Nomina a Responsabile interno del trattamento relativo al sistema di videosorveglianza

In conformità alle possibilità offerte dall'articolo 2-quaterdecies del D.Lgs. 196/2003 *"Codice in materia di protezione dei dati personali"* ed alla libertà organizzativa interna prevista dal Regolamento 679/2016/UE il Titolare del trattamento dei dati personali, Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario, attribuisce i seguenti ruoli:

Soggetto	Ruolo	Descrizione	Trattamenti
_____ _____ *(nome del dipendente)*	**RESPONSABILE INTERNO**	Il Responsabile del trattamento di dati personali supervisiona e controlla l'adozione delle misure necessarie messe in atto dal Titolare del trattamento, anche da parte del personale incaricato ai trattamenti di propria competenza. Nello specifico il responsabile è autorizzato a: ➢ visualizzare le immagini in diretta ➢ visualizzare le immagini in tempi differiti ➢ eseguire registrazioni ➢ copiare le registrazioni ➢ cancellare le registrazioni ➢ estrapolare le registrazioni ➢ spostare l'angolo visuale ➢ modificare lo zoom delle telecamere	**Gestione Videosorveglianza e Videocontrollo** per le finalità indicate nelll'art.4 del Regolamento Aziendale

Con la presente il soggetto è autorizzato esclusivamente all'accesso e al trattamento dei dati personali oggetto dei trattamenti sopra indicati, nella misura e nei limiti delle mansioni e del ruolo funzionale svolto presso le strutture ed i locali del Titolare del trattamento.

Il soggetto dichiara di avere ricevuto puntuali indicazioni in merito all'ambito del trattamento dei dati personali consentito, le istruzioni operative e le procedure recanti le modalità di trattamento dei dati personali (ai sensi dell'articolo 29 del Regolamento 679/2016/UE), nello specifico:

- Regolamento 00 - Reg QR 01 “Politica per la sicurezza delle informazioni”;
- Istruzione operativa 00 - IO DA 02 “Istruzioni per il trattamento dei dati personali” e relativo allegato “Introduzione al Regolamento 679/2016/UE”.

Il soggetto dichiara di aver ricevuto l’informativa ai sensi dell'Articolo 13 del Regolamento 679/2016/UE (00 – Mod DA 07).

Il soggetto dichiara inoltre di attenersi rigorosamente alle istruzioni impartite attraverso incontri formativi ed in forma scritta dal Titolare del trattamento dei dati personali.

Secondo quanto disposto dall'articolo 5 paragrafo 1) del Regolamento 679/2016/UE i dati personali oggetto del trattamento devono essere:

- trattati in modo lecito corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il loro utilizzo non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esatti e, se necessario, aggiornati (devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati medesimi sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza di dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti o dalla perdita, dalla distruzione o dal danno accidentali.

La presente lettera di nomina sostituisce ogni precedente atto della stessa natura sottoscritto dall'Incaricato.

La nomina è a tempo indeterminato sino alla revoca del Titolare del trattamento dei dati personali o all'interruzione del rapporto di lavoro, salvo eventuali e/o diversi accordi tra le parti.

Luogo e data _____

Firma del Titolare del Trattamento	**Firma per accettazione del Responsabile**
……	.....

Sistema Socio Sanitario
Regione Lombardia
ASST Valtellina e Alto Lario

Gestione Operativa: Next Generation EU - Qualità e Risk Management

REGOLAMENTO

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

INDICE di REVISIONE	00	
DATA AGGIORNAMENTO	08/02/2023	
DESCRIZIONE MODIFICHE	Emissione	
FASE	**NOMINATIVO**	**Firma**
	S. Ruffoni - SC Affari Generali e Legali	
	A. Panese - Direttore SC Sistemi Informativi Aziendali - Responsabile della Transizione Digitale	
	C. Russo - Referente SIA - Cybersecurity e Piattaforme elettromedicali	
	A. Rossodivita - Direttore SC Gestione Operativa: Next Generation EU – Qualità e Risk Management - Responsabile della sicurezza delle informazioni	
	C. Paganoni - Incarico di Organizzazione Qualità e Risk Management - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management	
PRE-VERIFICA Data ……..	A. Faccinelli - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management	
	C. Paganoni - Incarico di Organizzazione Qualità e Risk Management - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management	
VERIFICA Data…… ….	R. Coppola – DPO aziendale	
	A. Andaloro - Responsabile Servizio Prevenzione e Protezione	
	A. Panese - Direttore SC Sistemi Informativi Aziendali - Responsabile della Transizione Digitale	
	R. Paroli - Direttore SC Gestione Acquisti (Provveditorato – Economato)	
	C. Zanesi – Direttore SC Gestione Tecnico Patrimoniale	
	S. Benedetti - Responsabile SS Trasparenza e Internal Auditing - SC Affari Generali e Legali	
	V. Berta – Responsabile per la tenuta del protocollo informatico della gestione dei flussi documentali e degli archivi	
	A. Rossodivita – Direttore SC Gestione Operativa: Next Generation EU – Qualità e Risk Management - Responsabile della sicurezza delle informazioni	
	C. Cecchini – Responsabile SS Ingegneria Clinica	
	E. Tanzi - Direttore SC Gestione e Sviluppo delle Risorse Umane	
	M. Piazza – Direttore Medico dei Presidi	
APPROVAZIONE DATA……..	A. De Vitis - Direttore Amministrativo	
	G. Ardemagni – Direttore Sanitario	
	P. Formigoni - Direttore Socio Sanitario	

VISTO	T. Saporito - Direttore Generale	

INDICE

Premessa

La mission dell'Azienda Socio Sanitaria Territoriale della Valtellina e dell'Alto Lario (di seguito ASST) è quella di tutelare e promuovere la salute fisica e mentale della popolazione, attraverso l'erogazione dei LEA e degli eventuali livelli aggiuntivi definiti dalla Regione. La ASST assicura la continuità di presa in carico della persona nel proprio contesto di vita e affianca le persone croniche, fragili e le loro famiglie avviando un percorso culturale tra gli operatori che segni il passaggio dalla "cura" al "prendersi cura".

La ASST, consapevole del valore universale della salute, della sua natura di bene pubblico fondamentale e della rilevanza macroeconomica dei servizi sanitari pubblici, in linea con gli assi strategici e le priorità trasversali individuate nel Piano Nazionale di Ripresa e Resilienza (PNRR) [R16], ritiene che la digitalizzazione e l'innovazione dei propri processi e dei servizi erogati rappresentino un fattore determinante per la trasformazione del Paese.

D'altra parte, l'utilizzo pervasivo delle tecnologie dell'informazione e della comunicazione implica l'esposizione della Struttura Sanitaria a rischi cibernetici che devono essere opportunamente gestiti attraverso l'adozione di misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi, contribuendo in tal modo anche ad incrementare il livello comune di sicurezza del Paese, soprattutto alla luce del ruolo della Struttura Sanitaria come Operatore Essenziale nel quadro della normativa NIS [R9][R10].

A tal fine, la ASST adotta un approccio sistematico alla cybersecurity e più in generale alla sicurezza delle informazioni che indirizza un insieme organico e strutturato di misure di sicurezza logica, fisica, organizzativa e procedurale dedicate alla protezione dell'integrità, della riservatezza e della disponibilità delle informazioni e delle reti di comunicazione. L'implementazione di misure di sicurezza adeguate ed efficaci è, quindi, necessaria per garantire anche la sicurezza e la protezione dei dati personali contenuti all'interno del patrimonio informativo dell'ASST. L'approccio alla cybersecurity è, dunque, coerente con il modello organizzativo definito dalla ASST [R38] per assicurare la piena liceità e correttezza nei trattamenti dei dati personali effettuati.

In linea con tale approccio, la presente Politica declina un insieme di regole di base che indirizzano le strategie e le modalità di gestione della sicurezza delle informazioni della ASST, stabilendo:

- gli obiettivi di sicurezza;
- l'ambito di applicazione e i destinatari della Politica di Sicurezza;
- il modello organizzativo e gestionale definito per garantire la sicurezza delle informazioni;
- lo Statement formale e le contromisure logiche, fisiche o organizzative necessarie per la concreta realizzazione degli obiettivi di sicurezza prefissati;
- il sistema documentale inerente alla sicurezza delle informazioni.

Titolo I - Introduzione

Art. 1) Scopo del documento

1. Il presente documento descrive la Politica per la Sicurezza delle Informazioni della ASST, intesa come l'insieme delle regole volte ad indirizzare una corretta gestione della sicurezza del Patrimonio Informativo, al fine di contenere i rischi di compromissione della riservatezza, dell'integrità e della disponibilità degli asset informativi, sia in un'ottica di tutela della missione istituzionale che di contrasto agli eventi accidentali o di natura criminosa.

Art. 2) Campo di applicazione

1. La presente Politica è valida per l'intera ASST e si applica a tutte le informazioni trattate in qualsiasi modo e qualsiasi formato, a tutti i sistemi di gestione e supporti di memorizzazione utilizzati per il loro trattamento e conservazione.
2. Le informazioni oggetto di protezione si riferiscono, a titolo esemplificativo e non esaustivo, ai seguenti ambiti:
   a) informazioni associate ai servizi istituzionali erogati e in via di sviluppo;
   b) know-how strategico;
   c) informazioni contabili e finanziarie;
   d) informazioni condivise con gli stakeholder, le Agenzie e le Amministrazioni governative;
   e) dati personali del personale della ASST, clienti e soggetti terzi, con riferimento al GDPR [R1], alla normativa nazionale attuativa [R2] ed ai Provvedimenti del Garante per la protezione dei dati personali;
   f) informazioni relative al pubblico che interagisce con la ASST;
   g) informazioni inerenti ai processi di procurement e di gestione dei progetti/contratti;
   h) informazioni legate alla gestione dei servizi e dei sistemi dedicati alla sicurezza ICT;
   i) informazioni trattate nell'ambito dei servizi essenziali di pertinenza della ASST [R9][R10][R11].
3. Le risorse cartacee ed informatiche utilizzate per l'elaborazione e la custodia delle informazioni, alle quali si indirizzano gli interventi di tutela, possono comprendere:
   a) documentazione tecnica o altri documenti contenenti le informazioni della ASST;
   b) procedure operative o di supporto;
   c) piattaforme hardware e software, incluse quelle che supportano i dispositivi elettromedicali;
   d) infrastrutture di rete e di telecomunicazione;
   e) banche dati;
   f) applicazioni gestionali e di supporto all'erogazione dei servizi;
   g) supporti di memorizzazione utilizzati per la conservazione dei dati.
4. Le Informazioni, le risorse informatiche, i supporti digitali e cartacei di archiviazione, costituiscono le cosiddette "Risorse Informative della ASST". Le Risorse Informative devono essere protette durante l'intero ciclo di vita fino al momento della loro dismissione.

5. Le regole di seguito descritte sono in vigore a partire dalla data di emissione del presente documento, ma per particolari ambiti, definiti nel presente documento, diverranno effettivi secondo un piano e relativo cronoprogramma di realizzazione, condiviso con i differenti responsabili delle parti interessate, e che verrà dettagliato in un modulo allegato.
6. Sono ammesse deroghe alle regole riportate nel presente documento, solo nei casi in cui ne sia valutato ed accettato il rischio derivante da parte della Direzione della ASST, con autorizzazione da parte della Direzione stessa.

Art. 3) Definizioni e acronimi

1. Ai fini dell'applicazione della presente Politica devono intendersi le seguenti definizioni:
   a) **Agenzia per la cybersicurezza nazionale**: l'Agenzia istituita a tutela degli interessi nazionali nel campo della cybersicurezza, di cui all'articolo 5 del decreto-legge 14 giugno 2021, n. 82 [R18].
   b) **Cybersecurity**: l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza.
   c) **Collaboratore esterno**: persona fisica che collabora con la ASST in forza di un contratto libero professionale.
   d) **CSIRT Italia**: il Computer Security Incident Response Team, di cui all'articolo 8 del decreto legislativo NIS [R10].
   e) **Decreto-legge:** il decreto-legge 14 giugno 2021, n. 82 [R18].
   f) **Decreto legislativo NIS**: il decreto legislativo 18 maggio 2018, n. 65 [R10].
   g) **Dato Personale**:dato personale ai sensi del GDPR [R1]: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
   h) **Direttiva NIS :** Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione [R9], recepita in Italia con il decreto legislativo 18 maggio 2018, n.65 [R10].
   i) **Operatore di Servizi Essenziali:** soggetto pubblico o privato, della tipologia di cui all'allegato II al decreto legislativo 18 maggio 2018, n. 65 [R10], che soddisfa i criteri di cui all'articolo 4, comma 2, de medesimo decreto.
   j) **Personale :** dipendente o assimilabile (es. contratti atipici).
   k) **Strategia nazionale di sicurezza cibernetica:** la strategia di cui all'articolo 6 del decreto legislativo NIS [R10].
   l) **Soggetti terzi:** Fornitori, consulenti, collaboratori esterni, partner che operano con la ASST in forza di un contratto.
   m) **Risorse Informative:** cfr. Art. 2) comma 4.

2. Ai fini dell'applicazione della presente Politica devono intendersi i seguenti acronimi:
    a) **ACN**:Agenzia per la cybersicurezza nazionale.
    b) **ASST:** Azienda Socio Sanitaria Territoriale della Valtellina e dell'Alto Lario.
    c) **AgID:** Agenzia per l'Italia Digitale.
    d) **BCP:** Business Continuity Plan.
    e) **CCNL:** Contratto Collettivo Nazionale di Lavoro.
    f) **CSIRT:** Computer Security Incident Response Team.
    g) **LEA:** Livelli Essenziali di Assistenza.
    h) **NIS:** Network and Information Security.
    i) **OSE:** Operatore di Sevizi Essenziali.
    j) **PNRR:** Piano Nazionale di Ripresa e Resilienza.
    k) **RAEE**: Rifiuti e Apparecchiature Elettriche ed Elettroniche

Titolo II - Obiettivi di sicurezza

Art. 4) Obiettivi per la sicurezza delle informazioni

1. Considerando la missione istituzionale ed il quadro normativo di riferimento, la ASST si pone come obiettivo la salvaguardia di:
   a) la riservatezza delle informazioni, da attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle informazioni o la diffusione non controllata delle stesse;
   b) l'integrità delle informazioni, da attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico delle informazioni;
   c) la disponibilità delle informazioni, da attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse informatiche in tempi utili al compimento della propria missione.
2. Nello specifico la ASST deve, in via prioritaria:
   a) definire e applicare un processo di governance della sicurezza delle informazioni, che sia in grado di indirizzare le strategie di trattamento dei rischi in funzione dei cambiamenti derivanti dall'insorgere di nuovi scenari di minaccia, nuove tipologie di vulnerabilità, nuovi fattori di rischio derivanti anche dai cambiamenti organizzativi;
   b) definire e applicare un processo per l'analisi, la valutazione ed il trattamento dei rischi legati alla cybersecurity;
   c) prevedere, a tendere, l'integrazione tra il quadro di riferimento organizzativo e metodologico per l'analisi dei rischi legati alla cybersecurity e gli altri sistemi di gestione dei rischi della ASST, in modo da garantire una gestione e una valutazione unitaria dei rischi connessi ai servizi istituzionali della ASST;
   d) definire ed applicare un processo di gestione degli allarmi e degli incidenti di sicurezza informatica, che sia allineato e coerente con la procedura definita ed adottata dall'ASST per la gestione dei *data breach*;
   e) garantire al personale e ai soggetti terzi un'adeguata conoscenza e un grado di consapevolezza:
      - delle problematiche connesse alla sicurezza in termini di minacce, impatti e rischi derivanti da compromissioni della riservatezza, integrità e disponibilità del patrimonio informativo della ASST;
      - delle regole tecniche ed organizzative per l'utilizzo in sicurezza dei sistemi informativi della ASST;
      - delle procedure di rilevamento e segnalazione di eventi anomali o sospette violazioni della sicurezza informatica;
      - della normativa applicabile in materia di protezione dei dati personali [R1] e delle relative implicazioni, nonché delle modalità di applicazione delle misure previste dalla normativa nonché dalle procedure/istruzioni contenute all'interno del Modello Organizzativo Privacy dell'ASST;

f) garantire la conformità ai requisiti cogenti derivanti da normative di legge, dagli standard internazionali e dalle principali best practice di settore;

g) garantire il rispetto della politica per la sicurezza delle informazioni adottata dalla ASST.

Titolo III - Organizzazione e responsabilità

Art. 5) Organizzazione e responsabilità per la sicurezza delle informazioni

1. L'organizzazione è funzionale all'individuazione delle politiche dirette alla gestione e al controllo delle misure di sicurezza adottate e si concretizza nella definizione di ruoli, funzioni e responsabilità che concorrono alla realizzazione ed alla gestione del sistema di sicurezza delle informazioni, tenendo conto anche del ruolo della ASST come infrastruttura critica nel settore di riferimento e all'interno della filiera produttiva.
2. La ASST si impegna a definire specifici ruoli e responsabilità per la sicurezza delle informazioni, ad attribuirli alle diverse strutture organizzative interne e a comunicarli affinché siano pienamente compresi ed attuati.
3. I compiti e le aree di responsabilità in conflitto tra loro devono essere separati per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset della ASST.
4. Nella definizione delle responsabilità associate ai ruoli devono essere previste le attività di gestione dei contatti con le autorità nazionali ed internazionali e con gruppi specialistici e associazioni professionali pertinenti alla sicurezza delle informazioni, nonché le attività di gestione della sicurezza delle informazioni nell'ambito dei progetti.

Titolo IV - Valutazione dei rischi

Art. 6) Scenari di minaccia

1. Il progressivo e crescente ricorso alle tecnologie digitali delinea nuovi scenari di minaccia alla cybersecurity che potrebbero compromettere il corretto svolgimento dei servizi, l'integrità degli asset infrastrutturali e determinare violazioni dei diritti e delle libertà delle persone fisiche.
2. D'altra parte, le filiere di approvvigionamento (supply chain) possono a loro volta introdurre nuove minacce e talvolta aumentare il livello di complessità delle azioni di contrasto alle minacce, nonché rallentarne i tempi di attuazione.
3. La ASST ritiene pertanto fondamentale realizzare un processo di valutazione dei rischi legati alla cybersecurity (di seguito anche rischi cyber) ed alla supply chain, individuando allo stesso tempo le opportune procedure di gestione e riduzione di tali rischi.

