Allegato "2"

POLICY AZIENDALE PER L'ANALISI DEI RISCHI A CUI SONO SOGGETTI I DATI

L'art.32 del Regolamento Europeo 2016/679 Regolamento Generale sulla protezione dei dati e relative norme di armonizzazione (in seguito RGPD) prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento adotti misure tecniche ed organizzative adeguate a garantire un livello di sicurezza commisurato al rischio.
Il RGPD, nel rispetto dei principi che lo ispirano, non indica una metodologia specifica da seguire per effettuare la suddetta analisi, ma , nei considerando 75, 76, 83 ed 85, fornisce alcune indicazioni. Sugli item di rischio e di danno da valutare oggettivamente sia in termini di probabilità che in termini di gravità, con riguardo alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento, per classificare il trattamento dati come comportante un rischio od un rischio elevato.
Parimenti l'Autorità Garante per la Protezione dei Dati personali ha fornito alcune indicazioni, seppur con riferimento alla DPIA (valutazione d'impatto privacy).
Le linee guida dell'ENISA (Agenzia Europea per la sicurezza delle reti e delle informazioni) tradotte in italiano nel dicembre 2017 propongono poi un approccio alla valutazione del rischio, che si basa su quattro fasi:
1. Definizione dell'operazione di trattamento e del suo contesto.
2. Comprensione e valutazione dell'impatto, utilizzando una scala di valori a tre livelli (BASSO,MEDIO,ALTO).
3. Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia) mediante un questionario di 20 domande suddiviso in 4 aree rilevanti, che esita in un risultato graduato su una scala di valori a 3 livelli (BASSO,MEDIO,ALTO).
4. Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto, in una griglia 3x3, che esita in un risultato graduato su una scala di valori a tre livelli (BASSO,MEDIO,ALTO).
Le misure di sicurezza tecnico-organizzativa vengono poi individuate in coerenza con il livello di rischio così definito e tenendo conto delle indicazioni della norma ISO 27001:2013 sulla sicurezza delle informazioni (ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements :http://www.iso.org/iso/catalogue_detail?csnumber=54534).
L'analisi dei rischi è un momento fondamentale di crescita per il sistema privacy aziendale e non un semplice adempimento, pertanto già in fase di avvio ASL 3 ha dato indicazioni per una sua conduzione attraverso gruppi di lavoro interni alle singole strutture-aree aziendali interessate.
In una prima fase è stata preferita l'adozione di un modello semplificato di analisi, che già , peraltro, rispettasse le indicazioni sopra riportate.
Sono perciò state individuare tre aree di rischio e per ognuna alcune tipologie di rischio, lasciando un campo "altro" implementabile dal compilatore e richiesta la valutazione dell'impatto graduata su 3 livelli (BASSO,MEDIO,ALTO).
Per ognuno degli item di rischio è stata richiesta l'individuazione di misure di sicurezza informatica o non informatica coerenti ed una valutazione del grado di incidenza sul rischio individuato e della responsabilità di attuazione.

Nel 2019 l'analisi effettuata è stata sottoposta a verifica e monitoraggio e richiesta la formulazione di eventuali proposte migliorative , con indicazione dei tempi di attuazione e l'evidenziazione di criticità riscontrate.
L'analisi effettuata è entrata a far parte integrante del registro dei trattamenti aziendale di cui all'art.30 par.2 del RGPD.
Inoltre è stata richiesta alle strutture aziendali una autovalutazione di check sul livello di *compliance* col sistema privacy aziendale.

AREA DI RISCHIO	TIPOLOGIA DI RISCHIO
COMPORTAMENTI DEGLI OPERATORI	SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE
	CARENZA DI FORMAZIONE, DISATTENZIONE, INCURIA
	COMPORTAMENTI SLEALI O FRAUDOLENTI
	ERRORE MATERIALE
	ALTRO (SPECIFICARE)
EVENTI RELATIVI AGLI STRUMENTI	AZIONE DI VIRUS INFORMATICI O PROGRAMMI IN GRADO DI VIOLARE IN SISTEMA
	SPAMMING O TENCICHE DI SABOTAGGIO
	MALFUNZIONAMENTO, OBSOLESCENZA OD INDISPONIBILITA' DEGLI STRUMENTI
	ACCESSI ESTERNI NON AUTORIZZATI
	INTERCETTAZIONI DI INFORMAZIONI IN RETE
	ALTRO (SPECIFICARE)
ALTRI EVENTI	ACCESSI NON AUTORIZZATI AD AREE AD ACCESSO RISTRETTO
	ASPORTAZIONE - FURTO DI STRUMENTI CONTENETI DATI
	DISTRUZIONE CONSEGUENTE AD EVENTI NATURALI OD ARTIFICIALI (DOLOSI, ACCIDENZIALI O DOVUTI AD INCURIA)
	GUASTO AI SISTEMI DI SUPPORTO (IMPIANTI ELETTRICI, CLIMATIZZAZIONE, ETC.)
	ERRORI UMANI NELLA GESTIONE OPERATIVA DELLA SICUREZZA
	ALTRO (SPECIFICARE)

Asl3
Sistema Sanitario Regione Liguria

SCHEDA ANALISI E VALUTAZIONE RISCHI POTENZIALI TAB_CDC_SS

DENOMINAZIONE E CODICE DIPARTIMENTO :	
CENTRO DI COSTO DIPARTIMENTO	
DENOMINAZIONE E CODICE STRUTTURA :	
CENTRO DI COSTO DI STRUTTURA	
DATA:	

CODICE IDENTIFICATIVO DEL TRATTAMENTO	RISCHI POTENZIALI		SI	NO	IMPATTO SULLA SICUREZZA DEI DATI E GRAVITA' STIMATA			MISURE DI SICUREZZA ADOTTATE		MISURE DI SICUREZZA PROPOSTE				GRADO % DI INCIDENZA SULLE CAUSE DEL RISCHIO	STRUTTURA-SERVIZIO-CIRCOLO RESPONSABILE	TEMPI E MODALITA' DI MONITORAGGIO INTERNO (PRECISARE SE SONO STATI EFFETTUATI CONTROLLI SULLA EFFETTIVA APPLICAZIONE DELLE MISURE; SE NON SI SONO VERIFICATI INDICARE LE MOTIVAZIONI DEL LORO MANCATO SVOLGIMENTO)
	AREA DI RISCHIO	TIPOLOGIA DI RISCHIO			ALTA	MEDIA	BASSA	INFORMATICHE	NON INFORMATICHE	INFORMATICHE	TEMPI ATTUAZIONE	NON INFORMATICHE	TEMPI ATTUAZIONE			
	COMPORTAMENTI DEGLI OPERATORI	SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE														
	COMPORTAMENTI DEGLI OPERATORI	CARENZA DI FORMAZIONE, DISATTENZIONE, INCURIA														
	COMPORTAMENTI DEGLI OPERATORI	COMPORTAMENTI SLEALI O FRAUDOLENTI														
	COMPORTAMENTI DEGLI OPERATORI	ERRORE MATERIALE														
	COMPORTAMENTI DEGLI OPERATORI	ALTRO (SPECIFICARE)														
	EVENTI RELATIVI AGLI STRUMENTI	AZIONE DI VIRUS INFORMATICI O PROGRAMMI IN GRADO DI VIOLARE IN SISTEMA														
	EVENTI RELATIVI AGLI STRUMENTI	SPAMMING O TECNICHE DI SABOTAGGIO														
	EVENTI RELATIVI AGLI STRUMENTI	MALFUNZIONAMENTO, OBSOLESCENZA, O INDISPONIBILITA' DEGLI STRUMENTI														
	EVENTI RELATIVI AGLI STRUMENTI	ACCESSI ESTERNI NON AUTORIZZATI														
	EVENTI RELATIVI AGLI STRUMENTI	INTERCETTAZIONI DI INFORMAZIONI IN RETE														
	EVENTI RELATIVI AGLI STRUMENTI	ALTRO (SPECIFICARE)														
	ALTRI EVENTI	ACCESSI NON AUTORIZZATI AD AREE AD ACCESSO RISTRETTO														
	ALTRI EVENTI	DISTRUZIONE / PERDITA DI STRUMENTI CONTENENTI DATI														
	ALTRI EVENTI	DISTRUZIONE CONSEGUENTE AD EVENTI NATURALI OD ARTIFICIALI (DOLOSI, ACCIDENTALI O DOVUTI AD INCURIA)														
	ALTRI EVENTI	GUASTO AI SISTEMI DI SUPPORTO (IMPIANTI ELETTRICI, CLIMATIZZAZIONE, ETC.)														
	ALTRI EVENTI	ERRORE UMANO NELLA GESTIONE OPERATIVA DELLA SICUREZZA														
	ALTRI EVENTI	ALTRO (SPECIFICARE)														

LEGENDA STANDARD DI CODIFICA TRATTAMENTO :
CDC-<Struttura_ID>.....

