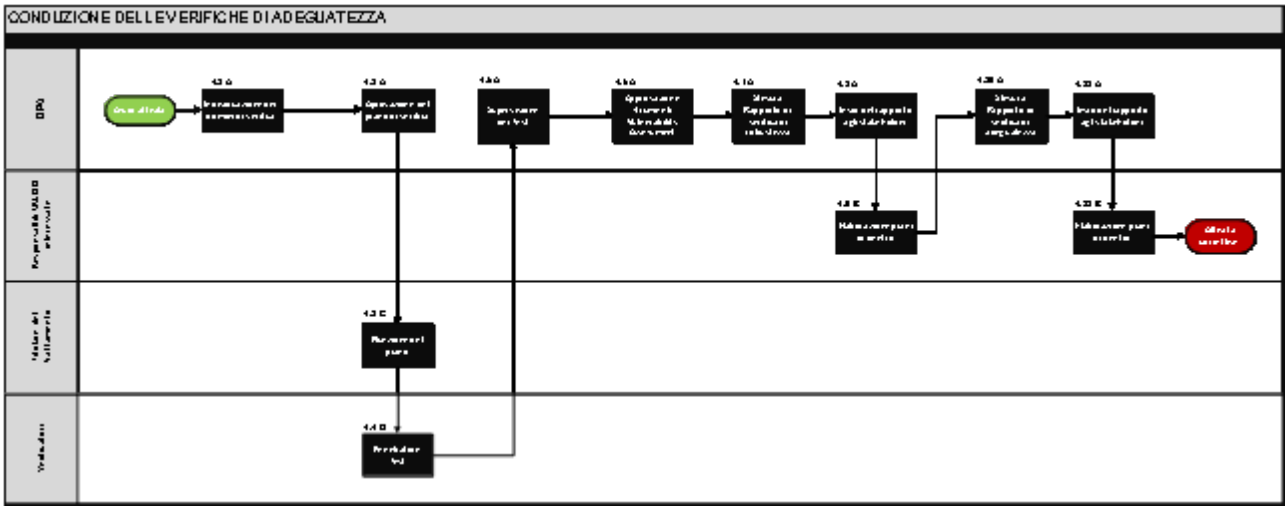
Le verifiche di adeguatezza sono finalizzate a verificare il grado di efficacia, efficienza e robustezza delle misure di sicurezza logica applicabili ai servizi automatizzati, ai sistemi informatici ed alle infrastrutture ICT che supportano i trattamenti di dati personali.

4.2 ATTIVITÀ DI VERIFICHE DI ADEGUATEZZA

Il processo da seguire per la conduzione delle verifiche di adeguatezza del sistema di gestione della privacy si articola con diverse fasi che possono essere racchiuse come di seguito:

- Individuazione dei domini di verifica
- Definizione del piano di verifica
- Esecuzione dei test inferenziali (Penetration Test)
- Esecuzione dei test automatizzati (Vulnerability Assessment)
- Stesura del rapporto di verifica di robustezza
- Stesura del rapporto di verifica di adeguatezza

4.2.1 WORKFLOW PER LA CONDUZIONE DELLE VERIFICHE DI ADEGUATEZZA



1.2.2 MATRICE PER LA CONDUZIONE DELLE VERIFICHE DI CONFORMITÀ

ID	Attività	Descrizione	Responsabilità
4.1.A	Individuazione dei	Un dominio di verifica o "scope" individua gli	DPO

	domini di verifica	apparati di rete ed i sistemi target che devono essere sottoposti alle verifiche di adeguatezza (efficacia, efficienza, robustezza). I criteri generali per la selezione dei domini di verifica si applicano alle infrastrutture tecnologiche trasversali (es. dispositivi di sicurezza delle reti, web server, piattaforme di Identity and Access Management, banche dati) che costituiscono un punto critico per la sicurezza dei trattamenti informatici e telematici di dati personali. I sistemi target attestati sulla intranet devono essere univocamente individuati dall'indirizzo IP privato mentre i sistemi accessibili da Internet, devono essere univocamente identificati dalla URL ovvero dall'indirizzo IP pubblico. 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 DPO deve prevedere come minimo due sessioni di penetretion test nell'arco di dodici mesi.	
4.2.A	Approvazione del piano di verifica	Ciascuna sessione programmata prevede una fase di pianificazione propedeutica all'esecuzione delle attività operative, che deve essere documentata attraverso uno specifico "Piano di verifica" nel quale sono dettagliate le seguenti informazioni: • Finalità e obiettivi della verifica (in conformità a quanto definito nel "Programma annuale delle verifiche privacy" nei casi applicabili); • Sistemi target oggetto di verifica; • Cronoprogramma generale delle attività di verifica;	DPO