Capo I - Rischi legati alla cybersecurity

Art. 7) Principi generali

1. Il processo di valutazione dei rischi cyber e la corrispondente metodologia, affinché siano allineati ai principali standard di riferimento e consentano di ottenere risultati utili, affidabili e rappresentativi della realtà del contesto analizzato, devono soddisfare i seguenti principi generali:
   a) **Ripetibilità e riproducibilità** - Uno dei risultati del processo di valutazione del rischio cyber è la misurazione del rischio. Tale operazione richiede di essere ripetibile, vale a dire, a parità di ogni altra condizione, si devono ottenere i medesimi risultati, anche in tempi successivi. Da qui la necessità di documentare il metodo utilizzato e almeno le principali assunzioni e semplificazioni.
   b) **Comprensibilità** - I criteri adottati nell'espressione dei parametri che compongono il rischio (probabilità di accadimento, valore delle informazioni, etc.) e i risultati prodotti devono essere logici e trasparenti, al fine di consentire il riutilizzo dei risultati nella ripetizione del processo di valutazione del rischio cyber.
   c) **Condivisione** - Il processo di valutazione del rischio cyber deve essere stabilito, gestito e concordato tra i responsabili della ASST (c.d. stakeholder) ed i valori attribuiti alle informazioni devono essere condivisi tra le diverse Strutture della ASST interessate.
   d) **Coerenza** - I valori attribuiti alle informazioni devono essere coerenti con quanto stabilito dalle politiche di sicurezza di alto livello della ASST.
   e) **Riutilizzabilità** - I risultati del processo di valutazione del rischio cyber, intermedi o finali, devono poter essere riutilizzabili nel caso in cui l'attività vada ripetuta a seguito di variazioni delle condizioni (valori delle informazioni, minacce, vulnerabilità, etc.) che ne hanno determinato l'esecuzione, anche al fine di realizzare economie di scala. Inoltre, è importante evidenziare che la revisione dell'analisi dei rischi contribuisce all'attuazione del concetto di miglioramento continuo e della sua misurazione. Se necessario, i parametri che definiscono le minacce, così come le vulnerabilità, possono essere ampliati in funzione delle variazioni del contesto di analisi, delle risorse impiegate e delle terze parti che entrano in contatto, per finalità diverse, con l'ambito dell'analisi.

f) **Fattibilità in termini temporali** - Le attività correlate al processo di valutazione del rischio cyber devono fornire i risultati in tempi utili, legati ad esempio, al livello di criticità del servizio oggetto di analisi ed al suo ciclo di vita, oppure commisurati con il livello di rischio e/o con il budget allocato secondo anche le regole di sistema.

g) **Adeguatezza al livello di consapevolezza dell'Organizzazione** - La complessità di una metodologia per la valutazione del rischio cyber deve essere adeguata al livello di consapevolezza esistente nella ASST sui temi relativi alla sicurezza delle informazioni, per evitare gli insuccessi derivanti dall'introduzione di sistemi di gestione e processi non recepiti e lasciati allo stato di evento occasionale, avulso dalla cultura interna alla ASST. In considerazione della complessità di tale politica e della sua applicabilità, si ritiene che tale politica e l'adeguamento del livello di consapevolezza richiederà un percorso di implementazione, attraverso la redazione di un piano attuativo dedicato, della durata stimata di 5 anni, dall'entrata in vigore del presente documento.

Art. 8) Processo

1. Il processo di valutazione del rischio cyber, in linea con quanto previsto dai principali standard ISO applicabili in materia [R24][R28] e con il Framework Nazionale per la Cybersecurity e la Data Protection [R20], deve essere costituito da un insieme di attività ben definite, da compiersi in sequenza ordinata, nell'ambito delle seguenti macro-fasi:

   a) **Context Establishment:** identificazione dell'ambito, dei confini e dell'organizzazione a supporto del processo di valutazione del rischio cyber;

   b) **Risk Assessment:** analisi e valutazione del rischio, che a sua volta deve prevedere le seguenti attività:

      - identificazione e documentazione delle vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione;
      - identificazione e valutazione delle minacce, sia interne che esterne e le relative probabilità di accadimento;
      - identificazione e valutazione dei potenziali impatti sulla mission istituzionale della ASST;
      - valutazione del rischio in base a quanto emerso dai suddetti punti.

      Ai fini della identificazione e valutazione delle minacce e delle vulnerabilità la ASST deve organizzarsi in modo da ricevere informazioni su minacce, vulnerabilità ed altri dati configurabili come Cyber Threat Intelligence da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing).

   c) **Risk Treatment:** definizione delle strategie per la gestione del rischio e definizione delle modalità operative per l'implementazione delle misure di sicurezza adeguate alla copertura dei rischi rilevati, che a sua volta deve prevedere le seguenti attività:

      - identificazione e comunicazione del livello di rischio tollerato;
      - definizione strategia di trattamento del rischio, con identificazione e prioritizzazione delle misure tecniche ed organizzative necessarie per contenere il rischio valutato entro la soglia di accettazione definita dalla ASST o soddisfare requisiti di compliance normativa non ancora pienamente soddisfatti.

2. Una caratteristica fondamentale dell'attività di valutazione del rischio cyber è che deve configurarsi come un processo continuo, da cui desumere le azioni da implementare per una

gestione del rischio consapevole, adeguata ai valori da proteggere (in termini di informazioni o servizi erogati dal sistema informativo) ed in linea, sul piano temporale, con i mutamenti ambientali e tecnologici.

Art. 9) Rischio tollerato

1. Con riferimento al rischio cyber tollerato, la ASST, tenendo conto del ruolo dell'Organizzazione come Operatore Essenziale ai sensi della Direttiva NIS [R9] e dei rischi specifici presenti nel settore di appartenenza, ha individuato in un livello basso su una scala di valori a tre livelli (Basso, Medio, Alto), la soglia di rischio accettabile, rispetto alla riservatezza, alla integrità e alla disponibilità delle informazioni.
2. Il livello di rischio tollerato implica che sugli asset esposti a livelli di rischio inferiori o uguali a tale soglia, non sia richiesta l'implementazione di misure di sicurezza specifiche ulteriori rispetto a quanto previsto dalle politiche adottate dall'Ente, dai requisiti normativi e contrattuali e dalle best practice internazionali.
3. Il rispetto delle politiche e dei requisiti normativi, infatti, risulta indipendente dalle attività di analisi del rischio e definisce quindi un insieme minimo di misure di sicurezza.
4. Nell'ambito delle specifiche analisi del rischio su servizi o applicazioni possono essere stabilite soglie di rischio accettato diverse da quelle esplicitate nel presente documento, solo in caso di deroga autorizzata dalla ASST per comprovate esigenze.

Capo II - Rischi legati alla supply chain

Art. 10) Processi di gestione del rischio inerenti alla catena di approvvigionamento cyber

1. La ASST deve inoltre definire ed implementare i processi di gestione del rischio inerenti alla catena di approvvigionamento cyber.
2. A tal fine i soggetti terzi che forniscono sistemi informatici, componenti e servizi ICT devono essere identificati, prioritizzati e valutati regolarmente da parte della ASST tramite attività di audit, verifica, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali (cfr. Art. 26).
3. Inoltre, i suddetti soggetti terzi devono essere opportunamente coinvolti nelle attività di pianificazione e verifica della risposta e del ripristino agli incidenti aventi impatto sulla sicurezza e sulla continuità operativa dei servizi erogati dalla ASST (cfr. Capo VIII - Capo IX -).

Titolo V - Controlli di sicurezza

Art. 11) Controlli di sicurezza delle informazioni

1. La ASST ritiene che la sicurezza delle informazioni si ottenga implementando un insieme adeguato e coerente di controlli organizzativi e tecnologici.
2. Di seguito sono formalmente declinati i controlli che costituiscono la presente politica, da attuare per il raggiungimento degli obiettivi di sicurezza definiti dalla ASST (cfr. Titolo II -), in base al contesto specifico di riferimento.
3. I controlli sono organizzati in funzione dell'ambito della sicurezza delle informazioni che indirizzano.
4. Tale politica richiederà per l'attuazione la realizzazione di un piano strategico dedicato di attuazione della durata complessiva stimata di 5 anni, nell'ambito del quale verranno declinate tempistiche, interventi di implementazione crescenti e progressivi, ruoli e responsabilità di realizzazione secondo un cronoprogramma predefinito.

Capo I - Sicurezza delle risorse informative

Art. 12) Risorse informative

1. Tutte le Risorse Informative della ASST (cfr. Art. 2) costituiscono un valore strategico per l'organizzazione e come tali devono essere adeguatamente protette.
2. Nell'ambito delle Risorse Informative, l'informazione assume un ruolo d'importanza primaria costituendo una risorsa critica immateriale, necessaria ai processi di pianificazione, organizzazione, esecuzione e controllo delle attività condotte dalla ASST.

Art. 13) Inventario degli asset

1. L'inventario delle risorse informative è necessario per monitorare l'obsolescenza delle risorse utilizzate, pianificare il loro ammodernamento, rinnovare le licenze e programmare gli investimenti in tecnologie dell'informazione.
2. L'inventario deve comprendere:
    a) **Informazioni:** database e archivi cartacei, documentazione di sistema, manuali per l'utente, materiale per l'addestramento, procedure operative o di supporto, piani di continuità, ecc.;
    b) **Risorse software:** software di base ed applicativo, strumenti di sviluppo, programmi di utilità, ecc.;
    c) **Risorse hardware:** apparecchiature informatiche (ad es. server fisici e virtuali, client fissi e portatili, monitor, sistemi di backup e restore, ecc.), apparecchiature di comunicazione (ad es. router, fax, segreterie telefoniche, ecc.), supporti magnetici (ad es. nastri e dischi), altre apparecchiature tecniche (ad es. alimentazioni elettriche, unità di climatizzazione, ecc.);
    d) **Sistemi informativi esterni** all'organizzazione utilizzati nell'ambito della ASST (ad es. cloud);
    e) **Flussi di dati e comunicazioni** inerenti all'organizzazione;

f) **Locali:** i luoghi fisici ove sono custodite le informazioni, le risorse software e hardware e dove vengono effettuate le elaborazioni;

g) **Capitale umano:** personale e soggetti terzi che operano presso la ASST.

3. A tal fine deve essere predisposto e mantenuto aggiornato un inventario delle principali Risorse Informative che includa tutti i suddetti asset. Inoltre, a tali asset devono essere associati i relativi servizi erogati dalla ASST, con specifica indicazione di quelli ritenuti essenziali ai sensi della Direttiva NIS [R9] e delle Linee Guida emesse dall'Autorità NIS-Settore Salute [R11].
4. Infine, devono essere identificati e catalogati tutti i trattamenti di dati personali effettuati dalla ASST ai sensi del GDPR [R1] (Registri dei trattamenti di dati personali).
5. Tutte le Risorse Informative sono di proprietà della ASST, a cui è riservato ogni diritto ai sensi della normativa vigente sulla Protezione del diritto d'autore, laddove applicabile.
6. La riproduzione, la pubblicazione e la distribuzione, totale o parziale, delle Risorse Informative sono espressamente vietate in assenza di una autorizzazione scritta da parte del proprietario.
7. L'inventario degli asset già iniziato, diversificato per l'aspetto informatico e quello cartaceo, richiederà per la completa realizzazione dell'intero processo un arco temporale non inferiore ai 5 anni (vedasi piano attuativo allegato).

Art. 14) Utilizzo degli asset

1. Il personale utilizza le Risorse Informative di proprietà della ASST nei limiti dell'autorizzazione assegnata e per esclusive finalità lavorative.
2. Tale utilizzo deve sempre ispirarsi ai principi di diligenza, correttezza e riservatezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto professionale, in coerenza con le vigenti normative, e tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.
3. La ASST, ammette l'uso degli strumenti informatici, ed in particolare di Internet, per motivi personali soltanto in caso di urgenza e comunque non in modo ripetuto e per periodi di tempo brevi, e in ogni caso sempre nel rispetto del principio di riservatezza e delle esigenze di funzionalità della rete e di semplificazione dei processi lavorativi.
4. La ASST perseguirà a norma di legge e del vigente contratto di lavoro, il personale che utilizza in modo non appropriato i sistemi di elaborazione delle informazioni, poiché l'eventuale esposizione al rischio impedirebbe alla ASST il corretto svolgimento delle proprie attività istituzionali ed il rispetto delle normative cogenti applicabili.
5. A tal fine devono essere predisposte idonee istruzioni per il personale, contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche derivanti, in caso di inosservanza.

Art. 15) Classificazione e trattamento delle informazioni

1. Le informazioni trattate nell'ambito delle attività della ASST devono essere tutelate e gestite sulla base del loro valore in termini di impatti derivanti dalla perdita della disponibilità, integrità e riservatezza delle stesse.
2. Tutte le informazioni trattate dalla ASST devono essere classificate attribuendo alle stesse un grado di criticità utile a determinarne il livello di protezione.

3. La protezione deve riguardare tutte le fasi connesse alla gestione dell'informazione: generazione, raccolta, classificazione, emissione, oscuramento ove previsto dalle norme (cfr. ad esempio [R13][R14] e s.m.i.), ricezione, custodia, divulgazione, consultazione, riclassificazione, modifica, conservazione e distruzione.
4. A tal fine, devono essere predisposte dalla ASST adeguate politiche contenenti, in conformità alle esigenze istituzionali ed alla normativa vigente in materia di tutela del trattamento dei dati personali [R1]:
   a) i criteri per la classificazione delle informazioni;
   b) le misure minime di sicurezza da adottare per il trattamento delle informazioni classificate e la relativa etichettatura.

Art. 16) Assegnazione di priorità agli asset

1. Gli asset della ASST (cfr. Art. 13) devono essere prioritizzati in base alla classificazione (cfr. Art. 15), criticità e valore per la mission dell'organizzazione, delle informazioni da essi trattate.
2. Inoltre, devono essere identificate e rese note le interdipendenze e le funzioni fondamentali per la fornitura di servizi critici.

Art. 17) Utilizzo di supporti e dispositivi informatici della ASST per la memorizzazione

1. La memorizzazione delle informazioni deve essere effettuata utilizzando le applicazioni istituzionali preposte (es. Sharepoint, OneDrive) ed è pertanto necessario limitare la memorizzazione di informazioni su supporti e dispositivi informatici della ASST (dischi locali del PC, memorie esterne, ecc.).
2. È comunque necessario regolamentare la memorizzazione di informazioni su supporti e dispositivi informatici della ASST (dischi locali del PC, memorie esterne, ecc.) prevedendo un processo formale di autorizzazione nel caso di memorizzazione di dati personali ai sensi del GDPR [R1] o critici della ASST.
3. Inoltre, i supporti e i dispositivi informatici della ASST per la memorizzazione, incluse le memorie esterne (es. cd rom, dvd, hard disk portatili, chiavi USB), devono essere protetti dai rischi di accesso non autorizzato e/o manomissioni, in funzione della classificazione delle informazioni in essi contenuti.

Art. 18) Utilizzo di supporti e dispositivi personali

1. Non è consentito l'utilizzo di supporti e dispositivi personali ai fini dello svolgimento dell'attività lavorativa, fatto salvo situazioni specifiche che dovranno essere di volta in volta autorizzate dalla ASST valutandone il rischio derivante.

Art. 19) Lavoro da remoto

1. La ASST è consapevole che il lavoro da remoto può risultare fondamentale per favorire l'efficienza e l'efficacia delle attività in particolari situazioni aziendali e sociosanitarie.
2. Tuttavia, tale modalità può comportare rischi anche significativi per la sicurezza delle informazioni della ASST e pertanto deve essere opportunamente regolamentato, nel rispetto di quanto consentito dalla legge vigente e dai contratti di lavoro.

Capo II - Sicurezza nell'ambito delle risorse umane

Art. 20) Individuazione del personale

1. Tutto il personale della ASST ed i collaboratori esterni, con particolare riferimento a quelli destinati a ricoprire ruoli di gestione della sicurezza, devono essere attentamente individuati, in funzione delle esigenze istituzionali della ASST e sulla base di criteri di affidabilità e competenza professionale.
2. Una volta individuato il personale si procederà ad assegnare i compiti al personale dedicato alla sicurezza delle informazioni, oltre alla struttura organizzativa di appartenenza, specifici ruoli operativi e profili professionali, previo adeguato percorso formativo ad hoc.

Art. 21) Responsabilità del personale e dei collaboratori esterni

1. Tutto il personale e i collaboratori esterni devono essere informati delle proprie responsabilità, anche giuridiche, derivanti da violazioni, frodi o dall'utilizzo improprio delle Risorse Informative della ASST, nonché da uno scorretto trattamento delle informazioni e dei dati personali.
2. I rapporti interpersonali ed i comportamenti, a tutti i livelli organizzativi, devono essere improntati a principi di onestà, correttezza, trasparenza, riservatezza, imparzialità, diligenza, lealtà e reciproco rispetto (per il personale si rimanda al Contratto Collettivo Nazionale di Lavoro, al Regolamento recante codice di comportamento dei dipendenti pubblici [R32], ai codici deontologici dei rispettivi ordini professionali ed al Regolamento per i procedimenti disciplinari relativi al personale dipendente del comparto della dirigenza della ASST [R37], mentre per i collaboratori esterni ai contratti individuali).

Art. 22) Sensibilizzazione e formazione

1. Tutto il personale ed i collaboratori esterni devono essere adeguatamente informati e sensibilizzati in merito alle politiche e alle procedure operative di sicurezza pertinenti alla propria attività lavorativa.
2. In particolare, devono essere definiti, erogati e aggiornati piani formativi mirati ad accrescere il grado di consapevolezza e di sensibilizzazione sugli obiettivi di sicurezza prefissati e sulle principali problematiche di sicurezza delle informazioni.
3. I piani di formazione devono prevedere un approfondimento specifico su:
   a) politiche, procedure e linee guida di sicurezza adottate dalla ASST;
   b) ruoli organizzativi previsti per la gestione delle tematiche di sicurezza delle informazioni, responsabilità del personale coinvolto e principali implicazioni di eventuali non conformità sulla sicurezza delle risorse della ASST;
   c) principali tematiche e controlli di sicurezza delle informazioni, inclusa la cybersecurity.

Art. 23) Cessazione e variazione del rapporto di lavoro

1. Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o variazione del rapporto di lavoro devono essere definiti, comunicati al personale ed ai collaboratori esterni e resi effettivi.

Capo III - Sicurezza nelle relazioni con i soggetti terzi

Art. 24) Controlli generali

1. Tutti i soggetti terzi devono essere informati delle proprie responsabilità, anche giuridiche, derivanti da violazioni della sicurezza o dall'utilizzo improprio delle Risorse Informative della ASST, qualora l'attività individuata possa comportare l'accesso a tali risorse.
2. È necessario garantire la sicurezza delle Risorse Informative accedute ed utilizzate anche dai soggetti terzi che a qualsiasi titolo, svolgono, anche temporaneamente, attività di lavoro per la ASST.
3. La ASST, come evidenziato nelle Linee Guida per la sicurezza nel procurement ICT [R31], è consapevole che i soggetti terzi in relazione alla natura dei servizi offerti, possono accedere al patrimonio informativo della ASST, introducendo potenziali rischi cyber in grado di vanificare, o comunque rendere meno efficaci, le misure prese dalla ASST per tutelare il proprio patrimonio informativo. Risulta pertanto fondamentale definire ed attuare procedure per garantire la sicurezza delle informazioni in relazione all'approvvigionamento di beni e servizi informatici (procurement ICT) che indirizzino tutte le fasi di approvvigionamento (prima, durante e dopo).
4. È necessario garantire la sicurezza delle Risorse Informative rese disponibili all'utilizzo da parte di soggetti terzi ai fini dell'esecuzione degli specifici obblighi contrattuali e nei limiti dell'autorizzazione assegnata.
5. A tal fine, devono essere predisposte:
    a) adeguate politiche e procedure contenenti i criteri e le modalità per la gestione delle Risorse Informative da parte dei soggetti terzi, in conformità alle esigenze istituzionali ed alle normative vigenti. Tali politiche e procedure devono risultare adeguate rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle Risorse Informative della ASST;
    b) idonee istruzioni contenenti indicazioni circa le modalità di corretto utilizzo delle Risorse Informative nonché le responsabilità, anche giuridiche, derivanti in caso di inosservanza.
    c) Il miglioramento e potenziamento di tali politiche e procedure richiederà un arco temporale stimato di 3 anni (vedasi piano attuativo allegato).