Asl3
Sistema Sanitario Regione Liguria

SCHEDA MONITORAGGIO RISCHI POTENZIALI TAB_CDC_04

DENOMINAZIONE E CODICE DIPARTIMENTO E CENTRO DI COSTO>	
DENOMINAZIONE E CODICE STRUTTURA E CENTRO DI COSTO>	

CODICE IDENTIFICATIVO DEL TRATTAMENTO	RISCHI POTENZIALI		SI	NO	IMPATTO SULLA SICUREZZA DEI DATI E GRAVITA' STIMATA			MISURE DI SICUREZZA ADOTTATE		MISURE DI SICUREZZA PROPOSTE				GRADO DI INCIDENZA SULLE CAUSE DEL RISCHIO	STRUTTURA /SERVIZIO /UFFICIO RESPONSABILE	TEMPI E MODALITA' DI MONITORAGGIO INTERNO (INDICARE SE SONO STATI ATTUATI CONTROLLI SULLA EFFETTIVA APPLICAZIONE DELLE MISURE; SE NON SI SONO VERIFICATI INDICARE LE MOTIVAZIONI DEL LORO MANCATO SVOLGIMENTO)	PRECISAZIONI SULL'APPLICAZIONE DELLE MISURE (DIFFICOLTA' RISCONTRATE NELL'APPLICAZIONE, MODALITA' DI COINVOLGIMENTO DEI SOGGETTI DI LAVORO, TEMPI E MODALITA')
	AREA DI RISCHIO	TIPOLOGIA DI RISCHIO			ALTA	MEDIA	BASSA	INFORMATICHE	NON INFORMATICHE	INFORMATICHE	TEMPI ATTUAZIONE	NON INFORMATICHE	TEMPI ATTUAZIONE				
	COMPORTAMENTI DAGLI OPERATORI	SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE															
	COMPORTAMENTI DAGLI OPERATORI	CARENZA DI FORMAZIONE, DISATTENZIONE, INCURIA															
	COMPORTAMENTI DAGLI OPERATORI	COMPORTAMENTI SLEALI O FRAUDOLENTI															
	COMPORTAMENTI DAGLI OPERATORI	ERRORE MATERIALE															
	COMPORTAMENTI DAGLI OPERATORI	ALTRO (SPECIFICARE)															
	EVENTI RELATIVI AGLI STRUMENTI	ASSENZA DI VALIDI SUPPORTATO DI PROGRAMMI IN GRADO DI VIGILARE IN SISTEMA															
	EVENTI RELATIVI AGLI STRUMENTI	SPAMMING O TENTATIVI DI SABOTAGGIO															
	EVENTI RELATIVI AGLI STRUMENTI	MALFUNZIONAMENTO, OBSOLESCENZA DEI MONITORABILITA' DEGLI STRUMENTI															
	EVENTI RELATIVI AGLI STRUMENTI	ASSENZA SISTEMA NON AGGIORNATO															
	EVENTI RELATIVI AGLI STRUMENTI	INTERCETTAZIONI DI INFORMAZIONI IN RETE															
	EVENTI RELATIVI AGLI STRUMENTI	ALTRO (SPECIFICARE)															
	ALTRI EVENTI	ACCESSI NON AUTORIZZATI AD AREE AD ACCESSO RISTRETTO															
	ALTRI EVENTI	FURTO DI STRUMENTI CONTENENTI DATI															
	ALTRI EVENTI	DISTRUZIONE CONSEGUENTE AD EVENTI NATURALI (ES ARTIFICIALI (DOLOSI), ACCIDENTALI) EVENTI A.D INCURIA)															
	ALTRI EVENTI	GUASTO AL SISTEMA DI SUPPORTO (MANCANTI ELETTRICI, CLIMATIZZAZIONE, ETC.)															
	ALTRI EVENTI	ERRORE UMANO NELLA GESTIONE															
	ALTRI EVENTI	OPERATIVA DELLA SICUREZZA															
	ALTRI EVENTI	ALTRO (SPECIFICARE)															

A SEGUITO DELLE RISULTANZE DEL MONITORAGGIO, SI ATTESTA CHE SONO STATE INDIVIDUATE ULTERIORI MISURE DI PREVENZIONE E/O CONTENIMENTO E/O MODIFICATE LE PRESCRITTE AL FINE DI PREVENIRE EPISODI DI VIOLAZIONE PRIVACY

LEGENDA STANDARD DI CODIFICA TRATTAMENTO>
CdC Direzione_01.....

DICHIARAZIONE

FIRMA DEL RESPONSABILE

DATA>

E’ stata inoltre effettuata in tal modo una prima sintesi delle valutazioni dei rischi mappati e delle relative misure di sicurezza adottate:

EVENTO	GRAVITA’ STIMATA	CONTROMISURE
Furto credenziali autenticazione	BASSA	Disposizioni sulla custodia e segretezza delle credenziali
Carenza di formazione, disattenzione, incuria o errore materiale degli autorizzati	BASSA	Formazione, internal auditing ed Istruzioni agli autorizzati circa l’attenzione da porre durante un trattamento
Comportamenti sleali o fraudolenti	BASSA	Informazione e formazione agli autorizzati al trattamento sulle responsabilità penali, civili e disciplinari ed internal auditing
Azioni di virus informatici o programmi in grado di violare il sistema informativo aziendale	MEDIA	Il sistemi server sono protetti da antivirus aggiornati quotidianamente. I personal computer connessi alla Rete Aziendale e facenti parte del dominio ASL 3 sono protetti da antivirus centralizzato aggiornato quotidianamente. I rimanenti pc acquisiscono l’aggiornamento dell’antivirus a richiesta dell’utente, attraverso il servizio di assistenza, e, comunque, almeno ogni tre mesi.
Spamming o altre tecniche di sabotaggio	BASSA	Utilizzo regolamentato dell’uso di Internet e della posta elettronica. Implementazione su server aziendali di programma anti-spam, che blocca la ricezione di e-mail indesiderate.
Malfunzionamento o degrado degli strumenti elettronici	BASSA	Aggiornamento programmato del parco macchine e installazione di patch per le applicazioni da parte del servizio di assistenza

Accessi esterni non autorizzati agli strumenti elettronici	BASSA	La Rete Aziendale si configura come una rete privata e l'accesso avviene attraverso credenziali di autenticazione personali.
Accessi non autorizzati a locali o reparti ad accesso ristretto	BASSA	Disposizioni sulle procedure di accesso e dispositivi di sicurezza fisici
Asportazione e furto di strumenti contenenti dati	BASSA	Dispositivi di sicurezza fisica e sorveglianza
Eventi distruttivi, naturali o artificiali, dolosi, accidentali	BASSA	Adozione sistema antincendio e sorveglianza
Guasti ai sistemi complementari	BASSA	Gruppi di continuità e gruppo elettrogeno per il CED
Errori umani nella gestione operativa della sicurezza	BASSA	copie di back up – formazione dipendenti - policy aziendali

Alla quale si è aggiunto il documento redatto secondo lo schema stabilito dalla circolare AGID 2/2017 del 18/04/2017 "Misure Minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del presidente del Consiglio dei Ministri 1 Agosto 2015), con le specifiche misure di sicurezza evidenziate nel DPS aziendale.

REQUISITI MINIMI DI SICUREZZA

Nello schema seguente sono state descritte le modalità di implementazione relativamente ai requisiti di livello M, ovvero quelli che rappresentano per lo più lo stato attuale dell'Azienda.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI: Sono stati analizzati solo i Requisiti Minimi

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Compliant Il blocco della connessione per i dispositivi non autorizzati è normato dal regolamento Aziendale Attualmente la ASL 3 dispone di inventari realizzati con sw differenti in base alle diverse categorie di dispositivi. Le postazioni di lavoro sono inventariate non automaticamente sulla piattaforma HP Service Manager che ne permette la gestione remota e il controllo delle postazioni e dei dispositivi (stampanti) connessi. Tale applicazione mantiene anche la correlazione tra pc/portatili e utenti ai quali sono assegnate le risorse. La console centralizzata dell'antivirus Symantec Endpoint Protection permette di visualizzare la lista di tutti i server e client con relativo indirizzo IP sulle quali tale sw è installato. L'inventario di tutti i sistemi	Aggiornare Il Regolamento Aziendale sull'utilizzo delle dotazioni informatiche per regolamentare oltre all' utilizzo dei dispositivi aziendali anche gli extraziendali eventuali e stabilendo le tipologie di dispositivi autorizzati esterni all'azienda (dispositivi connessi tramite VPN, dispositivi mobili connessi tramite wifi) Impedire l'accesso alla rete aziendale e VPN ai dispositivi che non sono inventariati e/o successivamente autorizzati.

					server fisici e virtuali in gestione a Liguria Digitale viene mantenuto all'interno di un CMDB che contiene anche le informazioni di configurazione e del sw installato. L'inventario dei cellulari, smartphone e tablet aziendali è mantenuto in un elenco aggiornato manualmente: Esiste un inventario su foglio Excel degli apparati di rete installati e viene aggiornato manualmente. L'elenco degli elettromedicali attivi è contenuto all'interno di un censimento costantemente aggiornato in cui però non viene evidenziato la connessione in rete o stand-alone. Non è ammesso da Regolamento Aziendale sull'utilizzo delle dotazioni informatiche l'utilizzo in rete Aziendale l'utilizzo di dispositivi personali .	Attivare un servizio di autenticazione con utenza di Dominio che separi la rete per i dispositivi aziendali da quella per i dispositivi personali, limitando questi ultimi alla sola navigazione Internet. Tracciare sul censimento delle apparecchiature elettromedicali l'eventuale collegamento in rete.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Compliant con le limitazioni di cui al punto 1.1.1 Il collegamento alla rete di ASL3 dei dispostivi autorizzati avviene dopo una procedura di inserimento manuale sulla piattaforma HP service Manager che ne garantisce la gestione centralizzata.	Aggiornamento del preesistente regolamento relativo all'utilizzo delle attrezzature informatiche aziendali. Attivare un servizio di autenticazione con utenza di Dominio che separi la rete