		• Elenco delle Unità Operative interessate; • Indicazione del referente interno alla struttura sanitaria, incaricato del coordinamento e controllo delle attività operative; • Data programmata per l'esecuzione dei test; • Data programmata per il termine dei test; • Nominativo dei verificatori (esecutori materiali dei test); • Modalità di esecuzione dei test (Vulnerability Assessment/ Penetration Test).	
4.3.C	Ricezione del piano	Il "Piano di verifica" così redatto deve essere approvato dal DPO che provvede ad inviarne una copia al Titolare del trattamento. Nel caso di attività di ethical hacking, riconducibili a sessioni di Penetration Test, il Titolare 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.	Titolare del trattamento
4.4.D	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 alla struttura sanitaria, previa verifica dei curricula e degli attestati (es. certificazioni internazionali) posseduti da ciascun elemento del gruppo di verifica. È buona prassi dichiarare gli obiettivi dei test che saranno effettuati sui sistemi target preventivamente individuati come ad	Verificatori

		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.	
4.5.A	Supervisione dei test	Le attività di esecuzione dei test devono essere supervisionate da un referente interno della struttura sanitaria, ovvero direttamente dal DPO qualora lo ritenga opportuno, 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.	DPO
4.6.A	Approvazione strumenti Vulnerability Assessment	I test di verifica di robustezza effettuati in maniera automatizzata devono essere condotti con strumenti preventivamente approvati dal 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	DPO

		(es. vulnerability signatures) 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: o Una codifica/descrizione comprensibile, tale che sia riconoscibile la sua natura o tipologia; o L'ambito entro il quale è stata rilevata; o La severità in termini di incidenza sul rischio di compromissione della sicurezza del sistema target; o 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).	
4.7.A	Stesura Rapporto di verifica di robustezza	Il "Rapporto di verifica di robustezza" costituisce il documento formale con il quale i DPO fornisce le informazioni dettagliate necessarie a: • Conoscere la tipologia, la natura e la severità delle vulnerabilità rilevate; • Consentire alle UU.OO. afferenti al comparto ICT di predisporre i piani di rientro per l'eliminazione delle	DPO

		vulnerabilità rilevate.	
4.8.A	Invio del rapporto agli stakeholder	Il "Rapporto di verifica di robustezza" è il documento con il quale i DPO comunica agli stakeholder gli esiti della verifica.	DPO
4.9.B	Elaborazione piani di rientro	La documentazione così strutturata deve essere inviata al/i Responsabile/i della/e UO affinché vengano predisposti adeguati piani di rientro per l'eliminazione delle vulnerabilità rilevate.	Responsabili UU.OO interessate
4.10.A	Stesura Rapporto di verifica di adeguatezza	Il "Rapporto di verifica di adeguatezza" costituisce il documento formale con il quale i DPO comunica 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.	DPO
4.11.A	Invio del rapporto agli stakeholder	Il "Rapporto di verifica di adeguatezza" costituisce il documento con il quale i DPO comunica agli stakeholder gli esiti delle attività di Penetration Test.	DPO
4.12.B	Elaborazione piani di rientro	La documentazione così strutturata deve essere inviata al/i Responsabile/i della/e UO affinché vengano predisposti adeguati piani di rientro per l'eliminazione delle vulnerabilità rilevate.	Responsabili UU.OO interessate

4.2.2 DELIVERABLE: I RAPPORTI DI VERIFICA

Al termine di questa fase vengono prodotti due rapporti di verifica:

Rapporto di verifica di robustezza costituisce il documento formale con il quale i DPO comunica agli stakeholder gli esiti della verifica.

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.

Rapporto di verifica di adeguatezza costituisce il documento formale con il quale i DPO comunica agli stakeholder gli esiti delle attività di Penetration Test.
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.

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.

Data la loro particolare criticità i rapporti di verifica di adeguatezza sono da considerarsi riservati ed accessibili esclusivamente ai seguenti soggetti:

- Titolare del trattamento, qualora ritenga opportuno visionare questo report tecnico di dettaglio;
- DPO e personale di supporto da questi incaricato;
- Responsabili delle UU.OO. afferenti al comparto ICT e personale tecnico di supporto, da questi incaricato.

•

5 VERIFICHE STRAORDINARIE

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

- Constatazione di violazioni della privacy "data breach" soggette a comunicazione obbligatoria al Garante privacy nazionale;
- Rilievi formulati dal Garante privacy 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 nella medesima modalità definita ai capitoli 3 e 4.

6 ALLEGATI

Di seguito inseriamo come allegato le "Linee Guida per la conduzione delle verifiche di conformità ed adeguatezza delle misure preposte alla tutela dei dati personali":