Art. 25) Clausole Contrattuali

1. Devono essere previste specifiche clausole per garantire la riservatezza e la non-divulgazione delle informazioni della ASST accedute ed utilizzate dai soggetti terzi, secondo quanto previsto dalle normative vigenti.
2. Gli accordi con i soggetti terzi devono necessariamente contemplare tutti i requisiti necessari ad assicurare la protezione delle Risorse Informative della ASST e devono indirizzare l'intera catena di approvvigionamento a garanzia del mantenimento della sicurezza delle informazioni in tutte le fasi.
3. Inoltre, i soggetti terzi devono essere informati sulle politiche, le procedure e le istruzioni di sicurezza della ASST relativamente al tipo di attività previste dal contratto.
4. Il miglioramento e potenziamento richiederà un arco temporale stimato di 3 anni (vedasi piano attuativo allegato).

Art. 26) Monitoraggio, revisione e gestione del cambiamento dei servizi delle terze parti

1. I servizi delle terze parti devono essere regolarmente monitorati, riesaminati e verificati al fine di rilevare scostamenti rispetto agli accordi contrattuali nonché gestire eventuali cambiamenti alla fornitura di tali servizi (in occasione ad esempio di interventi migliorativi, cambiamenti tecnologici o delle politiche e delle procedure di sicurezza, rivalutazione dei rischi).
2. Il miglioramento e potenziamento richiederà un arco temporale stimato di 3 anni (vedasi piano attuativo allegato).

Art. 27) Sicurezza delle informazioni per l'utilizzo dei servizi cloud

1. Devono altresì essere definite politiche specifiche e relativi processi atti ad indirizzare e gestire la sicurezza delle informazioni lungo tutto il ciclo di vita dei servizi cloud.

Capo IV - Sicurezza fisica e ambientale

Art. 28) Protezione da minacce di tipo fisico ed ambientale

1. Tutte le Risorse Informative, cartacee ed informatiche, della ASST devono essere protette dai rischi di accesso non autorizzato, sottrazione, manomissioni e danneggiamento derivanti da minacce di tipo fisico ed ambientale.
2. Saranno progettati ed implementati sistemi di sicurezza fisica per la protezione delle aree, degli uffici, delle stanze e degli impianti dai danni derivanti da incendi, allagamenti, esplosioni ed altre forme di disastro naturale o umano, in coerenza con le risorse tecnico-strutturali, economiche e logistiche aziendali.
3. I sistemi di sicurezza adottati devono essere regolarmente verificati e manutenuti.
4. Devono essere predisposte idonee procedure organizzative per la regolamentazione ed il controllo dell'accesso ai sistemi informatici da parte del personale e dei soggetti terzi autorizzati alla gestione/manutenzione degli stessi.
5. Il miglioramento e potenziamento richiederà per la realizzazione un arco temporale di 5 anni (vedasi piano attuativo allegato).

Art. 29) Sicurezza delle aree

1. Il perimetro di sicurezza delle aree contenenti le informazioni critiche e le strutture di elaborazione delle informazioni deve essere chiaramente definito e controllato.
2. Quando non presidiate, le aree devono essere tenute chiuse e controllate periodicamente.

Art. 30) Controllo degli accessi fisici

1. Tutte le risorse informative devono essere ubicate prevalentemente in edifici con accesso a personale preventivamente autorizzato. L'accesso fisico a tali strutture deve essere controllato e consentito solo al personale e agli eventuali soggetti terzi e visitatori preventivamente identificati ed autorizzati, solo per i compiti specifici e limitati alle attività di competenza.
2. Il personale che fornisce servizi di supporto e di manutenzione è autorizzato all'accesso nelle aree laddove necessario e in maniera limitata (anche temporalmente).
3. I diritti di accesso devono essere regolarmente verificati e revocati al personale ed ai soggetti terzi che lasciano gli incarichi per i quali era previsto l'ingresso alle aree stesse.

4. A tal fine:
    a) devono essere predisposte idonee procedure per la regolamentazione ed il controllo degli accessi alle aree e ai locali della ASST;
    b) devono essere previste “aree ad accesso ristretto”, ove necessario alla luce dei potenziali rischi per la sicurezza delle informazioni, dove l’ammissione è consentita solo in presenza di personale autorizzato (ad es. locali ove risiedono i sistemi server e le apparecchiature di rete, quelli dedicati alla medicina nucleare e risonanza magnetica, laboratori di analisi, archivi cartelle cliniche, ecc.).

Art. 31) Sicurezza degli uffici, delle stanze e degli strumenti di lavoro

1. Gli uffici e le stanze devono essere protetti in funzione della classificazione delle risorse informative ivi trattate e custodite (cfr. Art. 15).
2. L’accesso agli uffici ed alle stanze deve essere consentito solo al personale autorizzato, ai soggetti terzi ed ai visitatori preventivamente identificati.
3. Gli strumenti di lavoro devono essere fisicamente protetti dai rischi di accesso non autorizzato e da conseguenti manomissioni o furti.
4. Saranno predisposte idonee procedure organizzative per la regolamentazione ed il controllo degli accessi agli strumenti da parte del personale e dei soggetti terzi autorizzati alla gestione/manutenzione degli stessi.

Art. 32) Lavorare in aree sensibili

1. Devono essere progettati ed implementati idonei sistemi di sicurezza fisica per la protezione ed il controllo delle aree sensibili, qualora identificate.
2. Devono essere definite procedure organizzative per la gestione dell’accesso alle aree sensibili da parte del personale, dei soggetti terzi ed eventuali visitatori.
3. Devono essere altresì definite, linee guida ed istruzioni per la regolamentazione delle attività lavorative e dell’utilizzo delle risorse informative all’interno delle aree sensibili. Tali attività necessiteranno per la realizzazione completa di un arco temporale non inferiore a 5 anni (vedasi piano attuativo allegato).

Art. 33) Sicurezza delle aree di carico e scarico

1. Le aree di carico e scarico dei materiali, laddove presenti, devono essere controllate ed isolate dagli ambienti operativi e di elaborazione delle informazioni.
2. Le porte di accesso alle aree di carico e scarico dovranno essere sorvegliate e se possibile allarmate.
3. L’accesso alle suddette aree deve essere limitato al personale ed ai soggetti terzi previamente identificati e autorizzati.
4. Tutto il materiale in uscita ed in arrivo deve essere sempre registrato all'entrata. Il materiale in arrivo deve essere sempre possibilmente esaminato prima di venire trasportato dall'area di carico e scarico al punto di utilizzo.

Art. 34) Equipaggiamento di sicurezza

1. Tutti i locali della sala server aziendali della ASST devono essere dotati di equipaggiamento di sicurezza come rilevatori di fumo e di fiamme, allarmi antincendio, controllo delle

temperature, attrezzature per l'estinzione di incendi, uscite di sicurezza, sistemi antiallagamento e sistemi di protezione dalle interferenze nella fornitura elettrica.

2. Tali equipaggiamenti devono essere controllati periodicamente per accertarne lo stato di conservazione e l'efficienza seguendo le istruzioni dei costruttori e dei responsabili preposti.
3. Tutte le informazioni sulla collocazione degli equipaggiamenti devono essere riportate su planimetrie opportunamente dislocate nelle aree comuni.
4. Tutto il personale e gli eventuali soggetti terzi devono essere istruiti all'uso di tali equipaggiamenti. Le procedure di emergenza devono essere documentate e regolarmente testate.

Art. 35) Sicurezza del cablaggio

1. È necessario proteggere il cablaggio da minacce di tipo fisico, ambientale e organizzativo.
2. Il cablaggio deve essere collocato in posizione priva di rischi dovuti a perdita di fluidi e/o disturbi elettromagnetici indotti da altri sistemi e tale da consentirne un'agevole e sicura manutenzione.
3. Deve essere garantita la protezione fisica dei cavi di dorsale, dei cavi orizzontali e dei locali tecnici.

Capo V - Sicurezza delle attività operative

Art. 36) Procedure operative e responsabilità

1. Le procedure operative inerenti ai processi di gestione dei sistemi informatici devono essere documentate, manutenute e rese facilmente disponibili a tutto il personale incaricato di attuarle.
2. Qualsiasi modifica inerente ai sistemi e agli strumenti di gestione delle informazioni deve essere autorizzata, controllata e documentata.
3. Le responsabilità del controllo devono essere affidate a strutture o a personale esterno alle aree operative, onde ridurre le opportunità di modifiche non autorizzate o accidentali e manomissioni delle risorse informative della ASST.
4. Gli ambienti di sviluppo, di produzione e test devono essere separati al fine di ridurre al minimo i rischi di accessi o modifiche non autorizzate o anche accidentali dei relativi sistemi informativi.
5. La realizzazione di queste attività necessiterà un arco temporale di 3 anni (vedasi piano attuativo allegato).

Art. 37) Protezione da malicious software

1. L'integrità delle informazioni e delle risorse informatiche deve essere preservata dalla possibile compromissione da parte di software malevolo (ad esempio virus, worm, trojan horses).
2. Al riguardo è necessario definire:
   a) una politica di formazione ed informazione del personale e degli eventuali soggetti terzi sui danni potenziali arrecati alle Risorse Informative, legati all'introduzione di software malevolo;

b) idonee contromisure per l'individuazione di software malevolo nei sistemi informatici, nonché per il ripristino delle risorse eventualmente danneggiate. In tal senso, le postazioni di lavoro devono disporre almeno di un sistema antivirus aggiornato allo stato dell'arte.

c) I programmi antivirus devono essere gestiti e controllati in maniera tale da assicurarne una capillare diffusione ed un frequente aggiornamento.

d) Devono essere definite idonee contromisure atte a gestire gli eventi dannosi (isolamento, ripristino) ed a fornire supporto agli utenti coinvolti.

Art. 38) Software non autorizzato

1. Deve essere vietato l'utilizzo di software non espressamente autorizzati. Tutti i software installati sui sistemi informativi devono essere conformi ai termini delle licenze (vincoli d'uso) ed utilizzato per esclusive finalità lavorative.
2. Al riguardo è necessario impedire l'incauto prelievo di software e di file da computer remoti o la loro installazione non autorizzata in computer della ASST.
3. Tutto il personale deve essere reso consapevole dei danni potenziali arrecati alle Risorse Informative dall'introduzione di software non autorizzati, diversi da quelli standard in dotazione.
4. Devono essere definite idonee politiche e procedure di sicurezza e previsti strumenti per la prevenzione e l'individuazione di software non autorizzato nel sistema informatico nonché per il ripristino delle risorse eventualmente danneggiate.

Art. 39) Back-up

1. Per i sistemi ancora presenti sui Data Center aziendali devono essere previste, anche in conformità alle normative vigenti, adeguate politiche e procedure di back-up per preservare l'integrità e garantire la disponibilità delle informazioni (ad esempio in caso di manomissioni, atti vandalici, contaminazione da virus, perdita o distruzione anche involontaria).
2. Le procedure devono riguardare la verifica della corretta esecuzione dei back-up, il mantenimento di un elenco delle copie effettuate, l'archiviazione sicura, i criteri ed i tempi per la conservazione dei supporti di memorizzazione (dischi, nastri ecc.), i meccanismi e le modalità per la cancellazione sicura delle informazioni in caso di distruzione, smaltimento o riutilizzo dei supporti.
3. Laddove il back-up venga effettuato localmente nell'ambito dell'ufficio devono essere impartite al personale e agli eventuali soggetti terzi, le idonee istruzioni tecniche ed organizzative. Tali istruzioni devono indicare gli strumenti e le modalità con cui effettuare le copie di sicurezza, l'elenco delle banche dati e degli archivi per i quali è richiesta la copia, la sequenza temporale e la finestra operativa per garantire che i dati copiati siano tra loro congruenti.
4. Si stima, in termini di adeguamento di quanto già esistente, la completa realizzazione di queste attività in un arco temporale non inferiore ai 2 anni (vedasi piano attuativo allegato). Si precisa che tali attività sono già in corso al momento della delibera del documento.

Art. 40) Sicurezza della rete dati

1. La rete dati deve essere adeguatamente gestita e controllata. I sistemi e le applicazioni utilizzati nella rete dati devono essere mantenuti in sicurezza, incluse le informazioni in transito.

2. Devono essere definite politiche e procedure per la sicurezza della rete dati. Tutte le attività di manutenzione devono essere tracciate e verificate.
3. Gli aggiornamenti di sicurezza, i livelli di servizio ed i requisiti per la gestione dei servizi di rete devono essere identificati e formalizzati in specifici accordi contrattuali ogniqualvolta la gestione dei servizi sia affidata all'esterno.
4. Le prestazioni della rete dati devono essere controllate per verificare la conformità della gestione rispetto ai parametri attesi.
5. Il miglioramento e potenziamento delle procedure operative per la sicurezza delle reti dati richiederà un arco temporale non inferiore ai due anni e mezzo.

Art. 41) Sicurezza nello scambio di informazioni

1. Devono essere predisposte opportune procedure e controlli per lo scambio di informazioni e di software, sia all'interno della ASST che all'esterno, al fine di evitarne la perdita, la modifica o l'uso improprio. Tali attività verranno effettuate secondo il contesto organizzativo aziendale.
2. I supporti contenenti le informazioni devono essere protetti da accessi non autorizzati, manomissioni o alterazioni durante il trasporto.
3. Le informazioni critiche per la ASST contenute nei messaggi elettronici devono essere protette dai rischi di frode, accesso non autorizzato, alterazioni o distruzione mediante l'adozione di idonei sistemi di sicurezza.
4. Le informazioni scambiate nelle transazioni elettroniche devono essere protette al fine di prevenire trasmissioni incomplete, reindirizzamenti, accessi non autorizzati, alterazioni, duplicazioni non autorizzate dei messaggi.
5. Devono essere definite ed attuate specifiche procedure di sicurezza per garantire la protezione delle informazioni correlate ai sistemi a supporto dei servizi istituzionali, in funzione della loro classificazione.
6. Deve essere prevista un'idonea procedura contenente le raccomandazioni sulla sicurezza della rete interna, le regole per la navigazione in Internet e le indicazioni per l'uso appropriato del servizio di posta elettronica.
7. Il miglioramento e potenziamento richiederà, per la completa realizzazione di queste attività, un arco temporale non inferiore ai 3 anni (vedasi piano attuativo allegato).

Art. 42) Monitoraggio

1. Le informazioni inerenti alle attività effettuate dagli utenti dei sistemi ICT della ASST e più in generale agli eventi che possono compromettere la sicurezza delle risorse informative devono essere tracciate (ad esempio tramite file di log), memorizzate e conservate per un periodo di tempo ritenuto idoneo a supportare la risoluzione di problemi inerenti al funzionamento dei sistemi ICT, le future attività di accertamento e la "gestione degli incidenti", nel rispetto della normativa vigente (es. GDPR [R1], Statuto dei lavoratori [R36]).
2. Analogamente, devono essere definite procedure per il monitoraggio e il successivo accertamento del corretto utilizzo degli strumenti di elaborazione delle informazioni, nel rispetto della normativa vigente (es. Statuto dei lavoratori [R36]).
3. Gli strumenti di monitoraggio devono essere protetti contro i rischi di accesso non autorizzato e/o di alterazione.

4. I guasti ed i malfunzionamenti devono essere tracciati ed analizzati e devono essere intraprese opportune azioni correttive, nel rispetto dei livelli di servizio definiti contrattualmente o in assenza di questi, nel minore tempo possibile per non arrecare degradi prestazionali o rallentamenti delle attività di monitoraggio.

Art. 43) Crittografia

1. Ai fini dell'utilizzo della crittografia per la protezione delle informazioni, qualora richiesto, deve essere:
   a) definita una specifica politica di sicurezza;
   b) predisposta ed attuata un'idonea procedura per la gestione delle chiavi crittografiche.
2. Tali politiche e procedure devono risultare conformi alle vigenti normative nazionali ed agli standard internazionali in merito.

Art. 44) Smaltimento e cancellazione sicura dei dati

1. Le informazioni trattate presso la ASST devono essere cancellate o distrutte nei casi in cui:
   a) non siano più utili al raggiungimento delle finalità lavorative (ad es. copie di documentazione obsolete o relative a versioni superate o in soprannumero);
   b) siano relative alla cessazione per qualsiasi causa di trattamenti di dati personali/critici non più necessari, pertinenti o eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
   c) gli scopi per le quali sono state raccolte e trattate non siano più determinati, espliciti e legittimi oppure siano diventate incompatibili con tali scopi;
   d) risultino scaduti i termini legittimi di conservazione anche con riferimento al tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati, siano essi determinati da norme di legge generali e/o di settore (ad es. dieci anni per la conservazione delle scritture contabili) oppure dalle finalità per le quali i dati sono stati raccolti o in relazione alle quali devono essere conservati (ad es. contenziosi). La ASST per la conservazione dei dati si attiene ai tempi previsti dal Titolario e Massimario del Sistema Sanitario e Sociosanitario di Regione Lombardia, che deve pertanto essere rispettato;
   e) l'Interessato ne richieda la cancellazione, nell'esercizio dei propri diritti, nei casi applicabili e previsti dalle norme in materia di privacy[R1]. A tal riguardo la ASST ha adottato una specifica procedura per la gestione dei diritti degli interessati, tra cui rientra anche il diritto di cancellazione;
   f) il supporto elettronico sul quale sono memorizzate sia destinato allo smaltimento o dismissione, oppure quando sia destinato al reimpiego da parte di terzi.
2. A tal fine occorre definire un insieme di procedure operative per la cancellazione e distruzione sicura delle informazioni in linea con quanto previsto in materia dal Garante per la protezione dei dati personali [R5][R6]. Tali procedure devono garantire la non recuperabilità delle informazioni e la tecnica di cancellazione deve tenere conto della tipologia di supporto elettronico utilizzato e della classificazione delle informazioni in esso contenute.
3. Deve inoltre essere definito il processo di distruzione sicura di supporti rientranti nella categoria RAEE (Rifiuti e Apparecchiature Elettriche ed Elettroniche), nell'ambito del quale

deve essere garantito il rispetto delle normative ambientali “relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti” e di tutte le altre fonti normative in materia [R1][R35].

Capo VI - Controllo degli accessi

Art. 45) Accesso alle informazioni e alle risorse ICT

1. Deve essere protetto e controllato l'accesso alle informazioni ed alle risorse ICT utilizzate per la loro elaborazione.
2. A tal fine occorre definire formalmente e aggiornare periodicamente una politica di controllo degli accessi sulla base delle esigenze istituzionali della ASST e dei requisiti di sicurezza delle informazioni.
3. Il miglioramento e potenziamento richiederà un arco temporale non inferiore ai 5 anni (vedasi piano attuativo allegato).

Art. 46) Revisione dei diritti di accesso

1. Tutti i diritti di accesso assegnati al personale, nonché ai soggetti terzi ai quali l’accesso è consentito per l’esecuzione degli specifici obblighi contrattuali, devono essere regolarmente controllati ed aggiornati.
2. Deve essere prevista la modifica/revoca dei diritti d’accesso quando vengono meno le condizioni per le quali sono stati assegnati (ad esempio a seguito della cessazione del rapporto lavorativo o di cambio della mansione).
3. Si stima l’implementazione delle procedure di miglioramento in un arco temporale non inferiore a 5 anni (vedasi piano attuativo allegato).

Sezione I - Accessi logici

Art. 47) Gestione delle credenziali di accesso

1. Devono essere definiti politiche, procedure ed istruzioni per la gestione delle credenziali di accesso in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali. In tal senso:
   a) il codice identificativo (user-id) deve essere univoco e non riutilizzabile successivamente;
   b) le password devono essere individuali e l’utente è responsabile della loro riservatezza.
2. Inoltre, devono essere definiti standard per la maggiore complessità delle password in proporzione al livello di criticità dell’informazione e al livello di criticità dei sistemi sotto il profilo della sicurezza.
3. Si stima l’implementazione delle procedure di miglioramento in un arco temporale non superiore a 2 anni (vedasi piano attuativo allegato).