					L'inventario contenuto nel CMBD viene aggiornato ogni qual volta si connette un nuovo server alla rete. L'aggiornamento dei nuovi apparati di rete connessi avviene manualmente	per i dispositivi aziendali da quella per i dispositivi personali, limitando questi ultimi alla sola navigazione Internet. In tal modo associando i dispositivi autorizzati a ciascun utente di dominio viene regolamentato l'accesso di dispositivi alla intranet anche via wifi.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Compliant Su un foglio di calcolo è tenuta traccia di tutti gli ip statici in uso e relative macchine . Tale corrispondenza è confermata dalla Console Antivirus e su HP Service Manager dove applicabile.	Verifica e aggiornamento inventario. Per i dispositivi BYOD, tablet e smartphone vedi ABSC_ID 1.1.1. e 1.3.1.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire	Compliant Esiste un elenco del software applicativi formalmente autorizzato. Le postazioni di lavoro sono configurate dagli amministratori di sistema e, poiché gli utenti non hanno diritti	Aggiornare l'elenco dei sw autorizzati ed inserirlo nel Regolamento Aziendale da aggiornare annualmente.

				l'installazione di software non compreso nell'elenco.	amministrativi, non è loro consentito installare software in autonomia. Il CMDB mantiene un catalogo delle applicazioni implementate e del software installati sui sistemi server.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Compliant relativamente al contesto autorizzativo: Attualmente non vengono eseguite scansioni temporizzate per verificare il software installato in quanto, non essendo gli utenti amministratori non possono installare nulla sulle postazioni di lavoro(vedi Regolamenti Aziendale utilizzo dotazioni informatiche) Sui server sono installati solamente i software strettamente necessari al funzionamento dei relativi servizi.	E' comunque in fase di test il modulo symantec per la verifica dei sw autorizzati su macchine MS e Linux (server e client). Non appena validato può essere attivato.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorat
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Compliant Sia le postazioni di lavoro che i server vengono installati con configurazioni standard tali da garantire un livello di sicurezza adeguato, prevedendo ad	Formalizzare e/o aggiornare la procedura di configurazione dei sistemi

					esempio un numero minimo di porte di rete aperte e disponibili. Quando ritenuto necessario i sistemi vengono ulteriormente hardenizzati. Non è prevista una configurazione standard per quanto riguarda i dispositivi mobili.	client e server. Pianificare la dismissione dei sistemi obsoleti che non permettono l'applicazione di configurazioni sicure (es. Windows XP).
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Compliant Esiste documento configurazioni standard	Ref. Action proposed ABSC 3.1.1 (Vedi Azione proposta ABSC 3.1.1.)
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Compliant I sistemi compromessi vengono ripristinati come da procedura a partire da immagini di backup integre.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Compliant Esistono copie offline delle immagini di installazione dei sistemi che possono essere utilizzate per effettuare verifiche di integrità.	Formalizzare in procedura la conservazione e manutenzione offline di immagini di

						installazione costantemente aggiornate ed implementare il livello S (3.3.2).
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Compliant Solo gli utenti autorizzati possono accedere alle immagini conservate su una macchina dedicata in rete con storage ridondato.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Compliant /partially compliant per apparati di rete. Tutti i sistemi sono amministrati attraverso connessioni protette e ritenute sicure (SSH, RDP, HTTPS). Rimangono in uso alcuni apparati di rete obsoleti nei quali l'amministrazione remota tramite canali crittografati non è supportata E' in fase di predisposizione una configurazione di un sistema ACS (Access Contro System) su server Radius per la gestione degli apparati di rete	Pianificare la dismissione degli apparati obsoleti (che non supportano l'amministrazione remota tramite canali crittografati). Attivare il sistema ACS attualmente in fase di predisposizione.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Compliant sono a disposizione strumenti automatici gestiti da Liguria Digitale in grado di rilevare eventuali vulnerabilità su tutti i sistemi. Tali ricerche e relativi report sono eseguiti a seguito di segnalazione di nuove vulnerabilità o di significative modifiche della configurazione dei sistemi, su target critici in modo da non gravare significativamente sulle prestazioni della rete.	Nell'ambito del contratto di Gestione in outsourcing con Liguria Digitale, definire procedure formali di scansione sistematica della rete per l'implementazione del livello Standard di cui al punto 4.1.2.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.		
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Compliant Gli strumenti di scansione delle vulnerabilità sono aggiornati in modo automatico.	

4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Compliant Nei sistemi Microsoft, WSUS gestisce la verifica e l'installazione automatica degli aggiornamenti critici e delle patch di sicurezza del sistema operativo e delle applicazioni Microsoft. La gestione delle patch sui sistemi server è semiautomatica al fine di garantire la continuità dei servizi attivi. Attualmente non esiste una gestione centralizzata delle patch relative alle applicazioni non Microsoft. Al fine di garantire la continuità dei servizi in ambito ospedaliero, gli aggiornamenti che possono rivelarsi critici per applicazioni non interrompibili non sono installati automaticamente ma pianificati a seguito di esito positivo di test .	Valutare eventuale pianificazione di aggiornamenti sistematici centralizzati per sistemi Linux

4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono presenti sistemi isolati dalla rete poiché non ne sussistono le necessità	Verificare la presenza e necessità di sistemi air-gapped nella'rea elettromedicale
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Compliant Il personale adibito alla gestione della sicurezza di Liguria Digitale informa il personale IT delle principali vulnerabilità e minacce e, in accordo con esso, pianifica e verifica l'esecuzione delle relative contromisure. Il documento programmatico sulla sicurezza aggiornato contiene l'analisi dei rischi dei dati trattati dall'Ente.	Aggiornare periodicamente l'analisi dei rischi contenuta nel DPS.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Ad oggi non è disponibile un'analisi dei rischi relativi alla cyber security.	Inserire nel DPS l'analisi del rischi
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Compliant Per i sistemi client e server la procedura automatica prevede l'applicazione di tutte le patch relative ai	Prevedere aggiornamenti sistematici delle patch di sicurezza anche direttamente sugli apparati elettromedicali in rete.

					rischi di sicurezza e di quelle ritenute critiche.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Compliant Sulle applicazioni critiche le patch vengono preventivamente testate per valutarne gli impatti (4.5.1)	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Compliant Le utenze di amministrazione sono assegnate solo a personale idoneo e competente. Gli utenti non possiedono privilegi amministrativi nemmeno sulle macchine a loro assegnate	
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Partially Compliant Gli amministratori di sistema di Liguria Digitale utilizzano utenze amministrative sui sistemi di ASL3 unicamente per lo	

					svolgimento di attività di gestione. Gli amministratori di sistema dipendenti di ASL3 possiedono utenze amministrative per lo svolgimento dell'intera attività lavorativa. I log degli accessi degli amministratori sono comunque raccolti da un sistema gestito da Liguria Digitale dai quali si possono tracciare gli accessi	
5	1	3	S	Partially Compliant Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Partially Compliant A livello di server esistono privilegi differenziati per ciascuna utenza amministrativa. Per quanto riguarda i privilegi di amministratore dei client è possibile assegnare i privilegi di amministratore su diversi gruppi di macchine a gruppi di utenze di amministratore diverse.	Valutare l'impatto di definizione di policy più granulari su tutti i client.

5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Compliant L'inventario delle utenze amministrative è aggiornato ad ogni nuova assegnazione e formalmente autorizzata . Esiste lettera di incarico per gli amministratori di sistema di Liguria Digitale che specifica la responsabilità verso i sistemi client e verso gli amministratori di sistema dipendenti di ASL 3.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Compliant Prima di collegare alla rete un nuovo dispositivo le credenziali di amministratore predefinite vengono modificate secondo le policy delle password previste.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Compliant la lunghezza minima delle password degli amministratori attualmente non è impostata a 14 caratteri.	Formalizzare e impostare la lunghezza delle password di Amministratore a 14 caratteri con criteri di elevata robustezza.

						Verificare l'applicazione delle policy di robustezza delle password per i sistemi non gestiti centralmente.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Compliant Le policy MS impongono la modifica delle password almeno ogni 90 giorni, come prescritto dal Garante per la protezione dei dati personali.	Policy robustezza password vedi azioni proposte ABSC 5.7.1.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Compliant Le policy impediscono il riutilizzo delle ultime 4 password utilizzate.	Policy robustezza password vedi azioni proposte ABSC 5.7.1.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non compliant Non viene applicato il controllo temporale per problemi gestionali (password smarrite, reset..)	Applicare la policy temporale a tutti gli utenti tranne che per gli amministratori di dominio ai quali è concessa la modifica delle password degli utenti per ripristini, reser etc.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Partially compliant (cedi 5.7.6)	

					Non viene assicurato un tempo preciso ma viene impedito il restore delle ultime 3 password utilizzate	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Compliant Le utenze amministrative sono destinate esclusivamente ai gestori dei sistemi informativi e completamente distinte dalle utenze che non svolgono tali attività.	Vedi azioni proposte ABSC 5.1.2.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Compliant Sia le utenze standard che quelle amministrative sono personali . (All. B DLG 146/2003)	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Compliant Di norma le utenze amministrative "root" e "Administrator" sono utilizzate solo in caso di emergenza.	Formalizzare la procedura per l'utilizzo di utenze amministrative anonime in caso di emergenza che comprenda la custodia delle password, la registrazione degli utilizzatori e la sostituzione della password.