Art. 48) Gestione dei diritti di accesso

1. Devono essere definiti specifici profili di autorizzazione per l’accesso alle informazioni, da parte degli utenti del sistema informatico della ASST (personale, nonché soggetti terzi ai quali l’accesso è consentito per l’esecuzione degli specifici obblighi contrattuali).

2. I profili di autorizzazione di cui al comma precedente devono consentire di individuare a quali informazioni l'utente può accedere nonché quali azioni può compiere. Al riguardo, le elaborazioni/operazioni autorizzate devono essere limitate a quelle strettamente necessarie allo svolgimento delle mansioni assegnate e nell'ambito di operatività definito, conformemente al principio del "need to know/need to do" e del "at least privilege". In particolare, ai soggetti terzi deve essere consentito l'accesso alle informazioni della ASST solo ed esclusivamente in funzione del proprio incarico.
3. Devono essere definite procedure di gestione e controllo del ciclo di vita dei profili di autorizzazione degli utenti del sistema informatico della ASST (assegnazione, creazione, aggiornamento, disattivazione e revoca), inclusi i profili ad elevati privilegi.
4. Devono essere adottati controlli e procedure di sicurezza in grado di revocare, possibilmente tramite automatismi, i diritti di accesso degli utenti del sistema informatico della ASST.
5. Si stima l'implementazione delle procedure di miglioramento in un arco temporale non superiore a 2 anni (vedasi piano attuativo allegato).

Art. 49) Responsabilità dell'utente

1. Devono essere definite idonee istruzioni per rendere edotti gli utenti sulle regole di sicurezza da attuare in merito alla scelta ed all'utilizzo delle password e sulle cautele per assicurarne la segretezza.
2. Tali istruzioni devono, altresì, definire le modalità per il corretto utilizzo delle postazioni di lavoro e degli strumenti informatici e telematici.
3. Il personale e gli eventuali soggetti terzi, ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali, devono essere informati delle conseguenze, disciplinari e anche giuridiche, derivanti dalla mancata applicazione/violazione (volontaria o involontaria) delle istruzioni ricevute.

Art. 50) Accesso alla rete e relativi servizi

1. L'accesso alla rete ed ai servizi di rete deve essere consentito solo al personale autorizzato nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
2. In particolare, devono essere:
   a) monitorati gli accessi in conformità alle normative vigenti e regolarmente verificati;
   b) adottati appropriati sistemi di autenticazione per il controllo degli accessi remoti alla rete;
   c) controllati gli accessi fisici e logici per la diagnostica e la configurazione delle porte;
   d) attuati idonei controlli atti ad impedire l'accesso alla rete da parte di utenti non autorizzati.

Art. 51) Accessi al sistema operativo ed al software di base

1. L'accesso ai sistemi operativi ed al software di base deve essere controllato da un'idonea procedura di sicurezza.
2. L'accesso al sistema operativo ed al software di base deve essere consentito solo al personale autorizzato nonché ai soggetti terzi ai quali l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.

3. Gli accessi devono essere monitorati e periodicamente verificati con cadenza temporale prestabilita, in conformità alle normative vigenti, e regolarmente verificati.
4. Devono essere definite procedure atte ad assicurare la creazione di codici per l'identificazione univoca utenti (user-id).
5. Il sistema deve essere configurato in modo da prevedere la chiusura automatica della sessione lavorativa dopo un periodo predefinito di inattività e la riattivazione della stessa solo previa autenticazione informatica.

Art. 52) Accessi ai sistemi ed alle applicazioni

1. L'accesso ai sistemi ed alle applicazioni deve essere controllato da una idonea procedura di sicurezza e limitato al solo personale autorizzato nonché ai soggetti terzi cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.
2. Per l'accesso ai sistemi ed alle applicazioni che rivestono particolare criticità è opportuno che l'identificazione avvenga tramite meccanismi di autenticazione forte, la cui robustezza sia proporzionata al livello di criticità dei dati ivi contenuti.
3. Gli accessi ai sistemi ed alle applicazioni devono essere monitorati e regolarmente verificati, nel rispetto della normativa vigente.
4. Devono essere definite idonee procedure e controlli di sicurezza per proteggere i sistemi e le applicazioni dai rischi derivanti dall'utilizzo di computer portatili.
5. Nel caso in cui si utilizzino soluzioni per il lavoro da remoto devono essere definite ed attuate specifiche politiche e procedure per l'accesso in sicurezza ai sistemi ed alle applicazioni.
6. Si stima il miglioramento della gestione e il governo di queste attività in un arco temporale non superiore a 2 anni (vedasi piano attuativo allegato).

Capo VII - Acquisizione, sviluppo e manutenzione

Art. 53) Acquisizione, sviluppo e manutenzione dei sistemi

1. L'acquisizione, lo sviluppo e la manutenzione dei sistemi della ASST deve garantire la protezione delle informazioni da errori, perdite, modifiche non autorizzate o alterazioni.

Art. 54) Requisiti di sicurezza dei sistemi informativi

1. La sicurezza deve essere parte integrante dei sistemi informativi utilizzati per la gestione delle informazioni della ASST.
2. L'acquisizione di nuovi sistemi o di parti di sistemi esistenti deve includere, in accordo con i requisiti derivanti dagli scopi istituzionali e dalle politiche di sicurezza, la definizione di specifici requisiti e controlli di sicurezza.
3. Devono essere definiti specifici requisiti per l'identificazione e l'implementazione di appropriati controlli atti ad assicurare l'autenticità e l'integrità dei messaggi tra le applicazioni.

Art. 55) Sicurezza nei processi di sviluppo e supporto

1. Le applicazioni, sia commerciali che sviluppate appositamente per la ASST, devono rispettare le politiche e le linee guida di sviluppo sicuro derivanti dagli standard e dalle best practice applicabili.

2. Le applicazioni devono essere protette in modo da impedire errori, perdite, modifiche non autorizzate o alterazioni non autorizzate delle informazioni.
3. Inoltre, qualora possibile, devono essere previsti controlli di congruità delle informazioni, incorporati all'interno delle applicazioni, per rilevare eventuali alterazioni delle medesime derivanti da errori di processo o da azioni deliberate.
4. Per i processi critici devono essere previste procedure per la validazione dei dati inseriti all'interno delle applicazioni al fine di garantire che il dato sia corretto ed appropriato.
5. L'installazione del sistema operativo e dei software di base (middleware, application server, database, ecc.) deve essere controllata e verificata attraverso la predisposizione di idonee procedure di test.
6. Tutte le modifiche apportate ai sistemi devono essere controllate.
7. A seguito delle modifiche al sistema operativo, le applicazioni critiche devono essere controllate e verificate tramite test, al fine di scongiurare eventuali malfunzionamenti dell'operatività e della sicurezza della ASST.
8. Le modifiche ai pacchetti software devono essere limitate allo stretto necessario e, qualora effettuate, strettamente controllate.
9. Devono essere definite idonee procedure per il tracciamento delle modifiche e la successiva verifica.
10. Devono essere definite idonee procedure per la protezione degli ambienti utilizzati per lo sviluppo di nuove applicazioni o per le iniziative di integrazione, in termini di protezione delle informazioni, separazione degli ambienti di sviluppo, test, produzione e specifiche politiche di controllo accesso.
11. Per l'esecuzione dei test, non devono essere utilizzati dati personali ai sensi del GDPR [R1] o dati critici per l'ASST. Qualora fosse strettamente necessario utilizzare i suddetti dati, occorre adottare tecniche di mascheramento o soluzioni similari.
12. I risultati del test devono essere controllati e conservati.

Art. 56) Sicurezza nella manutenzione

1. Devono essere adottate procedure ed istruzioni operative per la regolamentazione delle attività di manutenzione dei sistemi informativi. Le procedure devono definire:
   a) i criteri e le modalità per l'aggiornamento periodico dei prodotti utilizzati;
   b) la pianificazione e l'attuazione di interventi di manutenzione programmata (dismissione, sostituzione, ecc.);
   c) il collaudo dell'operatività dei sistemi dopo gli interventi di aggiornamento e manutenzione;
   d) l'aggiornamento della configurazione del sistema in funzione delle modifiche apportate all'ambiente.
2. Tutte le attività di manutenzione devono essere tracciate e regolarmente verificate.
3. Si stima l'implementazione delle procedure di miglioramento in un arco temporale non inferiore ai 3 anni (vedasi piano attuativo allegato). Tale attività è in parte già in essere.

Capo VIII - Gestione degli incidenti rilevanti ai fini della sicurezza

Art. 57)Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti

1. Devono essere identificati, classificati e gestiti, in accordo con le normative nazionali ed interne alla ASST, gli incidenti rilevanti ai fini della sicurezza delle informazioni.
2. Devono essere definite procedure per la gestione degli incidenti rilevanti ai fini della sicurezza delle informazioni in conformità alle vigenti normative nazionali e interne alla ASST ed ai Service Level Agreement (SLA) previsti per i servizi erogati.
3. Tali procedure devono descrivere:
   a) le modalità di monitoraggio, rilevamento e classificazione degli eventi di sicurezza, anche in relazione a quanto richiesto dalle normative applicabili in materia;
   b) le modalità di gestione degli eventi rilevati e le procedure di escalation verso i soggetti interni ed esterni alla ASST;
   c) le finalità, le modalità, i criteri di protezione, di utilizzo ed i tempi di conservazione dei log rilevanti ai fini della ricostruzione delle cause di incidente.
4. La pianificazione e la verifica della risposta e del ripristino a seguito di un incidente devono essere condotti anche con i soggetti terzi, in relazione alle attività da questi svolte in forza degli accordi contrattuali.
5. Tutto il personale della ASST e i soggetti terzi devono attenersi alle indicazioni ricevute in materia di sicurezza delle informazioni e contenute nelle istruzioni operative di riferimento, che devono essere opportunamente redatte.
6. Tutto il personale della ASST e i soggetti terzi che individuano o abbiano il sospetto riguardante un incidente di sicurezza, devono segnalarlo immediatamente secondo le modalità appositamente stabilite allo scopo.
7. Devono essere previste sanzioni disciplinari in caso di violazione dei vincoli di sicurezza da parte del personale, in accordo con quanto previsto dalle norme contrattuali vigenti.
8. Devono essere, altresì, previste sanzioni in caso di violazione dei vincoli di sicurezza da parte dei soggetti terzi che accedono ed utilizzano le Risorse Informative per l'esecuzione degli specifici obblighi contrattuali.
9. Si stima l'implementazione delle procedure di miglioramento in un arco temporale non inferiore a 4 anni (vedasi piano attuativo allegato).

Capo IX - Gestione della continuità operativa

Art. 58) Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

1. Deve essere garantita la continuità operativa della ASST, con l'obiettivo di ripristinare una situazione di normalità entro un tempo prestabilito (in funzione dei livelli di servizio attesi), minimizzando gli impatti sui servizi erogati dall'Amministrazione, derivanti dall'interruzione delle attività a fronte di un incidente di sicurezza, un guasto o disastro.
2. Devono essere identificati e resi noti i requisiti di resilienza a supporto dell'erogazione dei servizi della ASST per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio).
3. Deve essere predisposto un piano di continuità operativa (Business Continuity Plan – BCP), inteso come l'insieme delle attività organizzative e tecnologiche finalizzate alla continuità dei processi che concorrono all'attuazione degli scopi istituzionali della ASST.
4. Tale piano deve descrivere i criteri, le procedure e gli strumenti adottati per la gestione delle emergenze (Contingency Plan) e per il ripristino delle condizioni operative antecedenti al verificarsi di un evento dannoso (Disaster Recovery), in conformità ai livelli di servizio prestabiliti.
5. Il piano deve altresì definire chiaramente la strategia di protezione delle attività istituzionali, sulla base delle attività di analisi e gestione del rischio, rispetto ad eventi di indisponibilità delle informazioni e delle risorse informatiche.
6. La pianificazione e la verifica della risposta e del ripristino a seguito di un evento dannoso che ha impatto sulla continuità operativa della ASST devono essere condotti anche con i soggetti terzi, in relazione alle attività da questi svolte in forza degli accordi contrattuali.
7. Si stima la completa realizzazione di queste attività in un arco temporale di 4 anni (vedasi piano attuativo allegato).

Titolo VI - Controlli di conformità

Art. 59) Conformità ai requisiti di sicurezza

1. La conformità ai requisiti di sicurezza definiti dalle normative cogenti, dagli standard internazionali e dalle best practice applicabili alla ASST, risulta imprescindibile nell'ambito del raggiungimento degli obiettivi di sicurezza espressi dalla Politica della Sicurezza delle Informazioni (cfr. Titolo II -).
2. Tali requisiti sono presi in considerazione nell'ambito della definizione delle direttive esplicitate negli Statement che indirizzano la tutela delle Risorse Informative della ASST (cfr. Titolo V -).

Capo I - Conformità ai requisiti cogenti e contrattuali

Art. 60) Normativa generale in materia di sicurezza delle informazioni

1. La ASST deve prevedere un processo di analisi periodica della normativa generale in materia di sicurezza delle informazioni applicabile alla ASST e attuare le attività necessarie per garantire la conformità a tale normativa.
2. In particolare, la ASST, nell'ambito della definizione delle strategie di gestione della sicurezza delle informazioni, deve ottemperare ai requisiti derivanti dai principi generali enunciati dall'attuale legislazione italiana ed europea inerente, a titolo esemplificativo e non esaustivo, alle seguenti tematiche:
   a) Infrastrutture critiche e cybersecurity;
   b) Criminalità informatica;
   c) Tutela del trattamento dei dati personali;
   d) Tutela del software e delle banche dati;
   e) Responsabilità amministrativa e penale a carico di amministratori e dirigenti;
   f) Validità giuridica del documento informatico;
   g) Contratto Collettivo Nazionale di Lavoro e sue integrazioni.

Art. 61) Normativa specifica e di settore applicabile ai servizi della ASST

1. La ASST deve prevedere un processo di analisi periodica della normativa specifica e di settore in materia di sicurezza ICT applicabile ai servizi istituzionali erogati dalla ASST e attuare le attività necessarie per garantire la conformità a tale normativa.

Art. 62) Requisiti contrattuali

1. La ASST deve documentare e mantenere aggiornati tutti i requisiti contrattuali inerenti alla sicurezza delle informazioni e attuare le attività necessarie per garantire la conformità a tali requisiti.

Capo II - Conformità a standard internazionali e best practices

Art. 63) Standard internazionali e best practice

1. La ASST deve adottare un approccio metodologico, per la gestione delle problematiche inerenti alla sicurezza delle informazioni, conforme agli standard internazionali ed alle best practice nazionali ed internazionali di riferimento per la definizione di ruoli, responsabilità, procedure formali di gestione dei processi legati alla sicurezza, sia per l'operatività della ASST, sia per il trattamento delle emergenze.
2. A tal riguardo occorre prevedere un processo di analisi periodica degli standard internazionali e best practice inerenti alla sicurezza delle informazioni applicabili alla ASST, tra questi identificare quelli più idonei in relazione al contesto della ASST e attuare le attività necessarie per recepirli nel contesto organizzativo.
3. La ASST si impegna alla realizzazione e l'implementazione di tali attività a regime in un arco temporale non inferiore a 3 anni dall'entrata in vigore della presente politica (vedasi piano attuativo allegato).

Capo III - Riesame della sicurezza delle informazioni

Art. 64) Verifica e riesame della sicurezza delle informazioni

1. Devono essere effettuate attività di verifica e riesame, al fine di assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche ed alle procedure della ASST.
2. La ASST deve effettuare, con periodicità predefinita e in occasione di cambiamenti significativi, un riesame indipendente dell'approccio definito per la sicurezza delle informazioni in termini di obiettivi, controlli, politiche, processi e procedure.
3. Deve inoltre essere riesaminata regolarmente la conformità dei processi inerenti alla sicurezza delle informazioni attuati presso la ASST rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza.
4. Infine, devono essere effettuate regolarmente verifiche tecniche dei sistemi informativi al fine di verificarne la conformità rispetto alle politiche e alle norme per la sicurezza delle informazioni.

Titolo VII - Il sistema documentale

Art. 65)Sistema documentale per la sicurezza delle informazioni

1. Il raggiungimento degli obiettivi di protezione delle Risorse Informative della ASST e l'attuazione controlli definiti nel presente documento (cfr. Titolo V - e Titolo VI -), presuppone la creazione di un adeguato sistema documentale.
2. La ASST ha definito e strutturato il sistema documentale specifico inerente alla sicurezza delle informazioni che consente di indirizzare il governo delle problematiche relative alla protezione delle Risorse Informative. A partire dalla presente politica, tale sistema si sostanzia in Politiche generali e specifiche per la Sicurezza delle Informazioni, Linee Guida, Procedure e Istruzioni operative, secondo il seguente schema:
    a) **Politica per la sicurezza delle Informazioni**: documento (il presente) che fornisce una serie di principi, modalità di azione, requisiti organizzativi, di alto livello e non derogabili, finalizzata a definire l'ambito di applicazione e a guidare il governo della sicurezza delle informazioni, in linea con le volontà dell'Alta Direzione;
    b) **Politiche generali per la Sicurezza delle Informazioni**: documentazione che fornisce regole inderogabili di alto livello su temi generali inerenti alla sicurezza delle informazioni, derivati dalla suddetta Politica per la sicurezza delle Informazioni;
    c) **Politiche Specifiche per la Sicurezza delle Informazioni**: documentazione che fornisce regole inderogabili di alto livello su temi specifici di sicurezza delle informazioni;
    d) **Linee Guida**: documentazione che fornisce raccomandazioni, a carattere generale o specifico, derogabili e la cui implementazione è rimessa alle figure responsabili dei servizi/processi/applicazione. In caso di deroga, le suddette figure devono documentare le ragioni della non aderenza alle linee guida e le scelte effettuate in alternativa;
    e) **Procedure operative**: documentazione che descrive le modalità operative (chi, cosa, come, quando, dove) nell'ambito dei processi di sicurezza e dei controlli implementati per l'attuazione delle Politiche e delle Linee Guida;
    f) **Istruzioni operative**: documentazione descrittiva dei compiti e delle attività effettuate dal personale operativo.
3. Le Politiche, le Linee Guida, le Procedure e le Istruzioni Operative devono essere strutturate in modo semplice e comprensibile al personale di ogni livello organizzativo. Tale documentazione deve essere pubblicata, resa disponibile a tutti i soggetti interessati e revisionata periodicamente.