5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Compliant Le credenziali amministrative sono conservate in busta chiusa accessibile ai soli amministratori di sistema in caso di necessità.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Compliant Attualmente non è prevista l'autenticazione mediante l'utilizzo di certificati digitali. In caso di necessità è tuttavia a disposizione presso Liguria Digitale un sistema di gestione delle chiavi crittografiche.	Valutare l'implementazione di una Public Key Infrastructure (PKI) aziendale.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Compliant Tutti i sistemi gestiti centralmente e collegati alla rete locale sono dotati di sistemi antivirus la cui configurazione e aggiornamento è gestita in maniera centralizzata tramite la console di Symantec Endpoint Protection.	Inserire sempre nei requisiti di gestione degli elettromedicali la dotazione e la gestione degli antivirus analogamnete a quanto avviene per gli altri

						dispositivi informatici connessi in rete
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Compliant I firewall locali sono attivi su sistemi di recente installazione nei quali tale protezione è attiva di default. Il software antivirus in uso è dotato di un modulo con funzionalità di IPS.	Verificare che antivirus e firewall locali siano attivi su tutti i sistemi.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Partially compliant Gli antivirus sono gestiti centralmente e monitorati per tutti i dispositivi in dominiio MS. Agli utenti, non essendo amministratori delle macchine , non è possibile altercarne la configurazione.	Monitorare la gestione degli antivirus anche su altri dispositivi (elettromedicali) per i quali non è possibile la gestione centralizzata
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Compliant Di norma l'utilizzo di dispositivi esterni non necessari per le attività lavorative è limitato. ed è normato dal Regolamento Aziendale	Aggiornare il "Documento programmatico sulla sicurezza" includendo una procedura per la verifica del rispetto della policy di utilizzo dei dispositivi esterni.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.		
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della	Compliant	Aggiornare il Regolamento Aziendale definendo

				connessione dei dispositivi removibili.	L'esecuzione automatica dei contenuti dei dispositivi removibili è disabilitata per tutti i sistemi Microsoft Windows client/server più recenti.	comunque norme di comportamento e policy per tutti gli utenti per la disattivazione dell'esecuzione automatica dei contenuti dinamici (unica cautela possibile per quei casi in cui non è possibile impedirlo tecnicamente).
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Compliant In tutti i sistemi Microsoft Windows client/server e nelle applicazioni più recenti è richiesta all'utente l'autorizzazione all'esecuzione di contenuti dinamici.	Vedi azioni proposte ABSC 8.7.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Compliant I client di posta in gestione a Liguria Digitale di norma impediscono l'apertura automatica dei messaggi come impostazione di default.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Not Compliant Al momento l'anteprima automatica dei contenuti dei file non è disabilitata poiché non ritenuta particolarmente significativa ai fini della sicurezza	Valutare l'impatto sugli utenti e le implicazioni di sicurezza di una policy che disattivi l'anteprima automatica dei contenuti dei file.

8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Partially Compliant La scansione avviene ad oggi prima dell'utilizzo della risorsa.	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Compliant Requisito rispettato attraverso il servizio Antispam (Sophos) gestito da Liguria Digitale	
8	9	2	M	Filtrare il contenuto del traffico web.	Compliant Tutto il traffico web diASL 3 è filtrato da sistemi avanzati di content filtering (Fortinet)	
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Compliant Fare riferimento al gestore del servizio Antispam e Web Filtering (Sophos + Fortinet) gestito da Liguria Digitale	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Compliant I backup delle informazioni necessarie al ripristino dei sistemi server critici e dei sistemi virtuali sono schedulati settimanalmente (vedi allegato tecnico	Inserire nel Regolamento Aziendale una policy che vieti di mantenere informazioni critiche sul

					PTE Liguria Digitale e gestione sistemi LIS e PACS)	disco locale non sottoposte ad attività di backup.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Partially compliant : Il ripristino di prova viene effettuato solo per immagini particolarmente critiche	Regolamentare il ripristino di prova per tutte le copie
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Compliant : I supporti fisici di conservazione dei backup sono adeguatamente protetti in locali chiusi accessibili al solo personale autorizzato e archiviati in cassaforte. Non viene effettuata attività di cifratura.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Compliant : I backup full di lungo periodo sono mantenuti offline su nastri magnetici.	

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai	Partially compliant Non è prevista una attività sistematica di analisi e classificazione delle informazioni	Analizzare la possibilità di applicazione di protezione crittografiche per le categorie più critiche;

				quali va applicata la protezione crittografica	gestite dall'ente salvo nell'ambito di alcuni progetti. Un'analisi circa la riservatezza di diverse tipologie di dati è contenuta all'interno del DPS. Non vengono applicate protezioni crittografiche.	Raffinare l'analisi all'interno del DPS.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Compliant Tutto il traffico internet è filtrato da sistemi avanzati di content filtering in grado di bloccare i flussi da e verso URL non autorizzate (Fortinet).	

Acquisita dagli operatori la familiarità con lo strumento di valutazione e con il lavoro di gruppo, in sinergia con il SIA, e di *internal auditing* , al fine di oggettivare ulteriormente la valutazione effettuata, una volta che si concluderà la fase di preventiva revisione di dettaglio dei trattamenti delle singole strutture-aree, laddove ancora raggruppati in macrocategorie, secondo un format di analisi predefinito, il passo successivo aziendale sarà quello di richiedere una rivalutazione del rischio sulla base del format di questionario per aree di attenzione.

Le fasi che si prevede di attuare come futura implementazione del sistema sono, quindi, nuovamente:

1. Definizione dell'operazione di trattamento e del suo contesto, con applicazione del format scheda di analisi di dettaglio del trattamento sotto riportata:

SCHEDA DI ANALISI DEL TRATTAMENTO	
Item informativi	
Processo di trattamento	
Area interessata	
Finalità del trattamento (sintetica)	
Descrizione dettagliata del processo di trattamento chi fa cosa chi vede cosa	
Modalità trattamento elettronico Indicando i profili di accesso di eventuali applicativi	
Modalità di trattamento cartaceo	
Base giuridica del trattamento	
Tipologia dati trattati	
Descrizione dei dati trattati: es. Nome cognome, indirizzi fisici e mail, contatti telefonici Precisare se è stato rispettato il principio di indispensabilità evitando quindi di richiedere, nel trattamento informazioni eccedenti a quelle strettamente necessarie in relazione alle finalità da raggiungere	
In caso di trattamento di dati supersensibili presenza della garanzia anonimato per legge di settore che tecnicamente viene realizzato con l'oscuramento ossia i dati restano nella sola disponibilità dei medici/reparto/servizio curante in luogo della gestione in forma anonima?	
Categorie dei soggetti INTERESSATI	
Trattamento su larga scala	
Origine del dato	
Responsabile-i esterno-i?	
Categorie dei soggetti DESTINATARI	
I dati vengono trasferiti all'estero?	

Se trasferiti descrivere la base di tutela per trasferimento all'estero	
Tempi di conservazione Indicando modalità e tempi di conservazione dei dati (con ciò facendo riferimento alla separazione dei dati ed alla loro criptatura; organizzazione o meno per moduli)	
Criterio di calcolo (in alternativa)	
Specificare la ragione della tenuta	
Come avviene la cancellazione chi se ne occupa e criteri di controllo	
Fornita idonea informativa ai soggetti interessati	
Consenso o elementi di esclusione del consenso (motivazione)	
Modalità di acquisizione del consenso ed eventuale processo di controllo	
I dati vengono diffusi?	
Se diffusi specificare motivo	
esistenza o meno di un Privacy Impact assessment (DPIA)	
Rischio integrità	
rischio riservatezza	
rischio disponibilità	
esistenza delle garanzie a tutela dell'esercizio dei diritti dell' interessato	

LEGENDA SPECIFICHE:

A seguito degli elementi raccolti , potrà essere necessario espletare da parte di codesta struttura una DPIA per valutare i rischi privacy correlati, qualora non già effettuata.

Processo di trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Area interessata: la struttura organizzativa che gestisce il trattamento
Finalità del trattamento (sintetica): descrizione delle finalità per le quali si effettua il trattamento (es. normativa di riferimento, rapporto contrattuale di riferimento, diagnosi e cura, etc.)
Descrizione dettagliata del processo di trattamento: es. chi fa cosa, chi vede cosa Deve essere analizzato singolarmente ad esempio il trattamento correlato ad uno specifico rapporto convenzionale/contrattuale/derivante da protocollo d'intesa, in quanto abbia una sua peculiarità di gestione del flusso dei dati tra le parti contraenti e/o i soggetti coinvolti nell'espletamento delle attività sanitarie e non , che ne sono oggetto e/o interessati alle stesse. L'analisi del flusso dati deve pertanto essere effettuata coinvolgendo gli operatori che concretamente lo gestiscono quale presupposto indispensabile alla corretta identificazione del trattamento
Precisare se il trattamento è effettuato quale: **titolare** («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) o quale **contitolare** (Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati) o quale **responsabile esterno** (Qualora un trattamento debba essere effettuato per conto del titolare del trattamento)? Precisare in quale dei suddetti ruoli rientra il trattamento. Si ricorda che sia il Titolare che il Contitolare che il responsabile esterno devono precisare in un loro registro dei trattamenti per ogni trattamento il ruolo ricoperto.
Modalità trattamento elettronico: Indicando i profili di accesso (cioè i diversi gradi di visibilità, inserimento dati, verifica dati, controllo dati etc.in relazione al ruolo ricoperto nel trattamento) di eventuali applicativi utilizzati per il trattamento; l'ubicazione di eventuali banche dati, precisando se in cloud e se all'interno dell'UE o all'esterno (cosa uso per trattare i dati e ubicazione dell'asset utilizzato). Precisare le operazioni svolte sui dati es. raccolta, registrazione, conservazione , etc. Si ricorda che detta precisazione va effettuata valutando, in caso di utilizzazione di responsabile esterno per il trattamento, anche analoghe informazioni riguardanti l'attività dello stesso
Modalità di trattamento cartaceo: indicare se si e descrivere modalità di raccolta ed archiviazione, responsabilità della stessa, modalità di reperimento della documentazione. Precisare se presente un archivio cartaceo e sua ubicazione. Precisare le operazioni svolte sui dati es. raccolta, registrazione, conservazione , etc. Si ricorda che detta precisazione va effettuata valutando, in caso di utilizzazione di responsabile esterno per il trattamento, anche analoghe informazioni riguardanti l'attività dello stesso
Base giuridica del trattamento: Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità laddove previsto; b)il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (indicare la fonte normativa dell'obbligo); d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (indicare la fonte normativa). Si ricorda che il trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (tramite legge) non richiede consenso, né si deve garantire la portabilità dei dati, ma occorre fornire l'informativa, nella quale va indicata la base giuridica del trattamento. La finalità deve essere specificata per legge.
Tipologia dati trattati: es. dati personali, dati particolari, dati biometrici, dati genetici, immagini
Descrizione dei dati trattati: Indicare ad es. per i dati personali se sono dati di contatto quali Nome cognome, indirizzi fisici e mail, contatti telefonici
In caso di trattamento di dati supersensibili presenza della garanzia anonimato per legge di settore che tecnicamente viene realizzato con l'oscuramento ossia i dati restano nella sola disponibilità dei medici/reparto/servizio curante in luogo della gestione in forma anonima? Si ricorda che un **dato anonimo** è diverso da un dato pseudoanonimizzato. Si ha infatti **pseudonimizzazione** quando il trattamento dei dati personali è fatto in modi tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Il dato è invece anonimo quando l'informazione è originariamente non associabile ad uno specifico interessato e neppure attraverso una successiva operazione di collegamento ad informazioni di diversa natura, risulti comunque idonea a rendere identificabile un soggetto.
Categorie dei **soggetti INTERESSATI**: L'interessato (*data subject*) al trattamento è la **persona fisica** a cui si riferiscono i dati personali. Tra gli interessati possono comparire anche minori e soggetti vulnerabili, il che comporta che il trattamento in parola, anche per tale aspetto, è soggetto a rischi per i diritti e le libertà delle persone fisiche.
Trattamento su larga scala:tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; **- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;** **- la durata, ovvero la persistenza, dell'attività di trattamento;** **- la portata geografica dell'attività di trattamento.** es. trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
Origine del dato: dove prendo il dato che tratto? Dall'interessato, da un soggetto terzo? E da chi?
Categorie dei soggetti DESTINATARI: **Destinatari** sono, quindi, tutti i soggetti che ricevono **dati** personali dal titolare, siano essi interni od esterni. I **destinatari** possono ricevere tali **dati** per eseguire trattamenti per conto del titolare, o per conseguire proprie specifiche finalità. Specificare chi sono nel trattamento di cui trattasi.
I dati vengono trasferiti all'estero? Precisare se intra UE od extra UE. Si ricorda che il trasferimento può essere anche collegato all'effettuazione di un trattamento da parte di un responsabile esterno che ad es. ha un cloud all'estero. Il trasferimento di dati personali da paesi appartenenti all´UE verso Paesi "terzi" (non appartenenti all´UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è vietato, in linea di principio, a meno che il Paese in questione garantisca un livello di protezione "adeguato" paragonabile a quello garantito dalla UE e l'interessato ne sia preventivamente informato
Se trasferiti descrivere la base di tutela per trasferimento all'estero e se l'interessato ne è preventivamente informato
Tempi di conservazione Indicando modalità e tempi di conservazione dei dati (con ciò facendo riferimento anche ad es.alla separazione dei dati ed alla loro criptatura; organizzazione o meno per moduli)
Criterio di calcolo dei tempi di conservazione (in alternativa) es.durata della vita dell'interessato
Specificare la **ragione della tenuta**: precisare perché devo conservare il dato
Come avviene la cancellazione : chi se ne occupa e criteri di controllo
Fornita **idonea informativa ai soggetti interessati**
Consenso o elementi di esclusione del consenso (motivazione)
Modalità di acquisizione del consenso, se dovuto, ed eventuale processo di controllo
I dati vengono diffusi? Per **diffusione** si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, ad es. diffusione anche quando si pubblica online, ad esempio una fotografia od un documento contenente dati personali.
Se diffusi specificare motivo : Precisare la base giuridica della diffusione es. pubblicità legale, normativa sulla trasparenza
Esistenza o meno di un Privacy Impact assessment **(DPIA):** La **valutazione di impatto del trattamento(D.P.I.A.**, cioè *Data Protection Impact Assessment*) è un **onere posto direttamente a carico del titolare del trattamento** (art. 35 RGPD) e per esso del dirigente con compiti specifici del sistema privacy aziendale che ha in carico il trattamento, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali. E' lo strumento cardine tramite il quale il titolare effettua l'analisi dei rischi derivanti dai trattamenti posti in essere. Il titolare, quindi,deve sviluppare una valutazione preventiva (quindi prima di iniziare il trattamento) delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Il responsabile del trattamento, se esistente, deve assistere il titolare fornendogli ogni informazione necessaria. La valutazione del rischio, da realizzare per ogni singolo trattamento, dovrà portare il titolare a decidere in autonomia se sussistono **rischi elevati** inerenti il trattamento, in assenza dei quali potrà procedere oltre. Se invece ritenesse sussistenti rischi per le libertà e i diritti degli interessati, dovrà individuare le **misure specifiche richieste per attenuare o eliminare tali rischi**. Solo nel caso in cui il titolare non dovesse trovare misure idonee a eliminare o ridurre il rischio, occorrerà consultare l'Autorità di controllo. L'Autorità interviene solo *ex post*, sulle valutazioni del titolare, indicando le misure ulteriori eventualmente da implementare, fino ad eventualmente ammonire il titolare o vietare il trattamento. In ogni caso il titolare e per esso il dirigente con compiti specifici del sistema privacy aziendale che ha in carico il trattamento, dovrà giustificare le sue valutazione e rendicontarle nel registro dei trattamenti.
Rischio integrità del dato: indicare la valutazione del rischio effettuata
Rischio riservatezza del dato: indicare la valutazione del rischio effettuata
rischio disponibilità del dato: indicare la valutazione del rischio effettuata
Esistenza delle **garanzie a tutela dell'esercizio dei diritti dell' interessato:** trattasi dei diritti di cui agli artt. da 15 a 22 del Regolamento UE 679/2016 e norme di armonizzazione, che riconoscono, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne la rettifica ovvero l'integrazione, la cancellazione ("diritto all'oblio"), salvo i casi previsti all'art. 17 comma 3 del Regolamento UE 679/2016 e norme di armonizzazione ("**Diritto alla cancellazione («diritto all'oblio»)-** 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia

necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.") , la limitazione del trattamento, se ricorrano le ipotesi di cui all'art. 18 del Regolamento UE 679/2016 e norme di armonizzazione **("Diritto di limitazione di trattamento")**, l'opposizione al loro trattamento ai sensi dell'art. 21 del regolamento UE 679/2016 e norme di armonizzazione **("Diritto di opposizione")** nonché il diritto alla portabilità dei dati.
Nonché il diritto di proporre reclamo all'Autorità di controllo (Autorità Garante per la protezione dei dati personali- secondo le modalità previste sul sito internet dello stesso **www.garanteprivacy.it**) nei casi previsti dalle disposizioni in materia di protezione dei dati di cui al Regolamento UE 679/2016 e norme di armonizzazione.

2. Comprensione e valutazione dell'impatto, utilizzando una scala di valori a tre livelli (BASSO,MEDIO,ALTO/MOLTO ALTO).

Solo dopo il completamento dell'analisi si potrà procedere in azienda ad una rivalutazione del rischio seguendo una metodologia ispirata alle linee guida dell'ENISA sopra citate.
I parametri sono quelli indicati dall'art.32 del RGPD :riservatezza del dato, disponibilità del dato, integrità del dato.
La valutazione d'impatto è un processo qualitativo e il Titolare del trattamento deve considerare una serie di fattori quali la tipologia di dati personali, la criticità dell'operazione di trattamento, il volume dei dati personali, le caratteristiche speciali del Titolare del trattamento, come anche le speciali categorie di interessati.
La valutazione ovviamente non può che essere effettuata a priori, prendendo in considerazione un evento ipotetico in cui vengano a mancare i suddetti parametri.
Il livello di impatto sarà, pertanto, valutato:
basso: quando gli interessati possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, maggior tempo di compilazione, fastidi, irritazioni, ecc.).
medio: quando gli interessati possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
alto/molto alto: quando gli interessati possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.)/ quando gli interessati possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).
Detta valutazione di impatto dovrà essere effettuata per ognuno dei tre parametri . riservatezza del dato, disponibilità del dato, integrità del dato.
Dopo questa valutazione, saranno ottenuti tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità). **Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali. Se manca un parametro, si prende come livello di impatto quello più alto dei tre livelli.**

Un set domande supporta la valutazione:

VALUTAZIONE DI IMPATTO DEL TRATTAMENTO			
CODIFICA TRATTAMENTO	**NUMERO DOMANDA**	**DOMANDE**	**VALUTAZIONE**
	1	**Si prega di riflettere sull'impatto che una divulgazione non autorizzata (perdita di riservatezza) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	2	**Si prega di riflettere sull'impatto che un'alterazione non autorizzata (perdita di integrità) dei dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	3	**Si prega di riflettere sull'impatto che una distruzione o perdita non autorizzata (perdita di disponibilità) di dati personali - nel contesto in cui il Titolare del trattamento svolge la propria attività - potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza.**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO

3. Definizione di possibili minacce e valutazione della loro probabilità (probabilità di occorrenza della minaccia) mediante un questionario di 20 domande suddiviso in 4 aree rilevanti, che esita in un risultato graduato su una scala di valori a 3 livelli (BASSO,MEDIO,ALTO).