Documenti di riferimento

[R1] Regolamento UE n. 679/2016 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE – General Data Protection Regulation (GDPR)

[R2] D.lgs. 101/2018: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

[R3] Deliberazione del Garante Privacy numero 53 del 23 novembre 2006: Linee guida in materia di trattamento di dati personali di lavoratori

[R4] Deliberazione del Garante Privacy numero 13 del 1° marzo 2007: Uso delle e-mail e di Internet

[R5] Provvedimento del Garante Privacy del 13 ottobre 2008: Smaltimento e cancellazione sicura dei dati

[R6] Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori - Scheda informativa del Garante per la protezione dei dati personali del 12 dicembre 2008

[R7] Provvedimento del Garante Privacy dell'8 aprile 2010: Videosorveglianza

[R8] Provvedimento del Garante Privacy: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008 e successive modifiche e integrazioni

[R9] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS)

[R10] D.lgs. 65/2018: Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione" (Attuazione Direttiva (UE) NIS 2016/1148) aggiornato dal Decreto-Legge 14 giugno 2021, n. 82

[R11] Linee Guida per gli Operatori di Servizi Essenziali – Autorità NIS-Settore Salute – luglio 2019

[R12] Direttiva 2009/136/CE, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e si servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori

[R13] DPCM 29 settembre 2015, n. 178. Regolamento in materia di fascicolo sanitario elettronico

[R14] "Linee guida in materia di Dossier sanitario" del Garante per la protezione dei dati personali del 4 giugno 2015 (G.U. n. 164 del 17 luglio 2015)

[R15] D.lgs. 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

[R16] PIANO NAZIONALE DI RIPRESA E RESILIENZA, #NEXTGENERATIONITALIA, Italia Domani

[R17] DPCM 14 aprile 2021, n. 81. Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del

decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza

[R18] Decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

[R19] D.lgs. 38/2014: Attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, nonché della direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro stato membro

[R20] Framework Nazionale per la Cybersecurity e la Data Protection

[R21] ISO 9001:2008: Sistemi di Gestione per la Qualità - Requisiti

[R22] ISO/IEC 73:2009: Risk management – Vocabulary – Guidelines for use in standards

[R23] UNI ISO 31000: 2010: Gestione del rischio – Principi e linee guida

[R24] ISO/IEC 27001: Tecnologie Informatiche - Tecniche per la Sicurezza - Sistemi di Gestione per la Sicurezza delle Informazioni - Requisiti

[R25] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

[R26] ISO/IEC 27003: Information Technology – Security Techniques – Information security management system implementation guidance

[R27] ISO/IEC 27004: Information Technology – Security Techniques – Information security management - Measurement

[R28] ISO/IEC 27005: Information Technology – Security Techniques – Information security risk management

[R29] D.lgs. n. 82/2005: Codice dell'amministrazione digitale e successive modificazioni e integrazioni

[R30] Misure minime di sicurezza per le PA, AgID

[R31] Determinazione n. 220/2020 del 17 maggio 2020 - Adozione delle Linee Guida – La sicurezza nel procurement ICT, AgID

[R32] Decreto del Direttore Della Repubblica 16 aprile 2013, n. 62: Regolamento recante codice di comportamento dei dipendenti pubblici

[R33] Linee guida regionali per l'adozione dei piani di organizzazione Aziendale delle aziende sanitarie e degli IRCCS di diritto pubblico della Regione Lombardia (DGR n. IX/3822 del 25.07.2012)

[R34] Regolamento (UE) 2019/881 (Cybersecurity act) del 17 aprile 2019

[R35] Decreto Legislativo 3 aprile 2006, n. 152 - Norme in materia ambientale

[R36] LEGGE 20 maggio 1970, n. 300 (Statuto dei lavoratori)

[R37] Regolamento per i procedimenti disciplinari relativi al personale dipendente del comparto della dirigenza della ASST

[R38] Modello Organizzativo Data Protection della ASST

Allegato 1 – Piano attuativo

CRONOPROGRAMMA

		1° ANNO				2° ANNO				3° ANNO				4° ANNO				5° ANNO			
	TRIMESTRE -->	1°	2°	3°	4°	1°	2°	3°	4°	1°	2°	3°	4°	1°	2°	3°	4°	1°	2°	3°	4°
AREA	**ATTIVITA'**																				
RISCHI LEGATI ALLA CYBERSECURITY	**Art. 7) Principi generali Adeguatezza al livello di consapevolezza dell'Organizzazione**																				
	Formazione																				
	Monitoraggio																				
	Azioni di miglioramento																				
CONTROLLI DI SICUREZZA	**Art. 11) Controlli di sicurezza delle informazioni**																				
SICUREZZA DELLE RISORSE INFORMATIVE	**Art. 13) Inventario degli asset**																				
	Inventario asset informatico																				
	Risorse software, risorse hardware, sistemi informativi esterni e locali																				
	Flussi di dati e comunicazioni																				
	Inventario asset cartaceo																				
	Capitale umano																				
SICUREZZA NELL'AMBITO DELLE RISORSE UMANE	**Art. 22) Sensibilizzazione e formazione Sensibilizzazione e formazione del personale ASST e dei collaboratori esterni**																				
SICUREZZA NELLE RELAZIONI CON SOGGETTI TERZI	**Art. 24) Controlli generali Predisposizione politiche, procedure e istruzioni per gestione e utilizzo delle risorse informative da parte di soggetti terzi**																				
	Art. 25) Clausole Contrattuali																				
	Art. 26) Monitoraggio, revisione e gestione del cambiamento dei servizi delle terze parti																				
SICUREZZA FISICA E AMBIENTALE	**Art. 28) Protezione da minacce di tipo fisico ed ambientale**																				
	Art. 32) Lavorare in aree sensibili Progettazione e implementazione sistemi di sicurezza fisica, definizione procedure per la gestione dell'accesso alle aree sensibili e predisposizione linee guida ed istruzioni per la regolamentazione delle attività all'interno di suddette aree																				
SICUREZZA DELLE ATTIVITA' OPERATIVE	**Art. 36) Procedure operative e responsabilità**																				
	Art. 39) Back-up																				
	Art. 40) Sicurezza delle reti dati - definizione procedure operative																				
	Art. 41) Sicurezza nello scambio di informazioni																				
CONTROLLO DEGLI ACCESSI	**Art. 45) Accesso alle informazioni e alle risorse ICT**																				
	Art. 46) Revisione dei diritti di accesso																				
ACCESSI LOGICI	**Art. 47) Gestione delle credenziali di accesso**																				
	Art. 48) Gestione dei diritti di accesso																				
	Art. 52) Accessi ai sistemi ed alle applicazioni																				
ACQUISIZIONE, SVILUPPO E MANUTENZIONE	**Art. 56) Sicurezza nella manutenzione**																				
	Procedure e Istruzioni Operative																				
	Monitoraggio																				
GESTIONE DEGLI INCIDENTI RILEVANTI AI FINI DELLA SICUREZZA	**Art. 57) Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti**																				
GESTIONE DELLA CONTINUITA' OPERATIVA	**Art. 58) Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa**																				
CONFORMITA' A STANDARD INTERNAZIONALI E BEST PRACTICES	**Art. 63) Standard internazionali e best practice**																				

INFORMATIVA PRIVACY
Regolamento 679/2016/UE
Informativa Interessati per il trattamento dei dati personali e particolari –
Personale dipendente e collaboratore

Ai sensi e per gli effetti dell'articolo 13 del Regolamento 679/2016/UE "General Data Protection Regulation", relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, informiamo che l'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario, in qualità di Titolare del trattamento, tratta i dati personali da Lei (di seguito anche "Interessato") forniti per iscritto o verbalmente e liberamente comunicati. L'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario garantisce che il trattamento dei Suoi dati personali si svolge nel rispetto dei diritti e delle libertà fondamentali, nonché della Sua dignità, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

1. Finalità del trattamento dei dati personali (Art. 13.1.c Regolamento 679/2016/UE)

Tutti i dati personali dell'Interessato, ed eventualmente quelli appartenenti a categorie particolari di cui all'art. 9 del Regolamento UE 679/2016 o relativi a condanne penali e reati ai sensi dell'art. 10 del Regolamento UE 679/2016, sono trattati dal Titolare del trattamento sulla base dei seguenti presupposti di liceità:

- il trattamento è necessario per l'esecuzione di un contratto cui l'Interessato è parte (art. 6.1.b Regolamento 679/2016/UE);
- il trattamento è necessario per assolvere ad adempimenti previsti da leggi, da regolamenti, dalla normativa comunitaria (art. 6.1.c Regolamento 679/2016/UE);
- 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 (art. 6.1.e e art. 9.2.g Regolamento 679/2016/UE);
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui è autorizzato dal diritto UE o dagli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato (art. 9.2.b Regolamento 679/2016/UE);
- il trattamento è necessario per finalità di medicina preventiva e di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari sociali sulla base del diritto UE o degli Stati membri o conformemente al contratto con un professionista della sanità (articolo 9.2.h Regolamento 679/2016/UE).

In elenco, le finalità per cui i dati personali dell'Interessato verranno trattati:

- inserimento nelle anagrafiche e nei database informatici aziendali;
- gestione amministrativa ed economica del rapporto di lavoro subordinato o di collaborazione (rilevazione presenze, permessi, adempimenti fiscali, contabili, previdenziali, sicurezza ed igiene sul lavoro e formazione);
- tracciabilità degli accessi alla rete Internet connessi all'eventuale svolgimento di controlli sporadici o difensivi (comunque preceduti da una prima fase di monitoraggio anonimo delle connessioni effettuate);
- archiviazione dei log degli accessi alla rete informatica dell'Ente in modalità non intellegibile allo stesso Titolare del trattamento ed esclusivamente destinati ad eventuali richieste dell'Autorità Giudiziaria;

- ottemperare a specifiche esigenze.

1.1. L'interessato ha la facoltà di autorizzare in forma scritta (consenso) l'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario ad essere fotografato, filmato (compresa la registrazione del suono della voce) sui luoghi di lavoro per la realizzazione di materiale cartaceo e digitale di natura promozionale e pubblicitaria legato esclusivamente all'attività dell'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario. Tale materiale sarà pubblicabile anche sul sito Internet e sui profili ufficiali attivati nelle varie piattaforme digitali di condivisione di contenuti (social network come Facebook, Twitter, Instagram, Youtube, etc.) di cui l'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario è amministratore. La liceità del trattamento dei dati personali per tale specifica finalità si fonda sul libero, espresso ed esplicito consenso scritto dell'Interessato ai sensi dell'art. 6.1.a e art. 9.2.a Regolamento 679/2016/UE.

2. Le modalità del trattamento dei dati personali

Il trattamento dei dati personali dell'Interessato avviene presso le sedi e gli uffici del Titolare o, qualora fosse necessario, presso i soggetti indicati al paragrafo 4, utilizzando sia supporti cartacei che informatici, per via sia telefonica che telematica, anche attraverso strumenti automatizzati atti a memorizzare, gestire e trasmettere i dati stessi, con l'osservanza di ogni misura cautelativa che ne garantisca la sicurezza e la riservatezza.

Il trattamento si svilupperà in modo da ridurre al minimo il rischio di distruzione o perdita, di accesso non autorizzato, di trattamento non conforme alle finalità della raccolta dei dati stessi. I dati personali dell'Interessato sono trattati:

- nel rispetto del principio di minimizzazione, ai sensi degli articoli 5.1.c e 25.2 del Regolamento 679/2016/UE;
- in modo lecito e secondo correttezza.

I dati personali dell'Interessato sono raccolti:

- per scopi determinati espliciti e legittimi;
- esatti e se necessario aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità del trattamento.

3. Natura della raccolta e conseguenze di un eventuale mancato conferimento dei dati personali (Art. 13.2.e Regolamento 679/2016/UE)

Il conferimento dei dati personali è obbligatorio per le finalità previste al paragrafo 1. Il loro mancato conferimento comporta la mancata erogazione del rapporto di lavoro o collaborazione (anche nelle forme assimilate come tirocini, stage, ecc.) e degli eventuali adempimenti di legge. I dati personali sono conservati presso gli uffici aziendali e, qualora fosse necessario, presso i soggetti indicati al paragrafo 4.

Il conferimento dei dati personali (fotografie e filmati che riprendono l'Interessato) per la realizzazione di materiale cartaceo e digitale di natura promozionale e pubblicitaria di cui al punto 1.1. del paragrafo 1 è facoltativo, ed il loro mancato conferimento non pregiudica l'instaurazione e prosecuzione del rapporto contrattuale e del suo corretto svolgimento.

I dati personali dell'Interessato sono conservati presso la sede aziendale dell'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario. Qualora fosse necessario, i dati personali dell'Interessato possono essere conservati anche da parte degli altri soggetti indicati al paragrafo 4.

4. Eventuali destinatari o eventuali categorie di destinatari dei dati personali (Art. 13.1.e Regolamento 679/2016/UE)

I dati personali dell'Interessato, qualora fosse necessario, possono essere comunicati (con tale termine intendendosi il darne conoscenza ad uno o più soggetti determinati), a:

- soggetti la cui facoltà di accesso ai dati è riconosciuta da disposizioni di legge, normativa secondaria, comunitaria;
- collaboratori, dipendenti, fornitori e consulenti dell'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario, nell'ambito delle relative mansioni e/o di eventuali obblighi contrattuali, compresi gli Autorizzati al trattamento nominati ai sensi del Regolamento 679/2016/UE;

- uffici postali, spedizionieri e corrieri per l'invio di documentazione e/o materiale;
- istituti bancari per la gestione d'incassi e pagamenti derivanti dall'esecuzione dei contratti.

I dati personali dell'Interessato non vengono in alcun caso diffusi (con tale termine intendendosi il darne conoscenza in qualunque modo ad una pluralità di soggetti indeterminati), fatti salvi gli obblighi di legge

ad eccezione delle fotografie e dei filmati realizzati per finalità promozionali e pubblicitarie legate all'attività dell'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario qualora l'Interessato abbia prestato il consenso scritto.

I dati particolari dell'Interessato possono essere comunicati esclusivamente ai seguenti soggetti, Enti od organizzazioni:

- organizzazioni sindacali ai fini della gestione dei permessi e delle trattenute sindacali relativamente ai dipendenti che hanno rilasciato delega;
- enti assistenziali, previdenziali e assicurativi e autorità locali di pubblica sicurezza a fini assistenziali e previdenziali, nonché per rilevazione di eventuali patologie o infortuni sul lavoro;
- Presidenza del Consiglio dei Ministri in relazione alla rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (D.Lgs. 165/2001);
- uffici provinciali competenti per il collocamento mirato relativamente ai dati anagrafici degli assunti appartenenti alle cd. "categorie protette";
- Comitato di verifica per le cause di servizio e Commissione medica territorialmente competente (per conseguire il parere definitivo di riconoscimento della causa di servizio ai sensi del D.P.R. 461/2001).

I dati personali dell'Interessato idonei a rivelare lo stato di salute (i certificati relativi agli infortuni sul lavoro, l'assenza per malattia o per maternità, l'eventuale gestione dei dati relativi all'appartenenza a categorie protette, le convinzioni politiche, religiose o di altro genere) vengono trattati al solo fine di adempiere agli obblighi derivanti dalla legge e/o dalle disposizioni contrattuali nazionali. I dati personali dell'Interessato non vengono in alcun caso diffusi (con tale termine intendendosi il darne conoscenza in qualunque modo ad una pluralità di soggetti indeterminati), fatti salvi gli obblighi di legge.

5. Titolare del trattamento dei dati personali (Art. 13.1.a Regolamento 679/2016/UE)

Il Titolare del trattamento dei dati personali è l'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario. Alla data odierna, ogni informazione inerente il Titolare, congiuntamente all'elenco aggiornato dei Responsabili e degli Amministratori di sistema designati, è reperibile presso la sede aziendale dell'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario – Via Stelvio, 25, 23100 Sondrio. PEC: protocollo@pec.asst-val.it.

6. Data Protection Officer (DPO)/Responsabile della Protezione dei dati (RPD) (Art. 13.1.b Regolamento 679/2016/UE)

I riferimenti del Data Protection Officier/Responsabile della Protezione dei dati individuato dall'Ente sono pubblicati al seguente link www.asst-val.it/dpo .
Il Data Protection Officer è reperibile presso la sede aziendale dell'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario – Via Stelvio, 25, 23100 Sondrio. In caso di istanze/comunicazioni scritte da inviarsi in modalità digitale, il Data Protection Officer può essere contattato utilizzando i recapiti istituzionali dell'Ente (dpo@asst-val.it) indicati sul sito web dell'Ente.

7. Criteri utilizzati al fine di determinare il periodo di conservazione (Art. 13.2.a Regolamento 679/2016/UE)

L'Azienda Socio Sanitaria Territoriale Valtellina e Alto Lario dichiara che i dati personali dell'Interessato oggetto del trattamento saranno conservati per il periodo necessario a rispettare i termini di conservazione stabiliti nel Massimario di Scarto approvato dalla Regione Lombardia attualmente in vigore e ss.mm.ii. e comunque non superiori a quelli necessari per la gestione dei possibili ricorsi/contenziosi.

8. Diritti dell'Interessato (Art. 13.2.b Regolamento 679/2016/UE)

Si comunica che, in qualsiasi momento, l'Interessato può esercitare:

- diritto di revocare il consenso espresso, ex art. 7, par. 3 Reg. 679/2016;
- diritto di chiedere al Titolare del trattamento, ex Art. 15 Reg. 679/2016, di poter accedere ai propri dati personali;
- diritto di chiedere al Titolare del trattamento, ex Art. 16 Reg. 679/2016, di poter rettificare i propri dati personali, ove quest'ultimo non contrasti con la normativa vigente sulla conservazione dei dati stessi;
- diritto di chiedere al Titolare del trattamento, ex Art. 17 Reg. 679/2016, di poter cancellare i propri dati personali, ove quest'ultimo non contrasti con la normativa vigente sulla conservazione dei dati stessi;
- diritto di chiedere al Titolare del trattamento, ex Art. 18 Reg. 679/2016, di poter limitare il trattamento dei propri dati personali;
- diritto di opporsi al trattamento, ex Art. 21 Reg. 679/2016.

9. Diritto di presentare reclamo (Art. 13.2.d Regolamento 679/2016/UE)

L'Interessato ha sempre il diritto di proporre un reclamo all'Autorità Garante per la protezione dei dati personali per l'esercizio dei suoi diritti o per qualsiasi altra questione relativa al trattamento dei suoi dati personali.

Il/la sottoscritto/a *(cognome e nome)* .....

dichiara di aver ricevuto e preso atto dell'informativa di cui all'Articolo 13 del Regolamento 679/2016/UE *"General Data Protection Regulation"*.

Luogo e data Firma

_____ _____

Richiesta del consenso per l'utilizzo di dati personali dell'Interessato (fotografie, filmati e suono della voce)

Il/la sottoscritto/a *(cognome e nome)* .....

☐ **presta il consenso** ☐ **nega il consenso**

alle finalità di cui al punto 1.1 della presente informativa e nello specifico ad essere fotografato e filmato (con eventuale raccolta audio) durante lo svolgimento dell'attività istituzionale, anche quando è deducibile lo stato di salute, per la diffusione della propria immagine sul sito ed eventuali social network istituzionali di cui l'Ente è amministratore.

Luogo e data Firma

_____ _____

ISTRUZIONE OPERATIVA

Istruzioni per il trattamento dei dati personali

INDICE di REVISIONE	00	
DATA di AGGIORNAMENTO	16/05/2023	
DESCRIZIONE MODIFICHE INTEGRAZIONI	Emissione	
FASE	**NOMINATIVO**	**FIRMA**
REDAZIONE Data _____	S. Ruffoni – SC Affari Generali e Legali	
PRE-VERIFICA Data _____	C. Paganoni – Incarico di Funzione Qualità e Risk Management – SC Gestione Operativa: Next generation EU – Qualità e Risk Management	
	A. Faccinelli - SC Gestione Operativa: Next Generation EU – Qualità e Risk Management	
VERIFICA Data _____	S. Benedetti – Responsabile SS Trasparenza e Internal Auditing – SC Affari Generali e Legali	
APPROVAZIONE Data _____	A. De Vitis – Direttore Amministrativo	

INDICE

SCOPO

La presente Istruzione Operativa ha lo scopo di trasmettere la completa e corretta conoscenza delle modalità operative alle quali le persone autorizzate al trattamento dei dati personali, nominate per iscritto dal Titolare, devono attenersi per garantire il rispetto del "Regolamento Europeo in materia di protezione dei dati personali 2016/679", del Codice Privacy novellato dal D. Lgs 101/18, delle linee guida e dei provvedimenti emanati dalle autorità di controllo, nonché delle misure tecniche ed organizzative adottate dal Titolare per garantire la riservatezza, l'integrità e la disponibilità dei dati.