Seguendo questo approccio, il livello di probabilità di occorrenza della minaccia può essere definito per ciascuna delle aree di valutazione, come segue:

- ✓ **Basso**: è improbabile che la minaccia si materializzi.
- ✓ **Medio:** c'è una ragionevole possibilità che la minaccia si materializzi.
- ✓ **Alto/Molto Alto**: la minaccia potrebbe materializzarsi.

In questa fase, lo scopo del Titolare del trattamento è comprendere le minacce correlate al contesto complessivo del trattamento dei dati personali (esterno o interno) e valutare la loro probabilità (probabilità di accadimento della minaccia).

Un set domande supporta la valutazione in relazione all'ambiente di elaborazione dei dati (che è direttamente rilevante per le minacce).

In tale prospettiva, le domande sono relative a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati , vale a dire:

- Risorse di rete e tecniche (hardware e software)
- Processi / procedure relativi all'operazione di trattamento dei dati
- Diverse parti e persone coinvolte nell'operazione di trattamento
- Settore di operatività e scala del trattamento

Si dovrà valutare il livello di probabilità di occorrenza di ogni singola minaccia.

VALUTAZIONE DI PROBABILITA' DI OCCORRENZA DELLE MINACCE AL TRATTAMENTO			
CODIFICA TRATTAMENTO	**NUMERO DOMANDA**	**DOMANDE**	**VALUTAZIONE**
A. RISORSE DI RETE E TECNICHE			
	1	**Qualche parte del trattamento dei dati personali viene eseguita tramite Internet?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	2	**È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	3	**Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	4	**Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	5	**Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI			
	6	**I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	7	**L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	8	**I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	9	**I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?**	o BASSO o MEDIO o ALTO/MOLTO ALTO
	10	**Le attività di elaborazione dei dati personali possono essere**	o BASSO o MEDIO

		eseguite senza la creazione di file di registro?	○ ALTO/MOLTO ALTO
C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI			
	11	**Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	12	**Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	13	**Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	14	**Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	15	**Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO			
	16	**Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	17	**La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	18	**Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	19	**Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO
	20	**Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?**	○ BASSO ○ MEDIO ○ ALTO/MOLTO ALTO

LEGENDA:

DOMANDA 1: Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e, quindi, rintracciabile / noto) a tutti gli utenti di Internet.

DOMANDA 2 Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in

spazi pubblici). Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione / amministrazione remota del sistema IT.

DOMANDA 3: La connessione a sistemi IT esterni può introdurre ulteriori minacce dovute alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale anche per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate a tale accesso).

DOMANDA 4: Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente all'IT, apparecchiature e componenti di rete, o non riuscendo a fornire protezione della sala computer in caso di disastro fisico)

DOMANDA 5: Componenti hardware e software mal progettate, implementate e / o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accrescono l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare esposizione (ai rischi) e raggiungere determinati livelli di resilienza.

DOMANDA 6: Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore trattamento) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.

DOMANDA 7: Quando un uso accettabile delle risorse non è chiaramente obbligatorio, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio, intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i rischi potenziali.

DOMANDA 8: I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.

DOMANDA 9: L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.

DOMANDA 10: La mancanza di adeguati meccanismi di registrazione e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/ procedure e risorse, con conseguente abuso di dati personali.

DOMANDA 11: Quando l'accesso (e l'ulteriore trattamento) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano incrementano. Definire chiaramente chi ha realmente bisogno di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.

DOMANDA 12: Quando l'elaborazione viene eseguita da contraenti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un massimo livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.

DOMANDA 13: Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. divulgazione o distruzione) di dati aumentano in modo significativo.

DOMANDA 14: Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.

DOMANDA 15: Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzo non autorizzati.

DOMANDA 16: Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore dell'organizzazione del Titolare del trattamento , questa è un'indicazione che l'organizzazione probabilmente dovrebbe prendere ulteriori misure per evitare un evento simile.

DOMANDA 17: Se l'organizzazione è già stata attaccata o ci sono indicazioni che questo potrebbe essere stato il caso, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.

DOMANDA 18: Bug di sicurezza / vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.

DOMANDA 19: Il tipo e il volume dei dati personali (scala) possono rendere l'operazione di trattamento dei dati di interesse per gli aggressori (a causa del valore intrinseco di questi dati).

DOMANDA 20: Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.

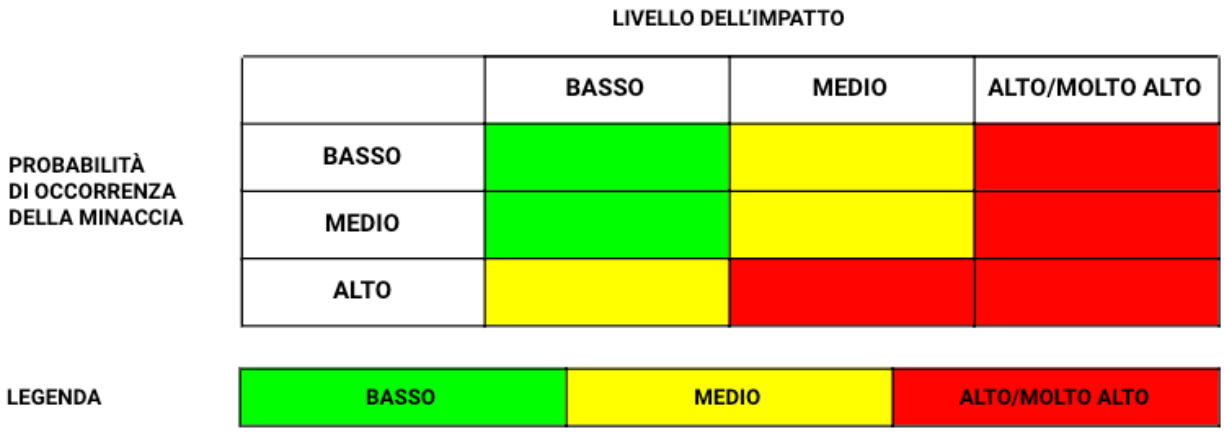
Per facilitare il calcolo del valore finale della probabilità , si possono utilizzare quindi le seguenti tabelle riassuntive per area di analisi per ciascun trattamento:

CODIFICA TRATTAMENTO	AREA DI VALUTAZIONE	PROBABILITA'	
		LIVELLO	PUNTEGGIO
	A. RISORSE DI RETE E TECNICHE	o BASSO	**1**
		o MEDIO	**2**
		o ALTO/MOLTO ALTO	**3**
	B. PROCESSI / PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO DEI DATI	o BASSO	**1**
		o MEDIO	**2**
		o ALTO/MOLTO ALTO	**3**
	C. PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	o BASSO	**1**
		o MEDIO	**2**
		o ALTO/MOLTO ALTO	**3**
	D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	o BASSO	**1**
		o MEDIO	**2**
		o ALTO/MOLTO ALTO	**3**

E per somma globale finale della probabilità di occorrenza per ciascun trattamento, ottenuta sommando i quattro diversi punteggi ottenuti nelle aree di valutazione per ciascun trattamento ed applicando i *range* di livello riportati nella sottostante tabella:

CODIFICA TRATTAMENTO	Somma globale punteggi della probabilità di occorrenza di minacce	LIVELLO DI PROBABILITA' GLOBALE DELLE MINACCE
	4-5	BASSO
	6-8	MEDIO
	9-12	ALTO/MOLTO ALTO

4. Valutazione del rischio (combinando la probabilità di accadimento della minaccia e l'impatto, in una matrice 3x3, che esita in un risultato graduato su una scala di valori a tre livelli (BASSO,MEDIO,ALTO).



In cui il verde è il livello di rischio ritenuto accettabile, il giallo richiede interventi di mitigazione ed il rosso richiede rapide contromisure.

Le misure di sicurezza tecnico-organizzativa vengono poi individuate in coerenza con il livello di rischio così definito e tenendo conto delle indicazioni della norma ISO 27001:2013 sulla sicurezza delle informazioni (ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=54534).
Le linee guida ENISA (**Tab. A allegata** , estratta dal Manuale sulla sicurezza nel trattamento dei dati personali) considerano due ampie categorie di misure (organizzative e tecniche), ulteriormente suddivise in sottocategorie specifiche codificate. In ogni sottocategoria vengono presentate le misure per livello di rischio (basso: verde, medio: giallo, alto: rosso). Al fine di ottenere la scalabilità, si assume che tutte le misure descritte nel livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, misure presentate nel livello medio (giallo) sono applicabili anche ad alto livello di rischio. Misure presentate nel livello alto (rosso) non sono applicabili a qualsiasi altro livello di rischio.
Ovviamente il valutatore potrà effettuare tutte le integrazioni ritenute, anche in relazione a specifici obblighi normativi connessi allo specifico trattamento.

TABELLA A

A.1 Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore BASSO.