CAMPO DI APPLICAZIONE

La presente Istruzione Operativa si applica alle modalità di trattamento di tutti i dati personali, al fine di garantire, così come indicato dall'art. 1, 2 e 3 del Regolamento Europeo 2016/679, che il trattamento stesso si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

RESPONSABILITÀ

La responsabilità di aggiornamento e revisione del presente documento è in capo all'Ufficio Privacy. La responsabilità di diffusione è in capo all'Ufficio Privacy. La responsabilità di applicazione è in capo ai soggetti autorizzati a compiere operazioni di trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

RIFERIMENTI NORMATIVI

- Regolamento 679/2016/UE "General Data Protection Regulation (GDPR)"

TERMINI E DEFINIZIONI

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. (Art. 4 Regolamento 679/2016/UE).

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. (Art. 4 Regolamento 679/2016/UE).

Dati particolari: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici *(i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione – Art. 4)*, dati biometrici *(i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici – Art. 4)* intesi a identificare in modo univoco una persona fisica, dati relativi alla salute *(i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute – Art. 4)* o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 Regolamento 679/2016/UE).

Dati giudiziari: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (Art. 10 Regolamento 679/2016/UE).

Titolare: 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 (Art. 4 Regolamento 679/2016/UE).

Responsabile: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (Art. 4 Regolamento 679/2016/UE).

Data Protection Officer: (in italiano Responsabile per la Protezione dei Dati) è una nuova figura introdotta dal Regolamento 679/2016/UE e rappresenta il punto di riferimento per i soggetti esterni che decidono di esercitare i propri diritti in ambito privacy nei confronti del Titolare del trattamento. La sua nomina è obbligatoria per le PA, per tutti i soggetti che trattano su larga scala dati sensibili relativi alla salute, alla vita sessuale, genetici, giudiziari o biometrici e per tutti i soggetti che svolgono attività in cui trattamenti richiedono il controllo regolare e sistematico degli interessati su larga scala.

Soggetti autorizzati (Incaricati): persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Interessato: la persona fisica alla quale si riferiscono i dati trattati. L'interessato è quindi il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del Titolare del trattamento.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dai soggetti autorizzati (Incaricati), in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un Interessato identificato o identificabile.

Blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmesse attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione: i dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.

Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Informativa: L'informativa sul trattamento dei dati personali è il documento con il quale il titolare del trattamento, in forma scritta o orale, informa il soggetto interessato circa le finalità e le modalità del trattamento medesimo.

DOCUMENTI DI RIFERIMENTO

Informative e Moduli Privacy disponibili sulla Intranet aziendale, "Area dipendenti" sezione Privacy" al seguente link: https://intranet.asst-val.it/group/guest/privacy

DOCUMENTI ALLEGATI

Allegato 1 - Introduzione al Regolamento 679/2016/UE

DESCRIZIONE DELL'ATTIVITÀ

Premessa

Le operazioni di trattamento dei dati personali possono essere effettuate esclusivamente da parte di **soggetti autorizzati**, adeguatamente istruiti, che operano sotto la diretta autorità del Titolare del trattamento oppure, se designato, del Responsabile, attenendosi alle istruzioni impartite.

Per soggetti autorizzati si intendono quindi ***le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile***.

Per i trattamenti di dati personali effettuati con o senza l'ausilio di strumenti elettronici, i soggetti autorizzati al trattamento **debbono attenersi alle Regole e Istruzioni di sicurezza dei dati personali stabilite dall'Organizzazione** ed **osservare le seguenti disposizioni**:

- **effettuare** esclusivamente trattamenti di dati personali che rientrano nell'ambito del trattamento definito e comunicato per iscritto all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea, degli strumenti informatici, elettronici, telematici e dei trattamenti dell'Organizzazione che contengono i predetti dati personali;
- **effettuare** il trattamento dei dati personali esclusivamente in conformità alle finalità previste e dichiarate, nei trattamenti di dati personali a cui risultano essere autorizzati;
- **provvedere** ad **aggiornare** tempestivamente i dati personali nell'ipotesi in cui risultino essere inesatti o incompleti;
- **osservare** tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione e/o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta;
- **conservare** con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso ed uso esclusivo (la parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito e non deve contenere riferimenti agevolmente riconducibili all'Incaricato);
- **modificare** la componente riservata delle credenziali di autenticazione (**parola chiave**) al primo utilizzo e, successivamente, almeno ogni sei mesi nell'ipotesi di trattamento di dati personali comuni identificativi e almeno ogni tre mesi, nell'ipotesi di trattamento di dati personali particolari (dati idonei a rilevare l'origine razziale od etnico, le opinioni politiche, le convenzioni religiose, le convinzioni filosofiche, l'appartenenza a sindacati e dati idonei a rivelare lo stato di salute nonché la vita e/o l'orientamento sessuale) e giudiziari;
- **non lasciare** incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

In particolare, per i trattamenti di dati personali effettuati **senza l'ausilio di strumenti elettronici**:

- **effettuare** le operazioni di trattamento dei documenti e del materiale cartaceo esclusivamente all'interno dei locali individuati per la loro conservazione;
- **ridurre** al tempo minimo necessario per effettuare le operazioni di trattamento l'asportazione dei documenti e del materiale cartaceo dai locali individuati per la loro conservazione;
- **verificare** che i supporti cartacei contenenti dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi e integri;
- **ricollocare** e archiviare tutti i documenti contenenti dati personali su supporti cartacei, nei locali individuati per la loro conservazione;
- **adottare** ogni cautela per evitare che soggetti non autorizzati al trattamento dei dati personali trattati su supporti cartacei possano venire a conoscenza del contenuto di documenti.

Principi da seguire quando si trattano dati personali

Come sancito dall'Articolo 5 ("Principi applicabili al trattamento di dati personali") del Regolamento 679/2016/UE i dati personali devono essere:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità […] («limitazione della finalità»);
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati […] («limitazione della conservazione»);
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Presupposti di liceità

Dati comuni

Per i dati comuni i presupposti di liceità enunciati all'articolo 6 del GDPR sono:

a. consenso da parte dell'interessato;
b. obbligo derivante da un accordo contratto;
c. obbligo di legge;
d. salvaguardia di interessi vitali;
e. compito di interesse pubblico connesso all'esercizio di pubblici poteri;
f. legittimo interesse del Titolare.

Per i presupposti elencati dalla lettera b) alla lettera e) non è necessario richiedere il consenso per il trattamento dei dati personali.

Dati particolari

Per le categorie di dati particolari, vi sono presupposti di liceità di carattere generale e trasversale e alcuni specifici per determinati ambiti di attività.

Presupposti di liceità di carattere generale e trasversale:

- consenso;
- salvaguardia di interessi vitali di una persona fisica o del terzo (no consenso);
- interesse pubblico (no consenso);
- dati resi manifestamente pubblici dell'interessato: l'interessato ha diffuso di propria iniziativa i dati particolari. In tal caso i titolari del trattamento hanno la liceità di trattarli senza consenso;
- esercitare un diritto in sede giudiziaria in quanto il diritto alla tutela giurisdizionale è prevalente rispetto a quello della tutela dei dati altrui;
- il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali: in tal caso il trattamento di dati è possibile anche senza il consenso nel momento in cui i dati siano relativi a soggetti membri o ex membri.

Presupposti di liceità di determinati ambiti di attività:

1 - Giuslavoristico:

- diritti specifici del Titolare e interessato in ambito di diritto del lavoro, della sicurezza sociale e protezione sociale;
- medicina del lavoro.

2 - Sanitario:

- finalità di medicina preventiva […], diagnosi, assistenza o terapia sanitaria o sociale;
- Interesse pubblico nell'ambito della sanità pubblica;
- Ricerca scientifica [es. sperimentazioni cliniche, studi osservazionali].

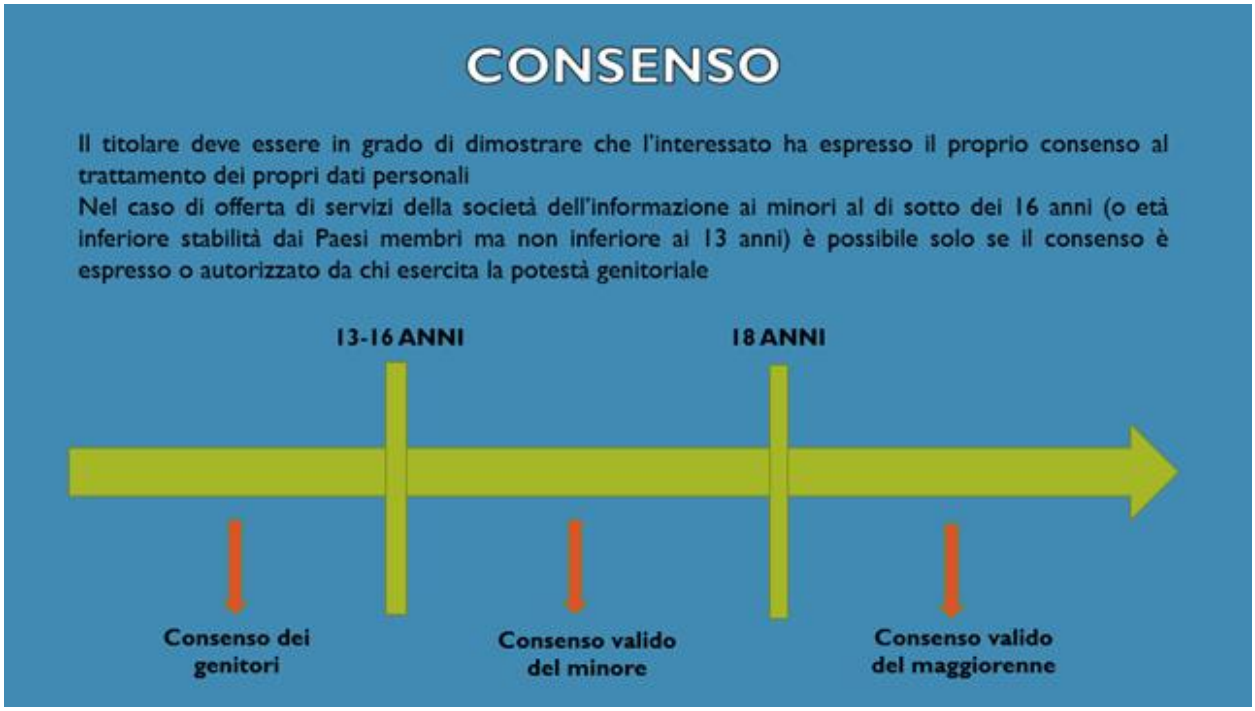
3 - Archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Consenso

Quando il Titolare del trattamento si trova nella condizione di dover effettuare un trattamento di dati personali che non derivi da uno dei presupposti di liceità (artt.6 e 9) **è obbligato a dover richiedere il consenso all'interessato**, prima di poter effettuare il trattamento.

L'interessato ha il diritto di prestare il proprio consenso dopo essere stato informato e messo nella condizione di essere libero nella scelta di concedere o meno il consenso. Deve prestarlo secondo le specifiche finalità per le quali sono raccolti i dati.

Il Titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato abbia prestato il suo consenso. Difatti, in caso di un possibile contenzioso, grava sul Titolare l'onere probatorio.



Informativa

L'informativa e in consenso sono due presupposti giuridici diversi.

L'informativa descrive le modalità in cui il Titolare del trattamento tratta i dati raccolti, mentre il consenso è richiesto solo nei casi in cui il trattamento non rientri nei presupposti di liceità già trattati precedentemente. A differenza del consenso (che resta un'attività residuale), **l'informativa va fornita all'interessato ogni qual volta vengano raccolti i suoi dati**.

L'informativa ha lo scopo di rendere edotto l'interessato delle modalità con cui vengono trattati i suoi dati da parte del Titolare del trattamento, mentre il consenso ha l'obiettivo di ricevere dall'interessato la possibilità di trattare i suoi dati.

L'informativa deve riportare:

a) identità del Titolare e dell'eventuale DPO

Il Titolare è 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. Il DPO (Data Protection Officer – Responsabile per la protezione dei dati), nuova figura del GDPR, rappresenta il punto di riferimento per i soggetti esterni che decidono di esercitare i propri diritti in ambito privacy nei confronti del Titolare del trattamento.

b) finalità del trattamento

Si tratta delle finalità per le quali sono raccolti i dati (es. attività promozionali, fatturazione, gestione del personale dipendente e collaboratori).

c) base giuridica

Si tratta dei presupposti di liceità.

d) ambito di circolazione dei dati

È necessario comunicare quali sono le categorie di soggetti esterni ai quali il Titolare può comunicare i dati personali raccolti. È in questa sezione che deve essere specificato se i dati possono essere trasferiti in Paesi extra UE.

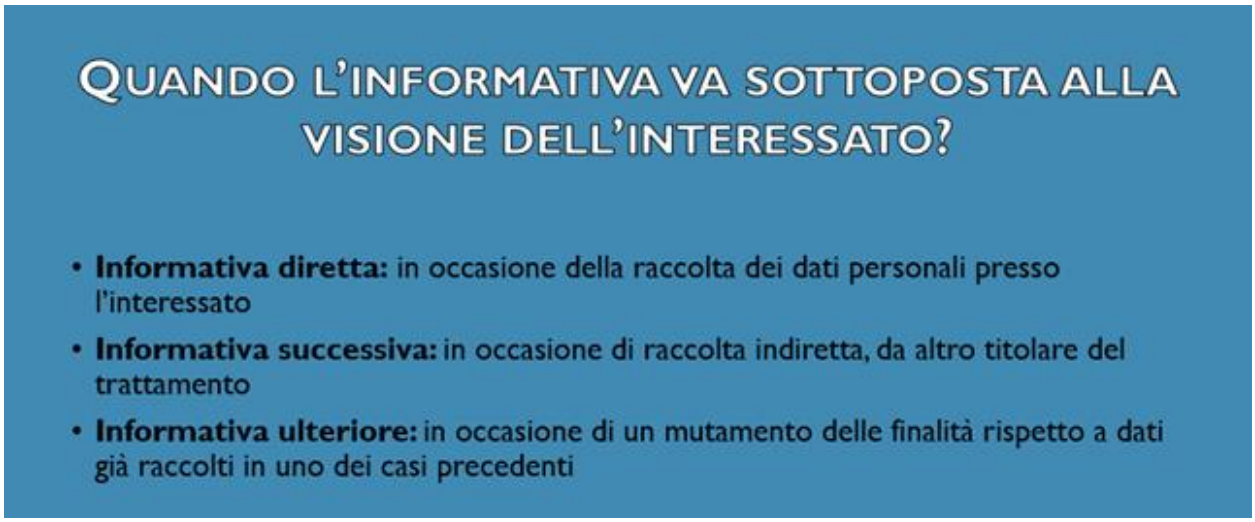
e) diritti dell'interessato

Il Titolare del trattamento deve comunicare le modalità attraverso le quali l'interessato può esercitare i diritti previsti dal GDPR.

f) durata del trattamento

L'interessato deve essere a conoscenza della durata del trattamento dei propri dati affinché non si verifichi un illecito (tempistica specifica individuata da parte del Titolare o l'indicazione dei criteri utilizzati per la determinazione dei termini di conservazione).

- Informativa diretta (art. 13): deve essere consegnata/comunicata dal Titolare del trattamento tutte le volte in cui raccoglie dati personali direttamente dall'interessato.
- Informativa successiva (art. 14): deve essere consegnata/comunicata dal Titolare del trattamento in un momento successivo alla raccolta di dati avvenuta da parte di un altro Titolare del trattamento.
- Informativa ulteriore (art. 13 par. 3): deve essere consegnata/comunicata quando sono cambiate le finalità per le quali il Titolare del trattamento aveva raccolto i dati in precedenza.



Diritti dell'interessato

L'Interessato deve avere sempre la possibilità di esercitare i propri diritti di cui al Regolamento 679/2016/UE Capo III – Diritti dell'interessato.

Il Titolare del trattamento ha l'obbligo di comunicare all'interessato quali sono i diritti che il GDPR gli riconosce e quali sono le modalità per esercitarli.

DIRITTO ALLA REVOCA DEL CONSENSO - Art. 7 par. 3 Reg. 679/2016/UE

L'interessato ha la facoltà di revocare, in qualsiasi momento, il consenso precedentemente prestato, con la stessa facilità con cui l'ha accordato. Questo diritto può essere sviluppato esclusivamente nel caso in cui il trattamento dei dati personali poggi sul presupposto di liceità del consenso; nel momento in cui il Titolare riceve la comunicazione di revoca del consenso ha l'obbligo di interrompere immediatamente il trattamento precedentemente accordato, pena l'illecito. Naturalmente il trattamento dati che si è sviluppato nella precedenza della revoca del consenso è pienamente valido.

DIRITTO DI ACCESSO DELL'INTERESSATO - Art 15 Reg. 679/2016/UE

L'interessato ha il diritto di poter accedere ai suoi dati al fine di essere consapevole delle modalità con le quali vengono trattati i dati, ma soprattutto per poter constatare che le modalità di trattamento enunciate dal Titolare nell'informativa, siano effettivamente rispettate.

DIRITTO ALLA RETTIFICA - Art. 16 Reg. 679/2016/UE

È il diritto riconosciuto all'interessato di modificare i propri dati precedentemente raccolto e trattato. Questo diritto è azionabile solo se i dati dell'interessato raccolti sono errati oppure hanno subìto una variazione dal momento in cui sono stati raccolti.

DIRITTO ALL' OBLIO (DIRITTO ALLA CANCELLAZIONE) - Art. 17 Reg. 679/2016/UE

Diritto all'oblio (o alla cancellazione) può essere richiesto qualora si verifichino uno dei seguenti casi, ovvero:

- i dati dell'interessato non sono più necessari rispetto alle finalità per cui sono stati raccolti;
- l'interessato in precedenza ha revocato il consenso;
- l'interessato si è opposto al trattamento di dati e non sussiste alcun motivo legittimo per continuare nel trattamento dei dati;
- i dati dell'interessato sono trattati in modo illecito;
- la legge ha imposto che i dati che sono stati raccolti per tale finalità devono essere cancellati;
- i dati dell'interessato sono raccolti sulla base di consenso prestato da minore relativamente all'offerta di servizi delle società dell'informazione.

I dati personali non possono essere cancellati, nonostante il diritto alla cancellazione, quando i dati sono trattati:

- nell'ambito all'esercizio del diritto alla libertà di espressione ed informazione;
- per adempimenti derivanti da un obbligo di legge, o se il trattamento è svolto nell'esercizio di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- ai fini di archiviazione e ricerca scientifica o storica (nel rispetto dell'art. 89, par. 1);
- perché necessari all'accertamento, esercizio o difesa di un diritto in sede giudiziaria.

DIRITTO DI LIMITAZIONE AL TRATTAMENTO - Art. 18 Reg. 679/2016/UE

Il diritto di limitazione concede all'interessato il diritto di richiedere al Titolare che il trattamento sia limitato per un determinato periodo di tempo. È possibile esercitarlo quando:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali;
- il trattamento è illecito, ma l'interessato si oppone alla cancellazione dei dati personali richiedendone la limitazione dell'utilizzo;

- il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto al trattamento in attesa dell'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Al par. 2 dell'art. 18, si afferma che se il trattamento è stato limitato in base ad uno dei sopra citati casi tassativi, i dati personali possono essere trattati, soltanto:

- con il consenso dell'interessato;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- per tutelare i diritti di un'altra persona fisica o giuridica;
- per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

DIRITTO ALLA PORTABILITA' DEI DATI - Art. 19 Reg. 679/2016/UE

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti.

L'interessato può azionare questo diritto nel momento in cui:

- il presupposto di liceità su cui si è sviluppato il trattamento dei dati, è il consenso;
- il trattamento sia effettuato con mezzi automatizzati.

Il Titolare a seguito di questo diritto promosso dall'interessato deve:

- trasmettere al richiedente tutti i dati di questa persona in suo possesso;
- trasmettere a soggetto individuato dal richiedente (nuovo Titolare di quel trattamento individuato dall'interessato) i dati di quest'ultimo, sempre se fattibile.

DIRITTO DI OPPOSIZIONE - Art. 21 Reg. 679/2016/UE

Tra la cerchia dei diritti annoverati in tema di privacy, il Legislatore Comunitario all'art. 21 del Regolamento, ha disciplinato inoltre il c.d. "Diritto di opposizione", il quale per definizione consente all'interessato di opporsi "in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano".

In virtù dell'esercizio di tale diritto, il Titolare potrà continuare a trattare i dati in suo possesso solo dove dimostri "l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria".

Allegato 1 - INTRODUZIONE AL REGOLAMENTO 679/2016/UE

Contestualizzazione nuovo regolamento

Il nuovo Regolamento Europeo - Regolamento (UE) 2016/679 del Parlamento Europeo (L. 119) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati è stato pubblicato sulla GUUE del 04 maggio 2016.

Il testo è disponibile alla risorsa:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Il Regolamento Europeo (di seguito indicato come "Regolamento UE" o come "GDPR") è direttamente applicabile e vincolante in tutti gli Stati membri e non richiede una legge di recepimento nazionale, fatta eccezione per alcuni ambiti sui quali rimanda, deroga o richiede l'integrazione regolatoria dei singoli Stati. La diversa forma dell'atto – da Direttiva a Regolamento, risponde alla primaria volontà del legislatore europeo di porre sullo stesso piano tutti gli Stati membri, garantendo medesimi diritti e doveri, assicurando uniformità alla protezione dei dati personali e certezza al diritto.

Il Regolamento UE è stato approvato il 27 aprile 2016, entrato in vigore il 25 maggio dello stesso anno con piena attuazione dal 25 Maggio 2018, data a partire dalla quale ha abrogato la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. Direttiva Madre). In data 4 settembre 2018 è stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo 101/2018 di armonizzazione al Regolamento UE che coordina la normativa nazionale con il nuovo regolamento europeo sulla privacy e che è entrato in vigore il 19 settembre 2018.

Campo di applicazione del regolamento

Le norme interessano tutti quei soggetti (anche extraeuropei) che sono chiamati a trattare (in maniera automatizzata o meno) i dati relativi, per esempio, a clienti, dipendenti, studenti, utenti, fornitori. In sostanza, viene introdotto il principio dell'applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o sevizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.

Il Regolamento, come espressamente affermato anche nei relativi considerando al testo, si applica anche al trattamento di identificativi prodotti da dispositivi, applicazioni, strumenti e protocolli, quali gli indirizzi IP, i cookies e i tag di identificazione a radiofrequenza, salvo il caso in cui tali identificativi non si riferiscano a una persona fisica identificata o identificabile. Le aziende e le istituzioni pubbliche sono tenute, pertanto, ad adottare politiche ed attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme - fin dalla fase embrionale - a tutte le disposizioni del Regolamento. Di importanza non secondaria, è l'impianto sanzionatorio. Al fine di rendere punibile chiunque, persona di diritto pubblico o di diritto privato, non ottemperi alle disposizioni del Regolamento, quest'ultimo ha richiesto agli Stati membri di garantire sanzioni efficaci, proporzionate e dissuasive e di adottare tutte le misure necessarie per la loro applicazione.

L'Autorità di Controllo può arrivare ad imporre sanzioni amministrative pecuniarie fino a 20 milioni di Euro o fino al 4% del fatturato mondiale annuo (se superiore) nel caso di un'impresa. Nella trattazione che segue viene fornita una sintesi, per punti distinti, delle principali e fondamentali novità derivanti dal nuovo Regolamento Europeo.

Cosa cambia con il nuovo regolamento

Il Regolamento UE cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali sebbene a una prima lettura possa rispecchiare una impostazione simile a quella della Direttiva Madre rispetto al costrutto portante (informativa, finalità, consenso), ai ruoli, ai diritti degli interessati e ai doveri dei titolari e dei responsabili.

Il GDPR consacra il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto alla autodeterminazione informativa. Questo è un principio portante fondato dalla Direttiva, che il Regolamento UE eredita, ma di cui ne ridisegna radicalmente l'implementazione passando dalla logica dell'adempimento prevalentemente formale ad un approccio regolatorio fortemente sostanziale e centrato sulla responsabilità di assicurare/mantenere la conformità al regolamento nonché di tutelare i diritti e la dignità degli interessati.

Il Regolamento UE, inoltre, traccia il passaggio da un diritto alla protezione dei dati personali di tipo *nazionale/individuale* ad un diritto di tipo *europeo/sociale*.

In generale il GDPR – collocandolo in questa premessa e provando a dimensionarlo su diritti-doveri-controllo:

- muta l'approccio regolatorio da "formale e re-attivo" in "sostanziale e pro-attivo", il trattamento e la protezione dei dati personali evolvono nell'acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali di una Organizzazione o di un'azienda;
- consolida le garanzie e i diritti azionabili dall'interessato per il controllo delle proprie informazioni e l'esercizio dell'autodeterminazione ereditati dalla Direttiva, riaffermandone molti (diritto all'accesso, rettifica, cancellazione, limitazione, revoca e opposizione); rafforzandone altri - in primis la disciplina del consenso del quale introduce un vera e propria definizione dell'istituto del consenso esplicito, e della trasparenza rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa; introducendone di nuovi (diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione);
- accresce le responsabilità del titolare e del responsabile con la positivizzazione del principio di accountability con la finalità di porre chi tratta i dati personali in una posizione di ridurre i rischi di operazioni non conformi o non consentite motivando, in tal senso, il titolare e il responsabile a comportamenti e prassi virtuose;
- centralizza la governance e il controllo sul rispetto e la conformità dei trattamenti alla normativa, tramite la cooperazione e la valorizzazione delle Autorità di Controllo nazionali verso il Comitato; incoraggiando meccanismi di certificazione; ampliando il sistema vigilanza; rafforzando quello sanzionatorio sia nelle specifiche comuni che nelle misure applicative.

Dovere di documentazione e di informazione

E' divenuto necessario elaborare un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento. È l'applicazione operativa del principio di rendicontazione (o di "accountability"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento (qualcosa di simile al Documento Programmatico sulla Sicurezza, ma di portata più ampia).

In tal senso, acquisisce ancora più importanza il principio di trasparenza e di informazione nei confronti dell'interessato, che il Titolare del trattamento fa valere sia attraverso l'adozione di politiche concise, trasparenti, chiare e facilmente accessibili, sia mediante la resa di informazioni e comunicazioni con un linguaggio semplice e chiaro (in particolare se le informazioni sono destinate ai minori). Ancora più rilevante diviene l'obbligo di resa dell'informativa privacy e della acquisizione "granulare" dei consensi (specifici per ogni tipologia di trattamento), quando dovuti. Il Regolamento amplia il contenuto da inserire nell'Informativa rispetto al dettato dall'art. 13 del D.Lgs. 196/2003.

Accresciuta responsabilità dei titolari e dei responsabili del trattamento.

La responsabilità dei titolari (art. 24 e 25) e del responsabile (art. 28) si configura come una sostanziale assunzione di rischio, atteso che il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, la conformità del trattamento al regolamento tenendo conto, inoltre, della natura, dell'obbligo, del contesto e delle finalità di trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le liberà delle persone fisiche.

A titolari e responsabili di trattamento si affianca una nuova figura obbligatoria per le pubbliche amministrazioni: il responsabile della protezione dei dati personali (c.d. "data protection officer").

Prioritariamente rientrano tra le responsabilità del Titolare e dei Responsabili: l'attuazione delle prassi di privacy by design/default, la valutazione d'impatto, la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi, la tenuta dei rispettivi registri delle attività di trattamento, la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto interessato.

Valutazione d'impatto sulla protezione dei dati

I Titolari sono tenuti ad effettuare una Valutazione degli impatti privacy (Data Protection Impact Analysis– DPIA) fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati. In particolare, a titolo meramente esemplificativo e non esaustivo, la DPIA va realizzata per

trattamenti quali: la valutazione sistematica di aspetti della personalità dell'interessato o quelli volti ad analizzarne la situazione economica, l'ubicazione, lo stato di salute, l'affidabilità o il comportamento, mediante un trattamento automatizzato; per trattamenti di dati concernenti la vita sessuale, la prestazione di servizi sanitari, lo stato di salute, la razza e l'origine etnica; o, ancora, per trattamenti di dati in archivi su larga scala riguardanti minori, dati genetici o dati biometrici, a sorveglianza di zone accessibili al pubblico, in particolare se effettuata mediante dispositivi ottico-elettronici (video-sorveglianza).

Stando a quanto disposto dal Considerando n° 70 del Regolamento, viene abolito l'obbligo di Notificazione di specifici trattamenti all'Autorità di Controllo (il nostro attuale Garante Privacy). Tale adempimento è considerato dal Legislatore europeo come un obbligo che comporta oneri amministrativi e finanziari senza aver mai veramente contribuito a migliorare la protezione dei dati personali (in particolare per le piccole e medie imprese). È pertanto necessario (continua il testo del Regolamento) abolire tale obbligo generale di notificazione e sostituirlo con meccanismi e procedure efficaci che si concentrino piuttosto su quelle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà degli interessati, per la loro natura, portata o finalità. In tali casi è necessaria una valutazione d'impatto sulla protezione dei dati, da effettuarsi prima del trattamento, che verta, in particolare, sulle misure, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare il rispetto del Regolamento.

L'Autorità di controllo redige e pubblica l'elenco di tipologie di trattamenti soggetti a preventiva valutazione di impatto.

La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti, delle finalità e l'eventuale ricorrenza di un legittimo interesse;
- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le previste misure organizzative e tecniche (comprese quelle di sicurezza) e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti interessati.

La responsabilità della valutazione d'impatto attiene prioritariamente il Titolare supportato dal Responsabile protezione dai dati.

Introduzione dei registri delle attività di trattamento – considerando 82, art. 30.

Il titolare e il responsabile di trattamento devono tenere i rispettivi registri delle attività.

Il registro del titolare deve contenere: riferimenti di contatto del titolare/i, del rappresentante del titolare del trattamento nell'Unione (in caso di non stabilimento nell'Unione) e del responsabile della protezione dei dati; le finalità; descrizione degli interessati e dei destinatari; la categoria dei dati personali trattati; la presenza di trasferimenti di dati verso un Paese Terzo un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie; la tempistica della cancellazione dei dati; la descrizione della misure di sicurezza e organizzative adottate.

Il registro del responsabile deve contenere oltre alle due ultime voci previste ed elencate per il registro del titolare: i riferimenti di contatto dei responsabili, dei titolari per conto dei quali operano, dei rappresentanti e del responsabile della protezione dei dati; le categorie dei trattamenti effettuati per conto del titolare.

Smaltimento di dispositivi e supporti contenenti dati personali

Permane l'obbligo di garantire la protezione dei dati anche mediante un'accurata cancellazione al momento della distruzione dei supporti che li contengono. Sul tema, si segnala un provvedimento dell'Autorità Garante su "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1571514).

Attuazione dei requisiti di sicurezza dei dati

L'attuale testo del Regolamento richiede la messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta. L'adeguatezza di tali misure deve derivare dai risultati della valutazione di impatto (DPIA), dall'evoluzione tecnica e dai costi di attuazione. Tale politica di sicurezza deve includere:

1. la capacità di assicurare che sia convalidata l'integrità dei dati personali;

2. la capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
3. la capacità di ripristinare la disponibilità e l'accesso ai dati in modo tempestivo, in caso di incidente fisico o tecnico che abbia un impatto sulla disponibilità, sull'integrità e sulla riservatezza dei sistemi e dei servizi di informazione;
4. in caso di trattamento di dati personali sensibili, misure di sicurezza aggiuntive per garantire la consapevolezza dei rischi e la capacità di adottare in tempo reale azioni di prevenzione, correzione e attenuazione, contro le vulnerabilità riscontrate o gli incidenti verificatisi, che potrebbero costituire un rischio per i dati;
5. un processo per provare, verificare e valutare regolarmente l'efficacia delle politiche, delle procedure e dei piani di sicurezza attuati per assicurare la continua efficacia.

Le misure appena citate devono come minimo:

1. garantire che ai dati personali possa accedere soltanto il personale autorizzato agli scopi autorizzati dalla legge;
2. proteggere i dati personali conservati o trasmessi dalla distruzione accidentale o illegale, dalla perdita o dalla modifica accidentale e dalla conservazione, trattamento, accesso o comunicazione non autorizzati o illegali;
3. assicurare l'attuazione di una politica di sicurezza in relazione con il trattamento dei dati personali.

È assai probabile che l'adesione a codici di condotta (approvati ai sensi dell'articolo 38 del Regolamento) o un meccanismo di certificazione (approvato ai sensi dell'articolo 39 del Regolamento) possano essere utilizzati come elementi per dimostrare la conformità ai requisiti di sicurezza sopra elencati. E' il Comitato europeo per la protezione dei dati l'ente deputato ad emettere orientamenti, raccomandazioni e migliori prassi, per le misure tecniche e organizzative, compresa la determinazione di ciò che costituisce l'evoluzione tecnica - per settori specifici e in specifiche situazioni di trattamento dei dati - in particolare tenuto conto degli sviluppi tecnologici e delle soluzioni per la protezione fin dalla progettazione e per la protezione di default. Inoltre, se necessario, la Commissione UE può adottare atti di esecuzione per precisare i requisiti delle misure sopra elencate, in particolare per:

1. impedire l'accesso non autorizzato ai dati personali;
2. impedire qualunque forma non autorizzata di divulgazione, lettura, copia, modifica, cancellazione o rimozione dei dati personali;
3. garantire la verifica della liceità del trattamento.

Privacy by design e protezione di default

Si tratta dell'esplicitazione del principio dell'incorporazione della privacy fin dalla progettazione del processo aziendale e degli applicativi informatici di supporto, ovvero la messa in atto di meccanismi per garantire che siano trattati - di default - solo i dati personali necessari per ciascuna finalità specifica del trattamento (si tratta della ri-attualizzazione in chiave moderna del principio di necessità sancito dal Codice Privacy). I Titolari del trattamento devono, pertanto, prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati - dalla raccolta alla cancellazione - incentrandosi sistematicamente sulle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica ed alla cancellazione dei dati.

Tali meccanismi vanno identificati sia nel momento in cui si definiscono le finalità e i mezzi del trattamento sia allatto del trattamento stesso, tenuto conto dell'evoluzione tecnica (e dei costi di attuazione) delle migliori prassi (best pratices) internazionali e dei rischi del trattamento. A livello operativo vuol dire sia fare in modo che la quantità dei dati raccolti e la durata della conservazione (o eventuale diffusione) non vada oltre il minimo necessario per le finalità perseguite, sia predisporre meccanismi che garantiscano che, di default, non siano resi accessibili dati ad un numero indefinito di persone e che gli interessati siano in grado di controllarne il flusso. Questo ha un forte impatto nello sviluppo di software destinati al trattamento di dati (es. CRM, ERP, gestionali aziendali) e sul rinnovamento del parco informatico delle amministrazioni, delle imprese e degli studi professionali.

Sicurezza e valutazione dei rischi - considerando 83, 84, art. 32

Il regolamento prevede misure di sicurezza idonee da adottare in relazione alla valutazione dei rischi.

Titolare e responsabile sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione, la cifratura; misure implementative della riservatezza, dell'integrità, della

disponibilità delle informazioni; la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico.

Le misure vanno contemperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento. Alcuni indicatori di rischio (soprattutto connessi ai trattamenti informatizzati) sono declinati nella definizione di violazione di dato personale.

Obblighi di segnalazione in caso di violazioni sui dati

Con la nozione di violazione dei dati personali (c.d. "personal data breaches"), si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati. I Titolari del trattamento, in caso di una violazione come sopra descritta, dovranno mettere in atto due differenti azioni: la notificazione della violazione all'Autorità di controllo e la segnalazione al diretto interessato.

Nel primo caso, accertata la violazione, la relativa notificazione deve contenere una serie nutrita di informazioni: la natura della violazione medesima, le categorie e il numero di interessati coinvolti; l'identità e le coordinate di contatto del DPO; l'elenco delle misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione dei dati; la descrizione degli impatti derivanti; le misure proposte o adottate per porre rimedio alla violazione e attenuarne gli effetti. Inoltre, l'Autorità di Controllo conserva un registro pubblico delle tipologie di violazione notificate. Nel caso in cui, poi, la violazione rischi di pregiudicare i dati, attentare alla vita privata, ai diritti o agli interessi legittimi dell'interessato, il Titolare, dopo aver provveduto alla notificazione, deve comunicare la violazione al diretto interessato senza ritardo. In mancanza l'Autorità di Controllo, considerate le presumibili ripercussioni negative della violazione, può obbligare il Titolare a farlo. La comunicazione all'interessato deve essere esaustiva e redatta in un linguaggio semplice e chiaro e descrivere la natura e le conseguenze della violazione, le misure raccomandate per attenuare i possibili effetti pregiudizievoli, i diritti esercitabili dall'interessato.

La comunicazione non è richiesta quando il Titolare dimostra in modo convincente all'Autorità di Controllo di aver utilizzato le opportune misure tecnologiche di protezione (es. cifratura) e che tali misure sono state applicate, proprio, ai dati violati (es. furto tablet con dati sanitari cifrati). Queste misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

Diritti dell'interessato

Consenso – considerando 39 e 42, art. 6, 7

Il consenso in generale deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto.

Deve essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente (come la selezione di un'apposita casella in un sito web, la scelta di specifiche impostazioni tecniche o qualsiasi altra dichiarazione o comportamento che indichi chiaramente la volontà dell'interessato di accettare il trattamento proposto). Non è richiesta necessariamente la forma scritta anche se questa risulta essere la modalità più idonea ad accertare che il consenso sia stato inequivocabilmente fornito e che sia esplicito.

Si precisa che nel caso il trattamento richieda il consenso, il titolare dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto.

Per il trattamento di dati sensibili (il GDPR parla di categorie particolari di dati) è necessario il consenso (art.9 comma 2 lettera a)) a meno che il trattamento non sia necessario per la tutela di diritti di grado superiore dell'interessato stesso o pubblici o di terzi, oppure per obbligo di legge, qualora l'interessato non sia in grado di fornire il consenso (art. 9 comma 2 lettere c, f, g, i, j).

Informativa – considerando da 58 a 73, art. 12, 13, 14

Il titolare del trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisire il consenso, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13 co. 4) o in altri casi particolari descritti nel regolamento (art. 14 co. 5).