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	IDENTIFICATORE DELLA MISURA	DESCRIZIONE DELLA MISURA DI SICUREZZA	PERTINENTE ALLA CERTIFICAZIONE ISO / IEC 27001: 2013 CONTROLLO
Politica di sicurezza e procedure per la protezione dei dati personali	**A.1**	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	**A.5 Politica di sicurezza**
Politica di sicurezza e procedure per la protezione dei dati personali	**A.2**	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	**A.5 Politica di sicurezza**
Ruoli e responsabilità	**B.1**	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	**A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni**
Ruoli e responsabilità	**B.2**	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo , l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	**A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni**
Politica di controllo degli accessi	**C.1**	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati .	**A.9.1.1 Politica di controllo degli accessi**
Gestione risorse/asset	**D.1**	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	**A.8 Asset management**
Gestione risorse/asset	**D.2**	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	**A.8 Asset management**
Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT	**E.1**	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	**A. 12.1 Procedure operative e responsabilità**

Gestione delle operazioni di sviluppo software e dei test di sviluppo	**E.2**	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	**A. 12.1 Procedure operative e responsabilità**
Responsabili del trattamento	**F.1**	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	**A.15 Rapporti con i fornitori**
Responsabili del trattamento	**F.2**	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	**A.15 Rapporti con i fornitori**
Responsabili del trattamento	**F.3**	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	**A.15 Rapporti con i fornitori**
Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)	**G.1**	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	**A.16 Gestione degli incidenti sulla sicurezza delle informazioni**
Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)	**G.2**	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna.. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	**A.16 Gestione degli incidenti sulla sicurezza delle informazioni**
Business continuity	**H.1**	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	**A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa**
Obblighi di confidenzialità imposti al personale	**I.1**	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione .	**A.7 Sicurezza delle risorse umane**

Formazione	**J.1**	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	**A.7.2.2 Consapevolezza della sicurezza delle informazioni, educazione e formazione**
Controllo degli accessi e autenticazione	**K.1**	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.2**	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.3**	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.4**	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	**A.9 Controllo degli accessi**
Generazione di file di log e monitoraggio	**L.1**	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	**A.12.4 Registrazione e monitoraggio**
Generazione di file di log e monitoraggio	**L.2**	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento	**A.12.4 Registrazione e monitoraggio**
Sicurezza di Server e Database	**M.1**	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	**A. 12 Operations security**
Sicurezza di Server e Database	**M.2**	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR) .	**A. 12 Operations security**
Sicurezza delle Postazioni di lavoro	**N.1**	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza delle Postazioni di lavoro	**N.2**	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza delle Postazioni di lavoro	**N.3**	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza delle Postazioni di lavoro	**N.4**	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**

Sicurezza delle Postazioni di lavoro	**N.5**	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica	**O.1**	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL).	**A.13 Communications Security**
Back-ups	**P.1**	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	**A.12.3 Back-Up**
Back-ups	**P.2**	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	**A.12.3 Back-Up**
Back-ups	**P.3**	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	**A.12.3 Back-Up**
Back-ups	**P.4**	I backup completi devono essere eseguiti regolarmente.	**A.12.3 Back-Up**
Dispositivi mobili / portatili	**Q.1**	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	**A. 6.2 Dispositivi mobili e teleworking**
Dispositivi mobili / portatili	**Q.2**	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati.	**A. 6.2 Dispositivi mobili e teleworking**
Dispositivi mobili / portatili	**Q.3**	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	**A. 6.2 Dispositivi mobili e teleworking**
Sicurezza del ciclo di vita delle applicazioni	**R.1**	Durante lo sviluppo del ciclo di vita si devono seguire le migliori pratiche, lo stato dell'arte e pratiche di sviluppo, framework o standard di protezione sicuri ben noti.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.2**	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.3**	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.4**	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.5**	Durante lo sviluppo, test e convalida deve essere eseguita l'implementazione dei requisiti di sicurezza iniziali.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Cancellazione / eliminazione dei dati	**S.1**	La sovrascrittura basata sul software deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), È necessario eseguire la distruzione fisica.	**A. 8.3.2 Smaltimento di supporti e 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**
Cancellazione / eliminazione dei dati	**S.2**	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	**A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**

Sicurezza fisica	**T.1**	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	**A.11 - Sicurezza fisica e ambientale**

A.2 Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore MEDIO.

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	IDENTIFICATORE DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA	PERTINENTE ALLA CERTIFICAZIONE ISO / IEC 27001: 2013 CONTROLLO
Policy di sicurezza e procedure per la protezione dei dati personali	**A.3**	L'organizzazione dovrebbe documentare una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La policy deve essere approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento e alle parti esterne interessate	**A.5 Policy di sicurezza**
Policy di sicurezza e procedure per la protezione dei dati personali	**A.4**	La policy di sicurezza dovrebbe almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali.	**A.5 Policy di sicurezza**
Policy di sicurezza e procedure per la protezione dei dati personali	**A.5**	Dovrebbe essere creato e mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.	**A.5 Policy di sicurezza**
Ruoli e responsabilità	**B.3**	Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.	**A.6.1.1 Ruoli e responsabilità della sicurezza delle informazioni**
Politica di controllo degli accessi	**C.2**	Dovrebbe essere dettagliata e documentata una politica di controllo degli accessi. L'organizzazione dovrebbe determinare in questo documento le regole di controllo appropriate degli accessi, i diritti di accesso e le restrizioni per specifici ruoli degli utenti nell'ambito dei processi e delle procedure relative ai dati personali.	**A.9.1.1 Politica di controllo degli accessi**
Politica di controllo degli accessi	**C.3**	Dovrebbe essere chiaramente definita e documentata la segregazione dei ruoli di controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).	**A.9.1.1 Politica di controllo degli accessi**
Gestione risorse / asset	**D.3**	I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati.	**A.8 Gestione delle risorse**
Gestione delle modifiche	**E.3**	Dovrebbe essere prevista e applicata una policy interna che disciplini la gestione delle modifiche e che includa per lo meno: un processo che governi l'introduzione delle modifiche, i ruoli / utenti che hanno i diritti di modifica, le tempistiche per l'introduzione delle modifiche. La policy di gestione delle modifiche dovrebbe essere regolarmente aggiornata.	**A. 12.1 Procedure operative e responsabilità**
Responsabili del trattamento	**F.4**	L'organizzazione del titolare del trattamento dovrebbe svolgere regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei di requisiti e obblighi.	**A.15 Rapporti con i fornitori**

Gestione degli incidenti / Personal data breaches	**G.3**	Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.	**A.16 Gestione degli incidenti di sicurezza delle informazioni**
Business continuity	**H.2**	Dovrebbe essere predisposto, dettagliato e documentato un Business Continuity Plan (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli.	**A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa**
Business continuity	**H.3**	Un livello di qualità del servizio garantito dovrebbe essere definito nel Business Continuity Plan per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.	**A. 17 Aspetti di sicurezza delle informazioni della gestione della continuità operativa**
Obblighi di confidenzialità imposti al personale	**I.2**	Prima di assumere i propri compiti, i dipendenti, lavoratori e persone autorizzate al trattamento dovrebbero essere invitati a rivedere e concordare le policy di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.	**A.7 Sicurezza delle risorse umane**
Formazione	**J.2**	L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici per l'introduzione (alle questioni di protezione dei dati) dei nuovi arrivati.	**A.7.2.2 Consapevolezza, educazione e formazione alla sicurezza delle informazioni**
Controllo degli accessi e autenticazione	**K.5**	Dovrebbe essere definita e documentata una policy specifica per la password. La policy deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili.	**A.9** Controllo degli accessi
Controllo degli accessi e autenticazione	**K.6**	Le password degli utenti devono essere memorizzate in una forma "hash".	**A.9** Controllo degli accessi
Generazione di file di log e monitoraggio	**L.3**	necessario Dovrebbe essere necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / cancellazione / modifica dei diritti dell'utente.	**A.12.4 Registrazione e monitoraggio**
Generazione dei file di log e monitoraggio	**L.4**	Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei file di registro. Anche l'accesso ai file di registro dovrebbe essere registrato oltre al monitoraggio per rilevare attività insolite.	**A.12.4 Registrazione e monitoraggio**
Generazione dei file di log e monitoraggio	**L.5**	Un sistema di monitoraggio dovrebbe generare i file log e produrre report sullo stato del sistema e notificare potenziali allarmi.	**A.12.4 Registrazione e monitoraggio**
Sicurezza del server / database	**M.3**	Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'implementazione di software o hardware.	**A. 12 Sicurezza delle operazioni**
Sicurezza del server / database	**M.4**	Dovrebbe prendersi in considerazione la necessità di applicare la crittografia alle unità/driver di archiviazione.	**A. 12 Sicurezza delle operazioni**
Sicurezza del server / database	**M.5**	Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione di dati provenienti da identificativi diretti per evitare il collegamento con l'interessato senza ulteriori informazioni	**A. 12 Sicurezza delle operazioni**
Sicurezza della Postazione di lavoro	**N.6**	Le applicazioni antivirus e le firme di rilevamento devono essere configurate su base giornaliera.	**A. 14.1 Requisiti di sicurezza dei sistemi di informazione**
Sicurezza della rete / comunicazione	**O.2**	L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e per processi specifici. Dovrebbe essere protetto da meccanismi di crittografia.	**A.13 Sicurezza delle comunicazioni**