Contenuti dell'informativa

Il titolare del trattamento è tenuto a informare il soggetto interessato in merito a:

- identità e dati di contatto del titolare del trattamento, del suo rappresentante e del responsabile della protezione dei dati personali;

- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento ed i legittimi interessi perseguiti dal titolare del trattamento o da terzi (qualora sia basato sull'art. 6, paragrafo 1, lettera f) del GDPR);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti di cui all'articolo 46 e 47, o all'articolo 49, comma 2, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'interessato comprendenti: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione; oltre al diritto alla portabilità dei dati; la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; il diritto di proporre reclamo a un'autorità di controllo;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative circa la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

A riguardo si segnalano alcuni punti di attenzione:

- Deve essere chiarito l'eventuale trasferimento di dati in un paese terzo (ad esempio nel caso di utilizzo di servizi cloud). Si ricorda che anche per tali servizi è responsabilità del titolare garantire la sicurezza dei dati e le modalità di accesso da parte dell'interessato.
- Rispetto alla normativa previgente, occorrerà garantire – in specifici casi - la limitazione del trattamento dati e la portabilità dei dati.
- La necessità di indicare eventuali processi automatici di profilazione e le conseguenze per l'interessato di tale trattamento dati.

Si precisa che:

- nel caso in cui i dati siano raccolti presso l'interessato, il titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, dovrà fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente
- nel caso in cui i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, potrà non fornire l'informativa all'interessato qualora risulti impossibile o farlo implicherebbe uno sforzo sproporzionato (in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici e fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di rendere l'informativa rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In questo caso, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.

<u>Caratteristiche dell'informativa</u>

Il regolamento specifica in dettaglio le caratteristiche espositive dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; veicolata da un linguaggio chiaro e semplice, soprattutto nel caso in cui gli interessanti siano minori.

Per agevolare la comprensione, il regolamento incoraggia l'utilizzo di icone in combinazione con la forma estesa per presentare i contenuti dell'informativa in forma sintetica, icone che dovranno essere identiche in tutta l'UE e dovranno essere definite dalla Commissione.

Una maggiore comprensione e chiarezza dell'informativa si potrebbe altresì ottenere mediante la redazione di più informative che si differenzino, ad esempio, in relazione alle diverse categorie di interessati e/o servizi resi loro disponibili.

Diritti "tradizionali" – considerando da 58 a 73, art. 12 a 17

I diritti azionabili dall'interessato già previsti dalla Direttiva e dal Codice, oltre a quello di ricevere idonea informativa riguardano: il diritto di accesso, la rettifica, la cancellazione, l'opposizione al trattamento.

Tra le novità previste nel nuovo GDPR rispetto alla Direttiva 95/46/CE e al Codice Italiano si citano:

- il riscontro deve essere fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Nel caso di diniego, il riscontro deve essere fornito al più tardi entro un mese dal ricevimento della richiesta
- la definizione da parte del titolare di eventuali oneri sull'interessato nei casi particolari previsti nell'art. 12 comma 5.

A differenza della normativa previgente, è posto meno l'accento sul riscontro da fornire all'interessato per quanto attiene le modalità del trattamento: viceversa è posto l'accento su altri elementi come, ad esempio, il periodo di conservazione e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi. Si precisa inoltre che, la risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Nuovi Diritti: diritto di limitazione; diritto di opposizione alla profilazione; diritto alla cancellazione / all'oblio; diritto alla portabilità; – art. 18, 20, 21, 22

Questi nuovi diritti estendono o rafforzano analoghi diritti presenti nella Direttiva e attuati dal Codice Italiano.

Il diritto alla limitazione rappresenta un diritto diverso e più esteso rispetto al "blocco" del trattamento già previsto dal codice, in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante.

Il diritto di opposizione alla profilazione che riconosce all'interessato il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare (legata ad esempio al proprio rendimento professionale o alla propria situazione economica, di salute, ecc…), al trattamento dei dati personali che lo riguardano compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata nel caso questi siano stati resi pubblici on-line. I titolari hanno l'obbligo di informare della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". Inoltre l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

Il diritto alla portabilità si applica ai dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo per i dati che siano stati "forniti" dall'interessato al titolare; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare.

Sintesi delle principali novità

Le principali novità sono sintetizzate per parole chiave nelle seguenti tabelle.

Consenso	Libero, specifico, informato, inequivocabile e concludente.
Informativa	Informazioni di contatto titolare, rappresentante e responsabile protezione dei dati; indicazione della finalità di trattamento; destinatari e categorie di dati trattati; trasferimento dati personali in paesi terzi; diritti azionabili e implicazioni; ricorrenza di altre basi giuridiche diverse dal consenso. Usabilità dell'esposizione.
Valutazione impatto	Ripensamento delle tecnologie a supporto dei trattamenti. Analisi e eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e le libertà delle persone. Obbligo del titolare, supportato dal responsabile protezione dati.
Sicurezza	Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative. Obbligo congiunto del titolare e del responsabile del trattamento dati.
Violazione dei dati	Equiparazione della fattispecie accidentale con quella dolosa.
Privacy by Design	Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio.
Privacy by Default	Pseudonimizzazione e Minimizzazione (di dati e tempi) come garanzia e misura di PbD. Obbligo del titolare.
Responsabile PDP (detto anche DPO)	Si interfaccia con le Autorità Garanti. Supporta titolare e responsabile del trattamento. Obbligatorio nelle PA.
Registro Trattamenti	Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono titolare e responsabile del trattamento.
Sanzioni	Sanzioni amministrative pecuniarie fino a 20 000 000 EUR. (per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente).
Autorità	Comitato di controllo europeo: assicura la uniforme applicazione del Regolamento. Autorità di Controllo: autorità pubblica indipendente di uno Stato membro.

NUOVI DIRITTI

Profilazione	L'interessato ha il diritto di non subire trattamenti automatizzati (profilazione) inconsapevoli.
Portabilità dei Dati	L'interessato ha il diritto ottenere la restituzione dei propri dati personali trasmessi e trattatati da un titolare e trasmetterli ad altri.
Oblio	L'interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.
Sportello Unico	Unicità dell'interlocutore territoriale. Semplificazione e uniformità di gestione nell'applicazione del nuovo regolamento.

I soggetti del trattamento

Il GDPR individua i soggetti coinvolti nel trattamento sulla base:

1) delle finalità per le quali sono raccolti:

- il Titolare è la persona giuridica o la persona fisica che raccoglie i dati personali per proprie finalità e decide i mezzi per il trattamento;
- il Contitolare è la persona giuridica o la persona fisica che condivide le finalità con altro Contitolare e stabilisce insieme a questi le modalità di trattamento,
- il Responsabile del trattamento è la persona giuridica o la persona fisica che esegue dei trattamenti di dati per conto del Titolare, sulla base di un contratto o altro atto giuridico,
- il Destinatario è la persona giuridica o la persona fisica che riceve i dati dal Titolare per eseguire i trattamenti secondo le istruzioni ricevute o che esegue trattamenti per proprie finalità, nel qual caso diventa a sua volta Titolare per i trattamenti dei dati ricevuti,
- il soggetto autorizzato è la persona fisica che ha ricevuto dal titolare precise istruzioni per l'esecuzione dei trattamenti dati di sua competenza;
- l'interessato è la persona fisica che fornisce i propri dati personali a un Titolare per le finalità specificate nell'informativa;

2) delle caratteristiche del Titolare/Responsabile e delle tipologie e quantità di dati trattati:

- il Responsabile della Protezione dei Dati è la persona giuridica o la persona fisica che segue tutti i vari aspetti relativi all'applicazione del GDPR per conto del Titolare/Responsabile, deve obbligatoriamente essere presente nelle pubbliche amministrazioni;

3) dell'ambito territoriale:

- il Rappresentante nell'Unione del Titolare/Responsabile che ha la propria sede in uno stato terzo è la persona giuridica o la persona fisica che su mandato del Titolare/Responsabile funge da interlocutore per gli interessati e per le Autorità di controllo dell'Unione (ferma restando la responsabilità generale del titolare del trattamento o del responsabile del trattamento);
- l'Autorità di Controllo è la persona giuridica pubblica istituita da ogni Stato membro per sovrintendere all'applicazione e al rispetto del GDPR nell'ambito del proprio territorio;
- il Comitato Europeo per la Protezione dei Dati è la persona giuridica che a livello europeo ha il compito di coordinare il lavoro delle varie Autorità di Controllo e di supportare la Commissione.

Titolare del trattamento

Il titolare è definito all'art. 4 come "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". Pertanto Il Titolare non viene designato o nominato ma diventa tale al momento che raccoglie dati personali con l'intento di trattarli per finalità lecite, come previsto all'art. 6, e decide le modalità di trattamento.

Contitolare

Il soggetto terzo che condivide le decisioni sulle finalità per le quali trattare i dati e che contribuisce a definire le modalità di trattamento. Il contenuto essenziale dell'accordo stipulato fra i contitolari deve essere reso noto all'interessato. Questi può esercitare i propri diritti nei confronti di ogni contitolare.

Responsabile del trattamento dati

Il GDPR definisce all'art. 4 il Responsabile del trattamento quale "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" e ne descrive le funzioni all'art. 28. Differisce dalla figura di responsabile prevista dall'attuale Codice, soprattutto per quanto concerne il rispondere in solido con il Titolare di eventuali inadempienze.

Il responsabile del trattamento dati è un soggetto esterno che esegue, in base a un contratto/convenzione o altro atto giuridico, dei trattamenti di dati personali per conto del titolare e ne risponde in solido in caso di inadempienze. Al Responsabile spettano tutti i compiti del Titolare all'interno del proprio organismo (valutazione impatto, registro dei trattamenti, eventuale nomina del Responsabile della Protezione Dati, ecc.) Il Responsabile così individuato non può a sua volta nominare un altro Responsabile se non dietro autorizzazione scritta del Titolare: la catena delle responsabilità deve essere nota al Titolare. Nei contratti con sub-responsabili devono essere riportati gli stessi obblighi in materia di protezione dei dati personali previsti dal contratto tra responsabile e titolare.

Nell'informativa devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento. Nel caso di trasferimento di dati in un paese terzo è obbligatorio informare di ciò l'interessato e il Titolare deve verificare che il responsabile assicuri un'adeguata protezione dei dati.

Soggetti autorizzati

Nelle linee guida del Garante si afferma che "le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento", ne consegue che quanto disposto all'art. 29 del GDPR possa concretizzarsi con l'individuazione dei soggetti autorizzati al trattamento dati all'interno dell'Organizzazione, prima denominati "incaricati". È sottolineata l'importanza di "istruire" i soggetti, sarà quindi opportuno prevedere percorsi formativi adeguati per coloro che saranno coinvolti nel trattamento dati.

Nell'informativa devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento.

Analogamente a quanto è stato fatto fino ad oggi, è possibile individuare i soggetti che sono autorizzati al trattamento dei dati, mediante una nomina individuale da parte del Titolare o Responsabile del trattamento dati, oppure individuando i trattamenti che competono all'unità organizzativa di afferenza del soggetto, che risulta pertanto incaricato per "documentata preposizione ad unità organizzativa".

La necessità di prevedere la designazione per iscritto del singolo incaricato o la documentata preposizione così come concepita dall'attuale normativa, non emerge in maniera esplicita dall'art. 29 del GDPR. Il termine" istruzione" del soggetto da parte del titolare indica che è necessaria una formazione/informazione specifica alla persona per ritenerla "autorizzata" ai trattamenti di dati personali di sua competenza. Del resto, già nella disposizione "data protection by default and by design" è previsto che in fase di progettazione di un'attività, che comporti trattamenti di dati personali, debbano essere individuate le misure di sicurezza idonee alla protezione dei dati e di conseguenza anche le opportune istruzioni per gli incaricati.

L'individuazione dei soggetti autorizzati al trattamento dati è una misura di sicurezza a livello organizzativo che comunque il Titolare è tenuto ad adottare.

Salvo ulteriori precisazioni da parte del Garante, gli amministratori di sistema risultano essere incaricati con particolari compiti, pertanto per questa tipologia è opportuno mantenere la nomina individuale.

Data Protection Officer – DPO (o Privacy Officer)

Già nel 2006, il Presidente del Garante Privacy Francesco Pizzetti, affermava "Vedo con molto favore l'istituzione della figura del Data Protection Officer (DPO) specialmente per le aziende e le corporation medie e grandi. La diffusione di questa figura non potrebbe che aiutare l'azione del Garante e la diffusione stessa della privacy nell'ambito delle strutture di impresa". Con l'avvento del nuovo Regolamento Ha trovato previsione la nuova figura del "Responsabile per la protezione dei dati". E' divenuto obbligatorio nominare il DPO nei seguenti casi:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari / sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il DPO va designato per un dato periodo ed in funzione delle qualità professionali, della conoscenza specialistica della normativa. I Titolari del trattamento devono assicurarsi che ogni altra eventuale funzione professionale della persona che riveste il ruolo di DPO sia compatibile con i compiti e le funzioni dello stesso in qualità di DPO e non dia adito a conflitto di interessi (deve quindi essere autonomo, indipendente e non ricevere alcuna istruzione per l'esercizio delle sue attività). Il DPO, il cui mandato può essere rinnovabile, può essere assunto oppure adempiere ai suoi compiti in base a un contratto di servizi. Il Titolare del trattamento, che a seconda della forma contrattuale, può essere datore di lavoro o committente, deve fornire al DPO tutti i mezzi inclusi il personale, i locali, le attrezzature e ogni altra risorsa necessaria per adempiere alle sue funzioni e per mantenere la propria conoscenza professionale. I principali compiti del DPO, il cui nominativo va comunicato all'Autorità di Controllo e al pubblico, sono quelli di:

- sensibilizzare e consigliare il Titolare in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti Regolamento;
- sorvegliare l'applicazione delle politiche compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli audit connessi;

- sorvegliare l'applicazione del Regolamento, con particolare riguardo alla protezione fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni dell'interessato ed alle richieste degli stessi per esercitare i diritti riconosciuti;
- controllare che il Titolare effettui la Valutazione d'impatto sulla protezione dei dati (c.d. DPIA) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
- fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento e consultarla, se del caso, di propria iniziativa;
- informare i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

Si può quindi affermare che ci si è incamminati verso la creazione di una nuova categoria professionale che deve disporre di precise e specifiche competenze sia giuridiche che informatiche nell'ambito della protezione dei dati personali. Allo stato attuale lo schema di certificazione più attendibile realizzato per attestare le competenze dei professionisti chiamati a svolgere il ruolo di DPO in outsourcing è quello realizzata dall'ente di certificazione TUV Italia (Schema di certificazione CDP) il cui registro pubblico degli abilitati è rinvenibile al seguente indirizzo: http://www.tuv.it/it-it/area-clienti/ricerca-figure-professionali-certificate.

Destinatario

Il GPDR all'art. 4 definisce destinatario "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi". Pertanto debbono essere considerati destinatari tutti i soggetti che ricevono dati personali da un titolare, sia che siano interni o esterni, sia che li ricevono per eseguire trattamenti per conto del titolare sia che li ricevono per conseguire proprie finalità. I destinatari o le categorie di destinatari ai quali verranno comunicati i dati devono essere definiti in fase di raccolta dei dati per inserirli nell'informativa all'interessato. Nel caso che il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, è richiesto che il Titolare verifichi che le garanzie offerte da questi per la protezione dei dati siano adeguate.

Nell'informativa da fornire all'interessato devono essere indicati i destinatari o le categorie di destinatari ai quali saranno comunicati i dati, dovranno essere elencati anche le strutture interne o le categorie di personale che verranno a conoscenza dei dati personali nello svolgimento della loro attività lavorativa.

Nel caso il destinatario sia un soggetto "terzo" che riceve i dati per perseguire proprie finalità, diventerà a sua volta titolare. Il destinatario che riceve i dati da altro titolare per perseguire finalità proprie è tenuto a dare l'informativa all'interessato nel più breve tempo possibile, sempre che ciò non sia impossibile o richieda uno sforzo sproporzionato o se l'interessato dispone già dell'informazione o nel caso in cui la comunicazione sia necessaria per adempiere a un obbligo di legge.

Interessato

L'interessato (data subject) è la persona fisica alla quale si riferiscono i dati trattati. È sempre una persona fisica. L'interessato è quindi il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del titolare del trattamento. Il GDPR al Capo III elenca nel dettaglio tali diritti. Alcuni di questi, a seconda della finalità per la quale i dati sono stati raccolti, potrebbero non essere esercitabili dagli interessati. La risposta alle richieste dell'interessato deve comunque essere tempestiva e, anche nel caso non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto. Il titolare ha il compito di facilitare l'accesso all'interessato ai suoi dati, predisponendo dei canali di comunicazione dedicati, quali ad esempio i recapiti del Responsabile della Protezione dei Dati.

Per la descrizione dei trattamenti si usa raggruppare gli interessati in categorie omogenee a seconda del tipo di rapporto che questi hanno con il titolare.

Autorità di controllo e comitato europeo

Le autorità di controllo sono incaricate di "sorvegliare l'applicazione del presente regolamento (GDPR) al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (punto 1) art. 51 del GDPR).

Ogni stato membro istituisce una o più autorità pubbliche indipendenti. Nel caso siano più di una deve essere designata quella che le rappresenterà nel Comitato europeo per la protezione dei dati, che ha funzioni di coordinamento delle varie autorità di controllo, per rendere coerenti e in linea con il GDPR le varie decisioni che a queste competono. Il Comitato ha inoltre funzioni di supporto per la Commissione europea.

All'Autorità di controllo nazionale devono essere comunicati eventuali data breach.

Le Autorità di controllo sono competenti ad accogliere e decidere su eventuali reclami presentati dagli interessati.

Conclusioni sul nuovo regolamento europeo

La rilevanza generale del regolamento, come appare chiaro, ha una notevole portata. Non si tratta di una semplice revisione, bensì di un intervento normativo a fronte dell'esperienza maturata negli ultimi anni su settori sino ad oggi solo sfiorati, che avrà effetti anche sulla concezione stessa della 'privacy', facendola calare sempre all'interno dei processi e dell'organizzazione aziendale non più come elemento/adempimento successivo ma presupposto ancillare e propedeutico già nelle fasi di progettazione dei processi. Il fine primario del nuovo quadro giuridico è, poi, quello di apportare migliorie per le persone fisiche e per i Titolari del trattamento (aziende, imprese, enti pubblici), di dimostrarsi valido anche per i prossimi anni ed in grado di reggere gli impatti posti, in particolare, dall'avvento delle nuove tecnologie (pensiamo per esempio alle sfide, in ottica privacy, derivanti dal Cloud Computing o dall'Internet of Things - IoT). Si può quindi affermare che si sta assistendo ad un passaggio da un sistema di tipo formalistico come quello attuale, ad uno di alta responsabilizzazione sostanziale in cui è richiesto un ruolo proattivo ai Titolari del trattamento.

In conclusione, una risposta efficace ed efficiente agli obblighi sopra descritti non può non passare dalla predisposizione e formalizzazione di un preciso organigramma privacy interno che "regoli il traffico" e vada a definire il "chi fa cosa", coerentemente alle mansioni aziendali. Di non meno importanza è anche, da una parte la predisposizione, a livello contrattuale in caso di trattamenti esternalizzati, di precise clausole che prevedano la sottoscrizione di Service Level Agreement (SLA) o Privacy Level Agreement (PLA), dall'altra la predisposizione di un "Sistema 231" (responsabilità amministrativa delle persone giuridiche), che si sostanzi sempre più in pratiche di controllo interno aziendale - anche secondo le schema PDCA: Plan, Do, Check, Act - per la protezione dell'organizzazione dalla commissione dei reati presupposto quali i reati informatici ed i trattamenti illeciti di dati (di cui, in particolare, all'art. 24 del D.Lgs. 231/2001).