Sicurezza della rete / comunicazione	**O.3**	In generale, l'accesso da remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti.	**A.13 Sicurezza delle comunicazioni**
Sicurezza della rete / comunicazione	**O.4**	Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.	**A.13 Sicurezza delle comunicazioni**
Back-ups	**P.5**	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza.	**A.12.3 Back-Up**
Back-ups	**P.6**	I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera.	**A.12.3 Back-Up**
Back-ups	**P.7**	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi.	**A.12.3 Back-Up**
Back-ups	**P.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 del trattamento.	**A.12.3 Back-Up**
Dispositivi mobili / portatili	**Q.4**	I ruoli e le responsabilità specifici relativi alla gestione dei dispositivi mobili e portatili dovrebbero essere chiaramente definiti.	**A. 6.2 Dispositivi mobili e telelavoro**
Dispositivi mobili / portatili	**Q.5**	L'organizzazione dovrebbe essere in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso.	**A. 6.2 Dispositivi mobili e telelavoro**
Dispositivi mobili / portatili	**Q.6**	I dispositivi mobili dovrebbero supportare la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.	**A. 6.2 Dispositivi mobili e telelavoro**
Dispositivi mobili / portatili	**Q.7**	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.	**A. 6.2 Dispositivi mobili e telelavoro**
Sicurezza del ciclo di vita delle applicazioni	**R.6**	Valutazione delle vulnerabilità, applicazione e test di penetrazione delle infrastrutture dovrebbero essere eseguiti da una terza parte certificata prima dell'adozione operativa. L'applicazione considerata non dovrebbe poter essere adottata fino a quando non sia stato raggiunto il livello di sicurezza richiesto.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.7**	Devono essere eseguiti test periodici di penetrazione.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.8**	Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi informatici utilizzati.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Sicurezza del ciclo di vita delle applicazioni	**R.9**	I patch software dovrebbero essere testati e valutati prima di essere installati in un ambiente operativo.	**A.12.6 Gestione della vulnerabilità tecnica e A.14.2 Sicurezza nei processi di sviluppo e supporto**
Cancellazione / eliminazione dei dati	**S.3**	Più passaggi di sovrascrittura basata su software devono essere eseguiti su tutti i supporti prima di essere smaltiti.	**A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**
Cancellazione / eliminazione dei dati	**S.4**	Se i servizi di terzi sono utilizzati per disporre in modo sicuro di supporti o documenti cartacei, è necessario stipulare un contratto di servizio e produrre un record di distruzione dei record, a seconda dei casi.	**A. 8.3.2 Smaltimento di supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**

Sicurezza fisica	**T.2**	Identificazione chiara, tramite mezzi appropriati, ad es. I badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbero essere stabiliti, a seconda dei casi.	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.3**	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi dovrebbero essere mantenuti e monitorati in modo sicuro	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.4**	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.5**	Se del caso, dovrebbero essere costruite barriere fisiche per impedire l'accesso fisico non autorizzato.	**A.11 – Sicurezza fisica e ambientale**
Sicurezza fisica	**T.7**	Un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS) dovrebbero essere attivati nella sala server.	**A.11 Sicurezza fisica e ambientale**
Sicurezza fisica	**T.8**	Il personale di servizio di supporto esterno deve avere accesso limitato alle aree protette.	**A.11 – Sicurezza fisica e ambientale**

A.3 Misure di sicurezza tecniche e organizzative da adottarsi in caso di rischi alla sicurezza qualificati come di valore ALTO.

CATEGORIA DI APPARTENENZA DELLA MISURA DI SICUREZZA	IDENTIFICATORE DELLA MISURA DI SICUREZZA	DESCRIZIONE DELLA MISURA DI SICUREZZA	PERTINENTE ALLA CERTIFICAZIONE ISO / IEC 27001: 2013 CONTROLLO
Procedure e policy di sicurezza per la protezione dei dati personali	**A.6**	Le policy di sicurezza dovrebbero essere riviste e corrette, se necessario, su base semestrale.	**A.5 Security policy**
Ruoli e responsabilità	**B.4**	Il responsabile della sicurezza dovrebbe essere nominato formalmente (documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati.	**A.6.1.1 Information security roles and responsibilities**
Ruoli e responsabilità	**B.5**	Compiti e responsabilità in conflitto, ad esempio i ruoli di responsabile della sicurezza, revisore della sicurezza e DPO, dovrebbero essere considerati separatamente per ridurre le ipotesi di modifiche non autorizzate o non intenzionali o un uso improprio di dati personali.	**A.6.1.1 Information security roles and responsibilities**
Policy di controllo degli accessi	**C.4**	I ruoli con molti diritti di accesso dovrebbero essere chiaramente definiti e assegnati a un numero limitato di persone dello staff	**A.9.1.1 Access control policy**
Gestione risorse / asset	**D.4**	Le risorse IT dovrebbero essere riviste e aggiornate su base annuale.	**A.8 Asset management**
Responsabili del trattamento	**F.5**	I dipendenti del responsabile del trattamento che stanno trattando dati personali devono essere soggetti a specifici accordi documentati di riservatezza / non divulgazione.	**A.15 Rapporti con i fornitori**
Gestione degli incidenti / Violazione dei dati	**G.4**	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti	**A.16 Gestione degli incidenti di sicurezza**

personali (data breaches)		l'evento e le successive azioni di mitigazione intraprese.	
Business continuity	**H.4**	Dovrebbe essere nominato del personale con la dovuta responsabilità, autorità e competenza per gestire la business continuity in caso di incidente / violazione dei dati personali.	**A.17 Aspetti di sicurezza nella gestione della business continuity**
Business continuity	**H.5**	Si dovrebbe prendere in considerazione una struttura IT alternativa (disaster recovery), a seconda dei tempi di inattività accettabili dei sistemi IT.	**A.17 Aspetti di sicurezza nella gestione della business continuity**
Obblighi di confidenzialità imposti al personale	**L.3**	I dipendenti coinvolti nel trattamento dei dati personali ad alto rischio dovrebbero essere vincolati a specifiche clausole di riservatezza (ai sensi del loro contratto di lavoro o altro atto legale).	**A7 Sicurezza delle risorse umane**
Formazione	**J3**	Dovrebbe essere predisposto ed eseguito su base annuale un piano di formazione con scopi e obiettivi definiti.	**A.7.2.2. Consapevolezza, educazione e formazione alla sicurezza delle informazioni**
Controllo degli accessi e autenticazione	**K.7**	L'autenticazione a due fattori (autenticazione forte) dovrebbe preferibilmente essere implementata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.	**A.9 Controllo degli accessi**
Controllo degli accessi e autenticazione	**K.8**	Dovrebbe essere una soggetto ad autenticazione ogni dispositivo (autenticazione endpoint) per garantire che il trattamento dei dati personali venga eseguita solo attraverso dispositivi autorizzati nella rete aziendale	**A.9 Controllo degli accessi**
Sicurezza Server/Database	**M.6**	Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le interrogazioni autorizzate, interrogazioni a tutela della privacy, tecniche che consentono la ricerca di informazioni su contenuti crittografati, etc.	**A.12 Operazioni di sicurezza**
Sicurezza della postazione di lavoro	**N.7**	Non dovrebbe essere consentito il trasferimento di dati personali dalla postazione di lavoro a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).	**A.14.1 Requisiti di sicurezza nei sistemi**
Sicurezza della postazione di lavoro	**N.8**	Le postazioni di lavoro utilizzate per il trattamento dei dati personali dovrebbero preferibilmente non essere collegate a Internet a meno che non siano in atto misure di sicurezza per impedire il trattamento, la copia e il trasferimento non autorizzati di dati personali.	**A.14.1 Requisiti di sicurezza nei sistemi**
Sicurezza della postazione di lavoro	**N.9**	La completa crittografia del disco dovrebbe essere abilitata sulle unità del sistema operativo della workstation postazione di lavoro.	**A.14.1 Requisiti di sicurezza nei sistemi**
Sicurezza della rete / comunicazioni	**O.5**	La connessione a Internet non dovrebbe essere consentita ai server e alle postazioni di lavoro utilizzate per il trattamento dei dati personali.	**A.13 Sicurezza delle comunicazioni**
Sicurezza della rete / comunicazioni	**O.6**	La rete del sistema informatico dovrebbe essere segregata dalle altre reti del Titolare del trattamento dei dati.	**A.13 Sicurezza delle comunicazioni**
Sicurezza della rete / comunicazioni	**O.7**	L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali pre-autorizzati utilizzando tecniche come il filtro MAC o Network Access Control (NAC)	**A.13 Sicurezza delle comunicazioni**
Back-ups	P.9	Le copie dei backup dovrebbero essere crittografate e archiviate in modo sicuro, anche offline.	A.12.3 Back-Up

Dispositivi Mobili/Portatili	**Q.8**	Per l'accesso ai dispositivi mobili è necessario prendere in considerazione l'autenticazione a due fattori (autenticazione forte)	**A.6.2 Dispositivi mobile e telelavoro**
Dispositivi Mobili/Portatili	**Q.9**	I dati personali memorizzati sul dispositivo mobile (come parte del trattamento dei dati aziendali) dovrebbero essere crittografati.	**A.6.2 Dispositivi mobile e telelavoro**
Cancellazione/Eliminazione dei dati	**S.5**	Dopo la cancellazione del software, dovrebbero essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda del caso, dovrebbe essere considerata anche la distruzione fisica.	**A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**
Cancellazione/Eliminazione dei dati	**S.6**	Se è una terza parte, (quindi un responsabile del trattamento) ad occuparsi della distruzione di supporti o file cartacei, il processo si dovrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento all'esterno dei dati personali.	**A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura**