POLICY PRIVACY AZIENDALE

REGOLAMENTO

Azienda tutela della salute Liguria (Ats Liguria)

Area Sociosanitaria Locale 5

Versione aggiornata al nuovo assetto organizzativo decorrente dal 1 gennaio 2026

Sommario

Premessa

Il presente testo sostituisce, per l'Area Sociosanitaria Locale 5, il precedente regolamento privacy aziendale riferito ad ASL 5, mantenendone l'impianto operativo e aggiornandone i contenuti essenziali al nuovo assetto organizzativo regionale.
Ai fini del presente regolamento si assume che, a seguito della Legge Regionale Liguria n. 18 del 12 dicembre 2025, a decorrere dal 1 gennaio 2026 le cinque Aziende sociosanitarie liguri e Liguria Salute si siano fuse in un'unica azienda regionale denominata Azienda tutela della salute Liguria, di seguito "**Ats Liguria**". Ats Liguria si articola in un'Area di gestione dei servizi accentrati e in cinque Aree sociosanitarie locali, di seguito anche "Asl", che erogano agli assistiti servizi e prestazioni sociosanitarie in continuità territoriale con le cessate Aziende.

Per effetto del nuovo assetto organizzativo, Ats Liguria, con sede in piazza della Vittoria, 15 - 16121 Genova, PEC protocollo@pec.atsliguria.it ed e-mail protocollo@atsliguria.it, assume la qualità di titolare del trattamento dei dati personali degli interessati afferenti alle Aziende sociosanitarie 1, 2, 3, 4, 5 e a Liguria Salute. Rimangono invariate le finalità e le modalità del trattamento, salvo gli adeguamenti organizzativi necessari alla gestione unitaria del sistema privacy regionale.

Il Responsabile della protezione dei dati nominato da Ats Liguria è raggiungibile all'indirizzo rpd@alisa.liguria.it. Gli interessati possono scrivere a tale indirizzo per l'esercizio dei diritti previsti dagli artt. 15 e seguenti del Regolamento (UE) 2016/679. Per l'Area Sociosanitaria Locale 5 è possibile scrivere anche a privacy@asl5.liguria.it.

Art. 1 Oggetto ed ambito di applicazione

Il presente regolamento disciplina, in attuazione del Regolamento (UE) 2016/679, di seguito anche "GDPR" o "Regolamento", del D.lgs. 30 giugno 2003, n. 196, come adeguato dal D.lgs. 10 agosto 2018, n. 101 e dalle successive disposizioni applicabili, nonché della normativa nazionale e regionale di settore, le operazioni di trattamento di dati personali effettuate da Ats Liguria e dai soggetti che operano sotto la sua autorità o per suo conto nell'ambito dell'Area Sociosanitaria Locale 5.

L'espressione "Area Sociosanitaria Locale 5" indica l'articolazione organizzativa territoriale di Ats Liguria e non un autonomo titolare del trattamento.

Rientrano nell'ambito di applicazione i trattamenti effettuati per finalità di prevenzione, diagnosi, cura, riabilitazione, assistenza sociosanitaria, medicina del lavoro, sanità pubblica, gestione amministrativa e contabile, gestione del personale, tutela del patrimonio aziendale, ricerca scientifica e statistica nei limiti previsti dalla legge.

Il presente regolamento tiene conto dei provvedimenti e degli orientamenti del Garante per la protezione dei dati personali in materia sanitaria, dossier sanitario, Fascicolo sanitario elettronico, data breach, trasparenza amministrativa, lavoro, posta elettronica e uso di tecnologie digitali, nonché delle linee guida e dei pareri dell'EDPB pertinenti ai diritti degli interessati, alla notifica delle violazioni di dati personali, ai trasferimenti verso Paesi terzi, alla pseudonimizzazione e ai trattamenti connessi a sistemi di intelligenza artificiale.

Ats Liguria garantisce che i dati personali, compresi quelli conservati negli archivi analogici e digitali ereditati dalle Aziende cessate, siano trattati nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone, secondo criteri di liceità, correttezza, trasparenza, minimizzazione, sicurezza, integrità, riservatezza e responsabilizzazione.

Restano ferme le norme speciali in materia sanitaria, sociosanitaria, documentazione clinica, cartelle cliniche, referti, Fascicolo sanitario elettronico, dossier sanitario, amministrazione digitale, trasparenza, accesso agli atti, segreto professionale, segreto d'ufficio, archivi pubblici e conservazione documentale.

Art. 2 Accountability e Sistema Privacy Aziendale

Ats Liguria per l'Area Sociosanitaria Locale 5 adotta un Sistema Privacy Aziendale fondato sul principio di responsabilizzazione. Il Sistema Privacy comprende l'insieme delle misure tecniche, organizzative, documentali e formative mediante le quali l'Azienda garantisce e dimostra la conformità dei trattamenti alla normativa applicabile.

Il Sistema Privacy Aziendale è definito tenendo conto della natura, dell'ambito di applicazione, del contesto, delle finalità dei trattamenti e dei rischi per i diritti e le libertà degli interessati, con particolare riguardo ai trattamenti su larga scala di dati relativi alla salute e di altre categorie particolari di dati.

Fanno parte del Sistema Privacy Aziendale per l'Area Sociosanitaria Locale 5:

- l'attribuzione formale dei ruoli privacy, delle responsabilità e delle autorizzazioni al trattamento;
- la designazione del referente del Responsabile della protezione dei dati per l'Area Sociosanitaria Locale 5 e la definizione dei relativi canali di contatto;
- il Registro delle attività di trattamento per l'Area Sociosanitaria Locale 5 e la valutazione periodica dei rischi;
- le informative agli interessati, i modelli di consenso ove richiesti, le procedure di revoca e le procedure di oscuramento;

- le valutazioni d'impatto sulla protezione dei dati e, ove necessario, la consultazione preventiva dell'Autorità Garante;
- le procedure per la gestione delle richieste di esercizio dei diritti;
- le misure di sicurezza fisica, logica, organizzativa e documentale;
- le procedure per la gestione delle violazioni dei dati personali;
- i contratti e gli atti di nomina dei responsabili esterni e dei sub-responsabili;
- le attività di formazione, verifica, audit e riesame periodico.

Il Sistema Privacy Aziendale è soggetto a riesame periodico e comunque in occasione di modifiche organizzative, tecnologiche, normative o contrattuali che possano incidere sui trattamenti, sui rischi o sui diritti degli interessati.

Nel periodo di transizione derivante dalla fusione regionale, gli atti, le procedure e le misure adottati dalle Aziende cessate restano applicabili solo se compatibili con il nuovo assetto di Ats Liguria e fino alla loro revisione o sostituzione con atti aziendali unitari.

Art. 3 Finalità del trattamento dati

L'Azienda tratta dati personali per l'esercizio dei compiti istituzionali attribuiti al Servizio sanitario nazionale, al Servizio sanitario regionale e alla normativa di settore.

Le principali finalità perseguite sono:

- erogare prestazioni sanitarie e sociosanitarie di prevenzione, diagnosi, cura, riabilitazione, assistenza, emergenza-urgenza, continuità assistenziale e medicina territoriale;
- gestire i percorsi di presa in carico, compresi ricoveri, accessi ambulatoriali, assistenza domiciliare, consultori, servizi per le dipendenze, salute mentale, screening e programmi di sanità pubblica;
- adempiere obblighi di legge in materia sanitaria, amministrativa, contabile, fiscale, assicurativa, previdenziale, contrattuale, di prevenzione della corruzione, trasparenza e controllo interno;
- tutelare la salute e la sicurezza dei lavoratori, dei pazienti, degli utenti, dei visitatori e della collettività;
- gestire il rapporto di lavoro, collaborazione, convenzione, tirocinio, formazione, volontariato o altro rapporto giuridico con Ats Liguria;
- gestire forniture, appalti, contratti, contenzioso, coperture assicurative, sinistri, reclami, segnalazioni e rapporti con autorità pubbliche;
- svolgere attività di programmazione, governo sanitario, controllo di qualità, audit clinico e amministrativo, valutazione delle performance, statistica e epidemiologia nei limiti previsti dalla legge;
- svolgere attività didattica, formativa, scientifica e di ricerca, ove consentito dalla normativa e nel rispetto delle garanzie applicabili.

I dati di dipendenti, collaboratori e soggetti equiparati sono trattati per le finalità connesse alla gestione del rapporto giuridico, economico, organizzativo e di sicurezza, con esclusione di impieghi ulteriori non fondati su una base giuridica idonea o incompatibili con la finalità originaria.

Ogni nuovo trattamento o modifica sostanziale di trattamento deve essere ricondotto a una finalità determinata, esplicita e legittima, registrata nel Registro delle attività di trattamento e valutata secondo il rischio.

Art. 4 Titolare e contitolari del trattamento dati

Ats Liguria, in persona del Direttore Generale quale legale rappresentante pro tempore, è il titolare del trattamento dei dati personali trattati per l'esecuzione dei compiti istituzionali e per le ulteriori finalità previste dalla legge.

In qualità di titolare, Ats Liguria determina le finalità e i mezzi essenziali dei trattamenti e, anche per il tramite dell'Area Sociosanitaria Locale 5, adotta misure tecniche e organizzative adeguate, individua i ruoli privacy, fornisce istruzioni ai soggetti autorizzati, designa i responsabili esterni del trattamento, tiene il Registro delle attività e garantisce l'esercizio dei diritti degli interessati.

Le Aree sociosanitarie locali, compresa l'Area Sociosanitaria Locale 5, operano come articolazioni organizzative di Ats Liguria. I loro direttori, responsabili, dirigenti, coordinatori, referenti e operatori trattano dati nell'ambito delle attribuzioni ricevute e secondo le istruzioni aziendali.

Quando Ats Liguria determina con uno o più soggetti le finalità e i mezzi del trattamento, si configura una contitolarità ai sensi dell'art. 26 GDPR. In tal caso le parti stipulano un accordo scritto che definisce in modo trasparente ruoli, responsabilità, punti di contatto, modalità di gestione delle informative, esercizio dei diritti, sicurezza, data breach, conservazione e riparto degli obblighi.

La parte essenziale dell'accordo di contitolarità è resa disponibile agli interessati secondo modalità idonee, ferma restando la possibilità per l'interessato di esercitare i propri diritti nei confronti di ciascun contitolare.

La mera trasmissione di dati tra enti pubblici o strutture del sistema sanitario non determina automaticamente una contitolarità. La qualificazione del ruolo privacy è valutata caso per caso, in base al potere effettivo di determinare finalità e mezzi del trattamento.

Art. 5 Compiti e funzioni dell'Azienda

Ats Liguria, quale titolare del trattamento, anche per il tramite dell'Area Sociosanitaria Locale 5, provvede a:

- adottare e aggiornare misure tecniche e organizzative adeguate al rischio, con particolare attenzione ai trattamenti sanitari digitali e ai sistemi informativi integrati;
- designare il referente per l'Area del team del Responsabile della protezione dei dati, assicurandogli accesso tempestivo alle informazioni necessarie;
- predisporre, aggiornare e conservare il Registro delle attività di trattamento;
- individuare soggetti designati, autorizzati, amministratori di sistema, referenti privacy, responsabili esterni e, ove previsto, sub-responsabili;
- fornire istruzioni documentate ai soggetti che trattano dati personali sotto la propria autorità;
- assicurare la formazione iniziale e periodica del personale e dei collaboratori;
- definire procedure per informative, consensi, revoche, oscuramenti, accessi, data breach, conservazione, archiviazione e scarto;
- verificare la conformità dei trattamenti affidati a terzi e inserire nei contratti clausole privacy adeguate;
- curare la sicurezza dei dati, dei sistemi, degli archivi, delle reti e delle postazioni di lavoro;
- garantire la tracciabilità degli accessi ai sistemi sanitari e amministrativi in base al rischio e alle norme applicabili.

Le strutture aziendali dell'Area Sociosanitaria Locale 5collaborano con la Direzione, con il RPD e il suo team, con i Sistemi Informativi e con le funzioni competenti per l'attuazione del presente regolamento. La collaborazione è obbligo organizzativo e rientra nei doveri di servizio.

Il RPD svolge funzioni di informazione, consulenza, sorveglianza e cooperazione con l'Autorità Garante. Il RPD non sostituisce le funzioni gestionali del titolare, dei direttori o dei responsabili delle strutture e non determina le finalità e i mezzi dei trattamenti.

Il referente del RPD per l'Area Sociosanitaria Locale 5 collabora, con riferimento all'Area stessa, per l'esecuzione dei compiti spettanti al RPD.

Art. 6 Protezione dei dati personali dalla progettazione e per impostazione predefinita

Ats Liguria applica i principi di protezione dei dati dalla progettazione e per impostazione predefinita in ogni progetto, servizio, procedura, affidamento, acquisto, sviluppo informatico, riorganizzazione o integrazione di banche dati che comporti trattamento di dati personali.

Prima di introdurre o modificare un trattamento, la struttura proponente valuta, con il supporto delle funzioni competenti e del RPD nei casi previsti, almeno i seguenti elementi:

- finalità del trattamento e relativa base giuridica;
- categorie di dati trattati, con attenzione ai dati relativi alla salute, genetici, biometrici, giudiziari e ai dati soggetti a maggior tutela;
- categorie di interessati e possibili impatti sui loro diritti;
- necessità e proporzionalità dei dati rispetto alla finalità;
- periodo di conservazione o criteri per determinarlo;
- soggetti autorizzati e profili di accesso;
- misure di autenticazione, autorizzazione, tracciamento, segregazione, cifratura, pseudonimizzazione o anonimizzazione;
- eventuali comunicazioni, interconnessioni, trasferimenti, accessi da remoto, uso di cloud o servizi gestiti da terzi;
- rischi residui e misure correttive.

Per impostazione predefinita devono essere trattati soltanto i dati necessari per ciascuna finalità. L'accesso ai dati è consentito solo ai soggetti autorizzati, nei limiti delle mansioni e per il tempo necessario allo svolgimento delle attività assegnate.

Le procedure informatiche devono prevedere profili differenziati, credenziali individuali, tracciamento degli accessi, blocco o revoca tempestiva delle utenze non più necessarie, riesame periodico delle autorizzazioni e controlli sulle anomalie di accesso, in coerenza con la natura del servizio e con il rischio.

L'adozione di tecnologie basate su algoritmi, sistemi decisionali automatizzati, strumenti di intelligenza artificiale, telemedicina, monitoraggio remoto o integrazione massiva di dati sanitari richiede una valutazione preventiva specifica, inclusa la valutazione d'impatto quando ricorrono i presupposti dell'art. 35 GDPR.

Art. 7 Dati trattati e categorie di interessati

Ats Liguria tratta dati personali comuni, dati identificativi, dati relativi alla salute, dati genetici, dati biometrici quando previsti da norme o da specifiche procedure, dati relativi alla vita sessuale o all'orientamento sessuale nei limiti consentiti, dati giudiziari ai sensi dell'art. 10 GDPR e dati soggetti a maggior tutela in base alla normativa sanitaria di settore.

Sono interessati dal trattamento, a titolo esemplificativo:

- assistiti, pazienti, utenti, familiari, caregiver, accompagnatori, delegati, fiduciari e soggetti legittimati a ricevere informazioni;
- minori, persone fragili, persone incapaci o impossibilitate, soggetti sottoposti a tutela, curatela, amministrazione di sostegno o altra misura di protezione;
- dipendenti, dirigenti, personale convenzionato, collaboratori, liberi professionisti, tirocinanti, borsisti, specializzandi, studenti, volontari e personale di soggetti esterni che operano presso Ats Liguria;
- fornitori, appaltatori, partecipanti a gare e selezioni, consulenti, visitatori, utenti dei servizi digitali e soggetti coinvolti in procedimenti amministrativi;
- persone fisiche coinvolte in sinistri, reclami, segnalazioni, audit, contenzioso o richieste provenienti da autorità pubbliche.

Rientrano tra i dati soggetti a maggior tutela, nei casi previsti dalla legge, quelli relativi a sieropositività, interruzione volontaria di gravidanza, violenza sessuale o pedofilia, uso di sostanze stupefacenti, psicotrope o alcool, servizi consultoriali, parto in anonimato, salute mentale, dipendenze e altre situazioni che richiedono speciali cautele per evitare pregiudizi alla persona.

Tali dati non devono essere diffusi. La loro comunicazione è ammessa soltanto nei casi previsti dalla legge, per finalità istituzionali o con il consenso dell'interessato quando necessario, adottando misure di minimizzazione, oscuramento, segregazione, limitazione degli accessi e tracciamento.

Nei casi previsti dalla normativa di settore, Ats Liguria garantisce il diritto all'anonimato, il diritto all'oscuramento e l'oscuramento dell'oscuramento, in modo che la scelta dell'interessato di oscurare un evento o un documento non sia visibile a soggetti non legittimati.

I dati sono raccolti, di norma, presso l'interessato. Possono essere raccolti presso terzi, altri enti del SSN o del SSR, pubbliche amministrazioni, esercenti professioni sanitarie, registri pubblici o altre fonti legittime quando ciò sia previsto dalla legge o necessario alla finalità perseguita.

Il trattamento per finalità di ricerca scientifica, studi clinici, sperimentazioni, registri, biobanche o indagini epidemiologiche è svolto nel rispetto delle norme di settore, dei pareri dei comitati etici ove richiesti, delle basi giuridiche applicabili, delle regole deontologiche e delle misure di garanzia previste dal Codice privacy e dai provvedimenti del Garante.

Art. 8 Liceità del trattamento

Il trattamento dei dati personali da parte di Ats Liguria è lecito quando è fondato su una delle basi giuridiche previste dall'art. 6 GDPR e, per le categorie particolari di dati, su una delle condizioni dell'art. 9 GDPR, integrate dalle disposizioni del Codice privacy e dalle norme sanitarie di settore.

Per le attività istituzionali sanitarie e sociosanitarie, le basi giuridiche ricorrenti sono l'adempimento di obblighi legali, l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, i motivi di interesse pubblico rilevante, la medicina preventiva o del lavoro, la diagnosi, l'assistenza o terapia sanitaria o sociale, la gestione dei sistemi e servizi sanitari e sociali, la sanità pubblica, la ricerca scientifica e statistica nei limiti previsti dalla legge, nonché l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il consenso dell'interessato non è richiesto per il trattamento necessario all'erogazione di prestazioni sanitarie o sociosanitarie da parte di professionisti soggetti al segreto professionale, quando il trattamento è fondato sulle condizioni previste dagli artt. 6 e 9 GDPR e dalle norme di settore.

Il consenso è invece richiesto per trattamenti facoltativi e ulteriori rispetto alla cura o agli obblighi istituzionali, quali, nei casi previsti, l'attivazione e la consultazione del dossier sanitario, specifici servizi digitali non necessari alla prestazione, particolari trattamenti tramite applicazioni o strumenti non

riconducibili alla telemedicina istituzionale, comunicazioni a soggetti terzi indicati dall'interessato, attività di ricerca che richiedano consenso e altri trattamenti espressamente subordinati a manifestazione di volontà.

Il trattamento di dati giudiziari è ammesso soltanto quando autorizzato dal diritto dell'Unione o dello Stato, anche per finalità di gestione del rapporto di lavoro, contenzioso, difesa in giudizio, controlli, obblighi anticorruzione, appalti, accertamenti amministrativi o altri casi previsti dalla legge.

Ogni trattamento deve rispettare i principi di necessità, proporzionalità, minimizzazione, limitazione delle finalità, esattezza, sicurezza e conservazione limitata. La disponibilità tecnica del dato non legittima il suo accesso o uso se non ricorre una concreta ragione di servizio.

Art. 9 Autorizzazioni, consenso e trattamenti facoltativi

Il trattamento dei dati da parte di persone fisiche che operano sotto l'autorità di Ats Liguria è consentito solo se il soggetto è formalmente autorizzato e istruito ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies del Codice privacy, oppure se opera come responsabile esterno del trattamento ai sensi dell'art. 28 GDPR.

Quando il trattamento si fonda sul consenso, Ats Liguria deve poter dimostrare che il consenso sia stato reso liberamente, in modo specifico, informato e inequivocabile. Per le categorie particolari di dati il consenso, quando necessario, deve essere esplicito.

La richiesta di consenso deve essere separata da altre dichiarazioni, formulata con linguaggio chiaro e accessibile, riferita a finalità determinate e accompagnata da informativa adeguata. L'interessato deve poter revocare il consenso con modalità semplici. La revoca non pregiudica la liceità del trattamento svolto prima della revoca.

Per il dossier sanitario aziendale, inteso come insieme logico di dati e documenti sanitari generati da eventi clinici presenti e passati presso un unico titolare, si applicano le garanzie previste dalla normativa e dai provvedimenti del Garante: informativa specifica, consenso ove richiesto, oscuramento, oscuramento dell'oscuramento, accessi selettivi, tracciamento, consultazione dei log nei casi previsti, misure di sicurezza e procedure per eventi di emergenza.

Per il Fascicolo sanitario elettronico si applicano l'art. 12 del D.L. 179/2012, il decreto del Ministero della salute 7 settembre 2023 sul FSE 2.0 e le successive disposizioni applicabili. L'alimentazione, la consultazione e gli ulteriori trattamenti tramite FSE sono gestiti secondo le basi giuridiche e i consensi previsti dalla disciplina vigente, con informativa conforme al modello nazionale ove applicabile e con garanzia dei diritti di oscuramento, consultazione degli accessi e opposizione nei casi previsti.

I consensi raccolti dalle Aziende cessate restano validi se documentati, riferibili alla medesima finalità e compatibili con il nuovo assetto di Ats Liguria. La mera successione nel ruolo di titolare, a finalità e modalità invariate, non richiede di regola una nuova raccolta del consenso, ferma la necessità di aggiornare le informative, i registri e i canali di esercizio dei diritti.

Qualora non sia possibile dimostrare la validità del consenso pregresso o qualora il trattamento sia modificato in modo sostanziale, la struttura competente deve sospendere il trattamento facoltativo e procedere alla nuova informazione e, ove necessario, alla raccolta di un nuovo consenso.

Art. 10 Valutazione d'impatto e consultazione dell'Autorità Garante

Prima di avviare un nuovo trattamento o una modifica sostanziale di un trattamento esistente, la struttura proponente verifica se il trattamento possa presentare un rischio elevato per i diritti e le libertà delle

persone fisiche. In tal caso deve essere effettuata una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR.

La valutazione d'impatto è di norma necessaria, tenendo conto delle liste e dei criteri del Garante e dell'EDPB, per trattamenti su larga scala di dati relativi alla salute o di altre categorie particolari di dati, monitoraggi sistematici, interconnessioni di banche dati, tecnologie innovative, sistemi di intelligenza artificiale, profilazioni, geolocalizzazioni, dati genetici o biometrici, dossier sanitari, piattaforme sanitarie integrate, telemedicina complessa e servizi digitali che possono incidere in modo significativo sugli interessati.

La DPIA deve descrivere il trattamento, valutarne necessità e proporzionalità, individuare i rischi, stimarne probabilità e gravità, indicare le misure previste per ridurli e documentare il rischio residuo. Deve inoltre tener conto dei diritti degli interessati, dei flussi di dati, dei destinatari, dei responsabili esterni, dei trasferimenti, dei tempi di conservazione e della sicurezza dei sistemi.

Il RPD è tempestivamente coinvolto e può rendere parere sulla DPIA. La responsabilità della valutazione e dell'adozione delle misure resta in capo ad Ats Liguria e alle strutture competenti.

Se, nonostante le misure individuate, il rischio residuo rimane elevato, Ats Liguria consulta preventivamente l'Autorità Garante ai sensi dell'art. 36 GDPR prima di procedere al trattamento.

La DPIA è riesaminata quando cambiano finalità, mezzi, fornitori, categorie di dati, categorie di interessati, flussi, tecnologie o misure di sicurezza, oppure quando emergono incidenti, violazioni, rilievi di audit o provvedimenti dell'Autorità che incidono sulla valutazione originaria.

Art. 11 Informazioni all'interessato

Ats Liguria fornisce agli interessati, anche per il tramite dell'Area Sociosanitaria Locale 5, le informazioni previste dagli artt. 13 e 14 GDPR con linguaggio chiaro, conciso, trasparente e comprensibile, tenendo conto della condizione dell'interessato e del contesto sanitario o amministrativo in cui avviene il trattamento.

Le informative devono indicare almeno: identità e dati di contatto del titolare; dati di contatto del RPD; finalità e basi giuridiche del trattamento; categorie di dati trattati; modalità essenziali del trattamento; natura obbligatoria o facoltativa del conferimento; conseguenze del mancato conferimento; destinatari o categorie di destinatari; eventuali trasferimenti verso Paesi terzi; periodo di conservazione o criteri per determinarlo; diritti dell'interessato; diritto di reclamo al Garante; eventuale esistenza di processi decisionali automatizzati, compresa la profilazione, con informazioni significative sulla logica utilizzata e sulle conseguenze previste.

Per i trattamenti sanitari e sociosanitari le informative devono spiegare, ove pertinente, il trattamento dei dati relativi alla salute, il ruolo dei professionisti sanitari, le comunicazioni a MMG/PLS o altri soggetti del percorso di cura, il dossier sanitario, il FSE, il diritto di oscuramento, il diritto di conoscere gli accessi effettuati quando previsto, le modalità di revoca dei consensi e i canali per esercitare i diritti.

In ragione della complessità dei servizi, le informazioni possono essere rese in forma stratificata: informativa sintetica presso sportelli, reparti e servizi; informativa completa sul sito istituzionale e sui portali digitali; modulistica specifica per singoli trattamenti facoltativi, dossier, FSE, ricerca, videosorveglianza, lavoro, posta elettronica e servizi online.

Ats Liguria aggiorna le informative per indicare il nuovo titolare, i suoi dati di contatto e i canali del RPD. L'aggiornamento deve riguardare anche siti web, modulistica, portali, applicativi, cartellonistica e documenti in uso presso l'Area Sociosanitaria Locale 5 e le altre Aree.

Quando i dati non sono raccolti presso l'interessato, l'informativa è resa secondo l'art. 14 GDPR, salvo i casi in cui l'interessato ne disponga già, la comunicazione sia impossibile o richieda uno sforzo sproporzionato, o l'acquisizione o comunicazione sia prevista dal diritto dell'Unione o dello Stato. In tali casi devono essere adottate misure adeguate a tutelare diritti, libertà e interessi legittimi degli interessati.

Art. 12 Diritti dell'interessato e loro esercizio

Gli interessati possono esercitare nei confronti di Ats Liguria i diritti previsti dagli artt. 15 e seguenti GDPR: accesso, rettifica, cancellazione, limitazione, opposizione, portabilità nei casi previsti, revoca del consenso, diritto di non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati nei casi disciplinati dall'art. 22 GDPR, reclamo all'Autorità Garante.

Le richieste possono essere presentate al titolare, al RPD o ai canali privacy aziendali. Per Ats Liguria il RPD è raggiungibile all'indirizzo rpd@alisa.liguria.it. Per l'Area Sociosanitaria Locale 5 è possibile scrivere anche a privacy@asl5.liguria.it.

La struttura che riceve una richiesta deve trasmetterla senza ritardo al canale privacy competente, identificare correttamente l'interessato o il soggetto delegato, verificare l'oggetto della richiesta e collaborare con il RPD e con le funzioni competenti per fornire riscontro nei termini di legge.

Il riscontro è fornito senza ingiustificato ritardo e comunque entro un mese dalla ricezione della richiesta, salvo proroga nei casi di particolare complessità o numero di richieste. L'eventuale proroga e i relativi motivi sono comunicati all'interessato entro un mese dalla ricezione.

Il diritto di accesso comprende il diritto di ottenere conferma che sia o meno in corso un trattamento di dati personali e di ricevere copia dei dati oggetto di trattamento, salvi i limiti previsti per la tutela di diritti e libertà altrui, del segreto professionale, del segreto d'ufficio, della sicurezza dei sistemi e delle norme speciali sanitarie o amministrative.

Il diritto di rettifica consente di correggere dati inesatti e integrare dati incompleti. Nella documentazione sanitaria la rettifica non comporta la sostituzione retroattiva del giudizio clinico legittimamente formato, ma può comportare annotazione, integrazione, correzione amministrativa o altra misura idonea a garantire esattezza e tracciabilità.

Il diritto alla cancellazione e il diritto alla limitazione operano nei limiti stabiliti dagli artt. 17 e 18 GDPR. Non si procede alla cancellazione quando la conservazione è necessaria per obbligo legale, compiti di interesse pubblico, sanità pubblica, archiviazione nel pubblico interesse, ricerca scientifica o statistica, accertamento, esercizio o difesa di un diritto.

Il diritto alla portabilità si applica solo quando ricorrono i presupposti dell'art. 20 GDPR, in particolare trattamento basato sul consenso o su contratto e svolto con mezzi automatizzati. Non si applica ai trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connessi all'esercizio di pubblici poteri, salvo diverse previsioni di settore.

I diritti relativi ai dati personali di persone decedute possono essere esercitati da chi ha un interesse proprio, agisce a tutela dell'interessato, in qualità di mandatario o per ragioni familiari meritevoli di protezione, salvo divieti di legge o volontà espressa dall'interessato nei limiti previsti dall'art. 2-terdecies del Codice privacy.

Ats Liguria per il tramite dell'Area Sociosanitaria Locale 5 documenta le richieste, le verifiche effettuate, i riscontri forniti e gli eventuali dinieghi motivati, conservando la documentazione per il tempo necessario a dimostrare la corretta gestione del procedimento.

Art. 13 Accesso agli atti e riservatezza

Le richieste di accesso documentale, accesso civico semplice e accesso civico generalizzato sono trattate nel rispetto della L. 241/1990, del D.lgs. 33/2013, della normativa sanitaria e della disciplina in materia di protezione dei dati personali.

Quando l'accesso riguarda documenti contenenti dati personali, la struttura competente valuta caso per caso la sussistenza dei presupposti, la posizione del richiedente, la finalità dichiarata, l'eventuale presenza di controinteressati, la pertinenza dei dati richiesti e la possibilità di consentire un accesso parziale mediante oscuramento dei dati non necessari.

I dati idonei a rivelare lo stato di salute o la vita sessuale non possono essere diffusi. L'accesso da parte di terzi a dati sanitari è ammesso soltanto quando il diritto da tutelare sia di rango almeno pari a quello dell'interessato, oppure consista in un diritto della personalità, in altro diritto inviolabile o in una libertà fondamentale, valutati in concreto.

L'accesso civico generalizzato non può tradursi in una diffusione indiscriminata di dati sanitari, dati soggetti a maggior tutela, dati giudiziari, dati di minori o informazioni eccedenti rispetto allo scopo di trasparenza. Devono essere applicati i limiti e le esclusioni previsti dalla legge e dalle Linee guida del Garante e dell'ANAC.

Le strutture preposte all'accesso agli atti collaborano con il RPD e il suo team nei casi complessi, quando siano coinvolti dati relativi alla salute, dati giudiziari, dati di soggetti vulnerabili, dati di dipendenti o pubblicazioni potenzialmente lesive della dignità personale.

Art. 14 Comunicazione dati all'interessato

L'interessato ha diritto di ricevere i propri dati e la documentazione sanitaria che lo riguarda secondo le modalità previste dalla legge, dai regolamenti aziendali e dalle procedure operative.

La comunicazione può avvenire mediante consegna diretta, consultazione in ambiente protetto, portale digitale, Fascicolo sanitario elettronico, PEC, posta elettronica ordinaria se richiesta dall'interessato e compatibile con il rischio, consegna a delegato, invio postale o altra modalità idonea adottata da Ats Liguria.

Prima di consegnare o trasmettere documenti contenenti dati personali, la struttura competente verifica l'identità dell'interessato, la validità dell'eventuale delega, la correttezza del recapito e la congruità della modalità richiesta rispetto alla natura dei dati.

La documentazione sanitaria analogica è consegnata in busta chiusa o con modalità equivalenti. La consegna a delegato è ammessa solo in presenza di delega scritta e documento di identità, salvo i casi in cui norme speciali impongano la consegna diretta all'interessato.

Le informazioni cliniche sono comunicate all'interessato da personale sanitario autorizzato e competente, con modalità rispettose della dignità della persona e idonee a evitare la conoscenza indebita da parte di terzi.

L'uso della posta elettronica ordinaria per l'invio di documenti sanitari è ammesso solo quando l'interessato lo richieda o lo accetti consapevolmente, dopo essere stato informato dei rischi essenziali, e quando siano adottate misure ragionevoli di verifica del destinatario e di protezione del contenuto. Per documenti particolarmente delicati si privilegiano PEC, portali autenticati o altre modalità sicure.

Art. 15 Comunicazione dati di salute a terzi indicati dall'interessato

Ats Liguria e per essa l'Area Sociosanitaria Locale 5 può comunicare dati relativi alla salute a soggetti terzi indicati dall'interessato nei limiti della volontà manifestata, della normativa applicabile e della necessità di garantire continuità assistenziale, assistenza familiare, delega al ritiro di documenti o informazione sul percorso di cura.

L'interessato può indicare una o più persone autorizzate a ricevere informazioni sul ricovero, sulla presenza presso una struttura, sullo stato di salute o sulla documentazione sanitaria. La volontà deve essere raccolta in modo documentabile, registrata ove previsto nei sistemi aziendali e resa disponibile ai soli operatori che ne abbiano necessità.

L'autorizzazione può essere modificata o revocata in qualsiasi momento. La modifica può avere carattere generale o riferirsi al singolo episodio di cura, ricovero o accesso, secondo le procedure aziendali.

La comunicazione a MMG, PLS, specialisti, strutture sanitarie, servizi territoriali o altri soggetti coinvolti nel percorso di cura avviene secondo la base giuridica e il ruolo privacy applicabili, che possono variare in base alla normativa, agli accordi regionali, alle convenzioni e alla concreta organizzazione del servizio.

In caso di emergenza, incapacità temporanea o impossibilità dell'interessato, le informazioni possono essere comunicate nei limiti necessari alla tutela della salute dell'interessato o di terzi, alla continuità assistenziale o all'adempimento di obblighi di legge, documentando le ragioni della comunicazione.

È vietata la comunicazione informale di dati sanitari a persone non autorizzate, anche se familiari, conoscenti, colleghi o visitatori, salvo che ricorra una base giuridica idonea o una chiara manifestazione di volontà dell'interessato.

Art. 16 Comunicazione dati personali all'esterno

La comunicazione di dati personali all'esterno di Ats Liguria è ammessa soltanto quando prevista da una norma di legge o regolamento, necessaria all'esecuzione di compiti istituzionali, richiesta da autorità competenti nei limiti dei rispettivi poteri, fondata su un contratto o atto di nomina a responsabile del trattamento, o autorizzata dall'interessato nei casi in cui il consenso sia base giuridica valida.

I destinatari possono comprendere, nei limiti di legge, enti del SSN e del SSR, Ministero della salute, Regione Liguria, AGENAS, Istituto Superiore di Sanità, autorità giudiziaria, organi di polizia giudiziaria, enti previdenziali e assicurativi, INAIL, INPS, Comuni, altri enti pubblici, organismi di controllo, fornitori, consulenti, compagnie assicurative, avvocati e altri soggetti legittimati.

Prima della comunicazione la struttura competente verifica finalità, base giuridica, pertinenza, non eccedenza, correttezza del destinatario, sicurezza del canale e tracciabilità dell'operazione. Le comunicazioni massive, ricorrenti o automatizzate devono essere censite nel Registro delle attività di trattamento.

È vietata la diffusione di dati relativi alla salute. La pubblicazione online di atti e documenti deve rispettare il principio di minimizzazione e le norme in materia di trasparenza, evitando la pubblicazione di dati sanitari, dati soggetti a maggior tutela, dati di minori, dati giudiziari o informazioni eccedenti.

Il trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali è consentito solo nel rispetto del Capo V GDPR, delle decisioni di adeguatezza, delle garanzie adeguate, delle deroghe applicabili e delle ulteriori istruzioni aziendali. Le richieste dirette di autorità di Paesi terzi sono gestite secondo l'art. 48 GDPR e gli accordi internazionali applicabili.

I servizi cloud, le attività di manutenzione da remoto, l'assistenza tecnica, l'hosting, la conservazione digitale e ogni trattamento che comporti accesso a dati da parte di fornitori devono essere valutati prima dell'affidamento e regolati da contratti conformi all'art. 28 GDPR, con specifica disciplina di sicurezza, localizzazione dei dati, subfornitori e trasferimenti.

Art. 17 Registro delle attività di trattamento dati

Ats Liguria, con la collaborazione dell'Area Sociosanitaria Locale 5, tiene il Registro delle attività di trattamento ai sensi dell'art. 30 GDPR in forma scritta, anche elettronica, e lo mette a disposizione dell'Autorità Garante su richiesta.

Il Registro riporta almeno: nome e dati di contatto del titolare, del RPD e degli eventuali contitolari; finalità del trattamento; basi giuridiche; categorie di interessati; categorie di dati personali; categorie di destinatari; trasferimenti verso Paesi terzi; termini di conservazione o criteri per determinarli; misure tecniche e organizzative di sicurezza; responsabili esterni; sistemi e banche dati utilizzati; strutture competenti; modalità di esercizio dei diritti.

Le strutture dell'Area di gestione dei servizi accentrati e delle Aree sociosanitarie locali collaborano all'aggiornamento del Registro fornendo informazioni complete e tempestive su trattamenti, banche dati, applicativi, flussi, destinatari, fornitori, autorizzazioni, conservazione, rischi e misure.

Ogni nuovo trattamento, cessazione, modifica significativa, nuova comunicazione, nuova interconnessione, introduzione di un sistema informatico, affidamento a un fornitore o variazione del periodo di conservazione deve essere comunicato alla funzione competente per l'aggiornamento del Registro.

Il Registro delle attività dei responsabili esterni è acquisito o verificato nei casi rilevanti, soprattutto per trattamenti sanitari, sistemi informativi, servizi cloud, conservazione digitale, manutenzione, call center, postalizzazione, archiviazione, distruzione documentale e servizi in outsourcing.

Il Registro è integrato, ove opportuno, con la valutazione dei rischi, le DPIA, le misure di sicurezza, gli atti di nomina e le procedure di esercizio dei diritti.

Art. 18 Politica di sicurezza aziendale

Ats Liguria anche per l'Area Sociosanitaria Locale 5 adotta una politica di sicurezza dei dati personali volta a preservare riservatezza, integrità, disponibilità, autenticità, resilienza e tracciabilità dei dati e dei sistemi che li trattano.

La politica di sicurezza si basa sui principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione.

Le misure sono determinate in base al rischio, tenendo conto di natura, oggetto, contesto e finalità del trattamento, stato dell'arte, costi di attuazione, probabilità e gravità dei rischi per le persone fisiche, nonché delle specifiche cautele richieste per i dati sanitari e sociosanitari.

La sicurezza riguarda dati digitali e analogici, sistemi informativi, archivi, reti, postazioni, dispositivi mobili, documentazione clinica, referti, applicativi, procedure amministrative, flussi con terzi, attività affidate a fornitori, supporti di backup, log e ambienti cloud.

Le misure di sicurezza devono essere riesaminate periodicamente e aggiornate in caso di incidenti, vulnerabilità, modifiche organizzative, nuove minacce, evoluzioni tecnologiche, provvedimenti delle autorità, audit o rilievi interni.

Le strutture aziendali sono tenute a segnalare tempestivamente al RPD e al suo team, ai Sistemi Informativi e alle funzioni competenti ogni anomalia, vulnerabilità, accesso indebito, perdita di documenti, invio errato, furto di dispositivi, sospetto malware o altra situazione che possa compromettere dati personali.

Art. 19 Responsabilità civile

Chi subisce un danno materiale o immateriale causato da una violazione del GDPR ha diritto al risarcimento ai sensi dell'art. 82 GDPR. Il titolare e il responsabile del trattamento rispondono secondo i rispettivi ruoli, obblighi e responsabilità.

Ats Liguria, in qualità di titolare, risponde dei danni derivanti da trattamenti non conformi quando non dimostri che l'evento dannoso non le è imputabile. Il responsabile esterno risponde se non ha adempiuto agli obblighi specificamente posti a suo carico dal GDPR o se ha agito in modo difforme o contrario rispetto alle istruzioni documentate del titolare.

Resta fermo il possibile rilievo delle norme civilistiche nazionali, comprese quelle in materia di responsabilità contrattuale ed extracontrattuale, ove ne ricorrano i presupposti. Le misure tecniche e organizzative adottate, la documentazione del Sistema Privacy, le istruzioni, la formazione, gli audit e la gestione degli incidenti costituiscono elementi essenziali per dimostrare la diligenza dell'Azienda.

Nella scelta dei responsabili esterni, Ats Liguria valuta affidabilità, competenze, misure di sicurezza, organizzazione, subfornitori, localizzazione dei dati, capacità di assistere il titolare e coperture assicurative ove pertinenti.

Il personale e i collaboratori che trattano dati personali in violazione della normativa, delle istruzioni ricevute o del presente regolamento possono essere soggetti a responsabilità disciplinare, civile, amministrativa o penale secondo le norme applicabili e i contratti di riferimento.

Art. 20 Organigramma aziendale privacy

L'organigramma privacy di Ats Liguria per l'Area Sociosanitaria Locale 5 individua i soggetti che, a diverso titolo, partecipano alla gestione dei trattamenti di dati personali. L'organigramma tiene conto del nuovo assetto regionale, dell'Area di gestione dei servizi accentrati e delle cinque Aree sociosanitarie locali.

All'interno dell'Azienda sono individuati: il titolare del trattamento; il RPD e il suo team; i soggetti designati e delegati a presidiare specifici trattamenti o ambiti organizzativi; i referenti privacy; gli autorizzati al trattamento; gli amministratori di sistema; le strutture competenti per sicurezza, sistemi informativi, personale, affari generali, legale, trasparenza, archivi e conservazione.

All'esterno dell'Azienda possono essere individuati, secondo i casi: contitolari, responsabili del trattamento, sub-responsabili, autonomi titolari, destinatari della comunicazione e soggetti autorizzati da altri titolari o responsabili.

La nomenclatura storica di "responsabile interno" può essere mantenuta solo come qualifica organizzativa interna, purché sia chiaro che non si tratta del responsabile del trattamento di cui all'art. 28 GDPR. I soggetti interni operano come designati o autorizzati sotto l'autorità del titolare ai sensi dell'art. 29 GDPR e dell'art. 2-quaterdecies del Codice privacy.

Gli atti di designazione, delega e autorizzazione devono indicare ambito, mansioni, trattamenti, banche dati, profili di accesso, istruzioni, obblighi di riservatezza e durata. Gli atti sono conservati dalla struttura competente e resi disponibili in caso di verifica.

Nel periodo transitorio, le designazioni adottate dalle Aziende cessate restano efficaci se compatibili con il nuovo assetto di Ats Liguria e fino alla loro revisione, integrazione o sostituzione.

Art. 21 Delegati e soggetti designati al trattamento dati

I direttori di dipartimento, i direttori di struttura complessa, i responsabili di struttura semplice dipartimentale, i responsabili di funzione e gli altri soggetti individuati da Ats Liguria per l'Area Sociosanitaria Locale 5 possono essere designati o delegati a presidiare, nell'ambito delle proprie competenze, specifici trattamenti di dati personali.

La designazione interna attribuisce compiti organizzativi, istruttori e di controllo sui trattamenti svolti dalla struttura, ma non trasferisce la titolarità del trattamento. Il titolare resta Ats Liguria.

I soggetti designati o delegati sono tenuti a:

- applicare e far applicare il GDPR, il Codice privacy, il presente regolamento e le procedure aziendali;
- assicurare che i dati trattati dalla struttura siano adeguati, pertinenti, esatti, aggiornati e limitati alla finalità;
- vigilare sul rispetto delle istruzioni da parte degli autorizzati;
- richiedere, modificare o revocare i profili di accesso in coerenza con mansioni e necessità operative;
- collaborare all'aggiornamento del Registro delle attività;
- segnalare tempestivamente nuovi trattamenti, criticità, incidenti, data breach, richieste degli interessati e non conformità;
- favorire la formazione del personale e la diffusione delle istruzioni operative;
- collaborare con il RPD e il suo team, con i Sistemi Informativi e con le funzioni competenti durante verifiche e audit;
- curare la corretta conservazione della documentazione e degli atti di designazione degli autorizzati;
- individuare, ove previsto, un referente privacy di struttura.

Il soggetto designato o delegato deve segnalare senza ritardo al RPD e alla Direzione competente eventuali istruzioni, prassi o richieste che appaiano non conformi alla normativa in materia di protezione dei dati personali.

La mancata attuazione delle misure privacy rientranti nell'ambito di competenza della struttura può rilevare ai fini della responsabilità organizzativa, dirigenziale, disciplinare o contrattuale.

Art. 22 Autorizzati al trattamento dati

Sono autorizzate al trattamento le persone fisiche che, operando sotto l'autorità di Ats Liguria o di un responsabile esterno, trattano dati personali per lo svolgimento delle mansioni assegnate e secondo istruzioni documentate.

Devono essere autorizzati, ove trattino dati personali: dipendenti, dirigenti, personale convenzionato, collaboratori, liberi professionisti, tirocinanti, studenti, specializzandi, volontari, borsisti, consulenti, lavoratori somministrati, personale di ditte esterne che opera sotto direzione aziendale e ogni altra persona fisica che acceda a dati personali nell'ambito delle attività aziendali.

L'autorizzazione deve indicare, anche per categorie omogenee di mansioni, i trattamenti consentiti, i sistemi e le banche dati accessibili, il profilo assegnato, le istruzioni operative, gli obblighi di riservatezza e le misure di sicurezza da osservare.

Gli autorizzati possono trattare solo i dati necessari allo svolgimento delle attività assegnate. È vietato accedere a dati di pazienti, colleghi, familiari, conoscenti o altri soggetti per curiosità, interesse personale, utilità privata, finalità difensive non autorizzate o ragioni estranee al servizio.

Gli autorizzati sono tenuti a custodire credenziali e dispositivi, non condividere password, bloccare la postazione in caso di assenza, non lasciare documenti incustoditi, verificare destinatari e allegati prima dell'invio, rispettare le procedure di stampa e archiviazione, segnalare incidenti e partecipare alla formazione.

L'accesso ai sistemi informatici è personale, tracciato e commisurato al ruolo. Le credenziali non possono essere cedute, prestate, annotate in luoghi accessibili o utilizzate da soggetti diversi dall'intestatario.

Alla cessazione o modifica dell'incarico, trasferimento, assenza prolungata, variazione di mansioni o cessazione del rapporto, la struttura competente richiede tempestivamente la modifica o la revoca delle autorizzazioni e delle credenziali.

Art. 23 Amministratori di sistema

Gli amministratori di sistema sono le persone fisiche che, per mansioni tecniche, possono accedere anche solo potenzialmente a sistemi, reti, banche dati, applicazioni o infrastrutture che trattano dati personali.

Ats Liguria anche per l'Area Sociosanitaria Locale 5 designa individualmente gli amministratori di sistema, previa valutazione di esperienza, capacità e affidabilità, indicando ambito di operatività, sistemi amministrati, privilegi assegnati, istruzioni, responsabilità, durata della designazione e obblighi di riservatezza.

I privilegi amministrativi devono essere limitati a quanto necessario, attribuiti con account nominativi, separati dagli account ordinari ove possibile, protetti da credenziali robuste e autenticazione rafforzata, tracciati e riesaminati periodicamente.

Gli accessi degli amministratori di sistema ai sistemi che trattano dati personali sono registrati mediante log idonei a consentire controlli su accesso, utenza, data, ora e attività essenziali, nel rispetto dei principi di proporzionalità e sicurezza. I log sono protetti da alterazioni e conservati per il periodo stabilito dalle procedure aziendali.

I fornitori nominati responsabili esterni che svolgono attività di amministrazione di sistema devono individuare i propri amministratori, imporre obblighi equivalenti, documentare le designazioni, garantire tracciamento e controlli, e fornire evidenza ad Ats Liguria su richiesta o secondo le scadenze contrattuali.

Le attività amministrative da remoto sono consentite solo con strumenti autorizzati, canali sicuri, tracciamento, autenticazione adeguata e, quando necessario, autorizzazione preventiva o ticket di intervento. È vietato l'uso di strumenti personali o non approvati.

Art. 24 Formazione

Ats Liguria assicura la formazione iniziale e periodica in materia di protezione dei dati personali, sicurezza delle informazioni, riservatezza, uso corretto dei sistemi, gestione del data breach, diritti degli interessati e regole specifiche per i trattamenti sanitari.

La formazione è differenziata in base al ruolo: personale sanitario, amministrativo, tecnico, operatori di front office, dirigenti e responsabili, autorizzati, referenti privacy, amministratori di sistema, personale neoassunto, tirocinanti, volontari e collaboratori.

I contenuti formativi riguardano, tra l'altro: GDPR e Codice privacy; dati sanitari e dati soggetti a maggior tutela; dossier sanitario; FSE; informative e consensi; oscuramento; accesso agli atti; comunicazioni a terzi; uso di posta elettronica e strumenti digitali; pubblicazione di atti; sicurezza dei documenti; gestione delle credenziali; uso di dispositivi mobili; data breach; comportamento nei reparti e negli sportelli; uso di strumenti di intelligenza artificiale.

La partecipazione alla formazione è documentata. Le strutture tengono conto della formazione svolta ai fini dell'attribuzione delle autorizzazioni e dei profili di accesso.

I responsabili esterni devono garantire che il proprio personale autorizzato al trattamento per conto di Ats Liguria sia istruito, formato e vincolato alla riservatezza, fornendo evidenza documentale su richiesta.

Art. 25 Responsabili esterni del trattamento dati

Quando Ats Liguria affida a un soggetto esterno attività che comportano trattamento di dati personali per conto dell'Azienda, il soggetto esterno, a cura dell'Area Sociosanitaria Locale 5, deve essere nominato responsabile del trattamento ai sensi dell'art. 28 GDPR prima dell'avvio delle attività.

La nomina è contenuta in contratto, convenzione, atto giuridico o allegato privacy vincolante e deve disciplinare almeno: oggetto, durata, natura e finalità del trattamento, categorie di dati, categorie di interessati, istruzioni documentate, misure di sicurezza, riservatezza, sub-responsabili, assistenza al titolare, gestione dei diritti, data breach, cancellazione o restituzione dei dati, audit, trasferimenti verso Paesi terzi e responsabilità.

Il responsabile esterno è scelto solo se presenta garanzie sufficienti in termini di competenza, affidabilità, organizzazione, sicurezza, continuità operativa, capacità di assistere Ats Liguria, gestione dei subfornitori, localizzazione dei dati e conformità normativa.

Il responsabile esterno deve trattare i dati soltanto su istruzione documentata di Ats Liguria, garantire che le persone autorizzate siano vincolate alla riservatezza, adottare misure adeguate al rischio, non ricorrere a sub-responsabili senza autorizzazione, assistere Ats Liguria nell'adempimento degli obblighi e mettere a disposizione le informazioni necessarie per dimostrare la conformità.

Il ricorso a sub-responsabili è ammesso solo previa autorizzazione specifica o generale di Ats Liguria secondo le condizioni contrattuali. Il responsabile deve imporre al sub-responsabile obblighi equivalenti e resta responsabile verso Ats Liguria dell'adempimento del sub-responsabile.

Nei contratti relativi a servizi informatici, cloud, manutenzione, conservazione, archiviazione, distruzione documentale, postalizzazione, call center, gestione di portali, assistenza, telemedicina o servizi sanitari esternalizzati devono essere previste clausole specifiche su sicurezza, localizzazione, accessi, log, backup, vulnerabilità, cifratura, continuità operativa, restituzione e cancellazione dei dati.

In caso di adesione a gare regionali, nazionali o centralizzate, la struttura competente verifica che gli atti di gara e i contratti quadro contengano clausole privacy idonee. Se tali clausole non sono sufficienti, prima dell'avvio del trattamento devono essere integrati gli accordi con istruzioni e garanzie adeguate.

Art. 26 Responsabili che effettuano operazioni di natura informatica

I responsabili esterni, i sub-responsabili e i fornitori che svolgono attività di sviluppo, gestione, manutenzione, assistenza, hosting, cloud, conservazione, sicurezza o amministrazione di sistemi informativi sanitari o amministrativi devono rispettare requisiti specifici di protezione dei dati.

Essi devono garantire che sistemi, applicativi e servizi siano progettati secondo i principi di protezione dei dati dalla progettazione e per impostazione predefinita, con profili differenziati, autenticazione adeguata, tracciamento degli accessi, segregazione degli ambienti, gestione delle vulnerabilità, backup, cifratura ove necessaria, continuità operativa e procedure di ripristino.

Le attività di manutenzione devono essere svolte solo per le finalità contrattuali, con personale autorizzato, canali sicuri, ticket o altra tracciabilità, tempi limitati e accesso ai soli dati strettamente necessari. È vietata la copia, estrazione, conservazione, riuso o analisi dei dati per finalità proprie del fornitore.

Il fornitore deve comunicare preventivamente ad Ats Liguria l'eventuale uso di cloud, data center, subfornitori, strumenti di teleassistenza, sistemi di monitoraggio, trasferimenti extra UE o accessi da Paesi terzi. Nessuna modifica sostanziale è ammessa senza autorizzazione nei modi previsti dal contratto.

I dati sanitari e sociosanitari devono essere separati, cifrati o pseudonimizzati quando il rischio lo richiede, in particolare negli ambienti di test, sviluppo, formazione e assistenza. L'uso di dati reali in ambienti non produttivi è ammesso solo quando indispensabile, documentato e protetto da misure adeguate.

Ats Liguria può richiedere audit, report di sicurezza, attestazioni, certificazioni, piani di rimedio, evidenze su vulnerability management, penetration test, backup, log, disaster recovery, gestione delle utenze privilegiate e formazione del personale tecnico.

Il mancato rispetto delle misure di sicurezza o delle istruzioni può costituire grave inadempimento contrattuale e comportare sospensione del trattamento, risoluzione, richiesta di rimedio, segnalazione alle autorità competenti e richiesta di risarcimento del danno.

Art. 27 Responsabile aziendale della protezione dati

Ats Liguria designa il Responsabile della protezione dei dati, o RPD/DPO, in base alle qualità professionali, alla conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché alla capacità di assolvere i compiti previsti dagli artt. 37, 38 e 39 GDPR.

Il RPD di Ats Liguria è raggiungibile all'indirizzo rpd@alisa.liguria.it. Tale dato di contatto è pubblicato sul sito istituzionale, riportato nelle informative e comunicato all'Autorità Garante.

Il RPD si avvale, nello svolgimento delle proprie funzioni, di un team di esperti collocati presso le diverse Aree.

Per l'Area Sociosanitaria Locale 5, il referente del team RPD è contattabile all'indirizzo privacy@asl5.liguria.it.

Ats Liguria garantisce che il RPD e il suo team siano coinvolti tempestivamente e adeguatamente in tutte le questioni riguardanti la protezione dei dati personali, in particolare in caso di nuovi progetti, sistemi informativi sanitari, dossier, FSE, telemedicina, data breach, DPIA, contratti con fornitori, pubblicazioni, richieste degli interessati, controlli o ispezioni.

Il RPD opera in autonomia, non riceve istruzioni per l'esecuzione dei propri compiti, non è rimosso o penalizzato per l'adempimento degli stessi e riferisce al vertice gerarchico del titolare. Eventuali altri compiti o funzioni affidati al RPD non devono generare conflitti di interessi.

Il RPD svolge i seguenti compiti:

- informa e fornisce consulenza ad Ats Liguria, ai soggetti designati e agli autorizzati in merito agli obblighi privacy;
- sorveglia l'osservanza del GDPR, del Codice privacy, delle altre norme applicabili e delle politiche aziendali;
- fornisce pareri sulle DPIA e ne sorveglia lo svolgimento quando richiesto;
- collabora con l'Autorità Garante e funge da referente per le questioni connesse al trattamento;
- supporta la predisposizione di procedure, informative, modelli, istruzioni e programmi formativi;
- formula raccomandazioni sulla gestione dei rischi e sulle misure di conformità.

Il RPD non è responsabile dell'adozione delle decisioni gestionali sul trattamento. Tali decisioni restano in capo ad Ats Liguria e alle funzioni competenti.

Art. 28 Accesso alle procedure informatiche aziendali

L'accesso alle procedure informatiche aziendali è consentito solo a soggetti autorizzati, per ragioni di servizio, con profili coerenti con mansioni, struttura, incarico, unità operativa e periodo di effettiva necessità.

Ogni utenza deve essere individuale. Sono vietati account condivisi, credenziali generiche, uso di credenziali altrui o accessi per finalità personali. Eventuali utenze tecniche o di servizio sono ammesse solo se indispensabili, documentate, protette e tracciate.

La richiesta di creazione, modifica o revoca delle utenze è attivata dalla struttura competente mediante i canali ufficiali individuati da Ats Liguria, con indicazione del ruolo, del profilo richiesto, dei sistemi interessati, della durata e della motivazione di servizio.

Prima del rilascio del profilo, la struttura richiedente verifica che il soggetto sia autorizzato al trattamento e abbia ricevuto le istruzioni necessarie. I Sistemi Informativi verificano la compatibilità tecnica e attivano le misure di sicurezza previste.

I profili di accesso sono differenziati secondo il principio del minimo privilegio. L'accesso a dati sanitari, dossier, FSE, sistemi di laboratorio, radiologia, pronto soccorso, cartelle cliniche, salute mentale, dipendenze, consultori, dati di personale o dati giudiziari richiede particolare attenzione e tracciamento coerente con il rischio.

Le utenze sono riesaminate periodicamente e comunque in caso di cessazione, trasferimento, mutamento di mansione, cambio di struttura, assenza prolungata, sospensione, fine rapporto o fine incarico. Le strutture competenti comunicano tempestivamente tali eventi ai Sistemi Informativi.

L'accesso ai log è consentito solo a soggetti autorizzati per finalità di sicurezza, audit, verifica di conformità, gestione incidenti, tutela dei diritti dell'interessato o accertamento di condotte illecite, nel rispetto della normativa sul lavoro e delle procedure aziendali.

Art. 29 Misure di sicurezza

Ats Liguria e i responsabili del trattamento adottano misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio, ai sensi dell'art. 32 GDPR.

Le misure includono, secondo il rischio e la fattibilità tecnica:

- autenticazione robusta e, per i sistemi a rischio più elevato, autenticazione a più fattori;
- gestione dei profili di accesso e principio del minimo privilegio;
- tracciamento e conservazione protetta dei log;
- cifratura, pseudonimizzazione o segregazione dei dati quando necessario;
- backup regolari, protetti e testati;
- capacità di ripristinare tempestivamente disponibilità e accesso ai dati;
- protezione da malware, phishing, ransomware e accessi non autorizzati;
- patch management, hardening, monitoraggio e gestione delle vulnerabilità;
- sicurezza fisica di locali, archivi, data center, armadi e supporti;
- procedure di cancellazione sicura e distruzione dei supporti;
- formazione e istruzioni operative per il personale;
- verifiche periodiche sull'efficacia delle misure.

Nei contesti di sportello, reparto, ambulatorio, pronto soccorso, sala d'attesa e front office devono essere adottate misure organizzative volte a evitare la conoscenza indebita di informazioni sanitarie: distanze di cortesia, chiamata non nominativa ove possibile, conversazioni riservate, documenti non visibili a terzi, schermi non esposti, consegna protetta di referti e limitazione delle informazioni rese al telefono.

Durante colloqui, visite, giro visita, passaggi di consegne, consulenze, formazione sul campo e discussione di casi clinici, il personale deve adottare cautele proporzionate per evitare la diffusione di dati non necessari a persone non coinvolte nel percorso di cura.

Gli autorizzati che non sono tenuti per legge al segreto professionale sono comunque vincolati da obblighi di riservatezza equivalenti per i dati trattati nell'ambito dell'attività aziendale.

Art. 30 Misure di sicurezza informatica a protezione dei dati

Le misure di sicurezza informatica sono definite dai Sistemi Informativi, con il supporto delle funzioni competenti e del RPD per i profili privacy, in coerenza con le linee guida AgID, le misure minime ICT, gli indirizzi dell'Agenzia per la Cybersicurezza Nazionale ove applicabili, la normativa sull'amministrazione digitale, il GDPR e le specifiche esigenze sanitarie.

Ats Liguria anche per l'Area Sociosanitaria Locale 5 mantiene un inventario aggiornato di hardware, software, applicativi, banche dati, servizi cloud, utenze privilegiate e sistemi critici. L'installazione o l'uso di software non autorizzato è vietato.

Sono adottate misure per proteggere endpoint, server, reti, dispositivi mobili, sistemi medicali connessi, apparati di rete e ambienti virtuali. Le misure includono antivirus o EDR, firewall, segmentazione, filtraggio, aggiornamenti di sicurezza, controllo delle configurazioni, protezione delle connessioni remote e monitoraggio degli eventi.

I backup devono essere periodici, protetti da accessi non autorizzati, separati dagli ambienti di produzione quando necessario, verificati mediante test di ripristino e strutturati per fronteggiare incidenti fisici, tecnici e attacchi ransomware.

I dati sanitari, i dati soggetti a maggior tutela e le credenziali devono essere protetti mediante misure adeguate, comprese cifratura, segregazione logica, restrizione degli accessi e protezione dei log. I dati reali non devono essere usati in ambienti di test o formazione se è possibile usare dati anonimizzati o sintetici.

Le anomalie di sicurezza, i malware, i sospetti accessi indebiti, le vulnerabilità critiche e i malfunzionamenti che incidono sulla disponibilità o riservatezza dei dati devono essere segnalati senza ritardo secondo la procedura data breach e incident response.

Gli strumenti di posta elettronica, collaborazione, videoconferenza, messaggistica, archiviazione condivisa e produttività digitale devono essere configurati per ridurre la raccolta non necessaria di dati e metadati, garantire conservazione proporzionata e prevenire forme di controllo non consentito dei lavoratori.

Art. 31 Misure di sicurezza per i trattamenti dati affidati a terzi

I responsabili esterni e i sub-responsabili devono adottare misure di sicurezza adeguate al rischio dei trattamenti affidati e dimostrarne l'attuazione ad Ats Liguria.

Prima dell'avvio del servizio, il responsabile esterno deve fornire, se richiesto, informazioni su organizzazione privacy, sicurezza, personale autorizzato, subfornitori, localizzazione dei dati, data center, certificazioni, backup, continuità operativa, gestione incidenti, cifratura, log, amministratori di sistema, cancellazione e restituzione dei dati.

Durante l'esecuzione del contratto, il responsabile esterno deve:

- trattare i dati solo secondo istruzioni documentate;
- proteggere dati e sistemi con misure adeguate;
- mantenere un elenco aggiornato dei soggetti autorizzati e degli amministratori di sistema;
- notificare ad Ats Liguria ogni violazione o sospetta violazione senza ingiustificato ritardo;
- assistere Ats Liguria nelle richieste degli interessati e nelle DPIA;
- consentire audit o fornire evidenze equivalenti;
- non trasferire dati verso Paesi terzi senza le condizioni richieste dal GDPR e dal contratto;
- restituire o cancellare i dati al termine del servizio, salvo obblighi di legge.

Le dichiarazioni generiche di conformità non sono sufficienti quando il servizio implica trattamenti sanitari rilevanti, accesso a dati su larga scala o gestione di sistemi critici. In tali casi Ats Liguria può richiedere documentazione tecnica e organizzativa più puntuale.

Il mancato rispetto delle misure di sicurezza o la mancata collaborazione nella gestione di incidenti, audit o richieste degli interessati può determinare sospensione del servizio, contestazione contrattuale, risoluzione e richiesta di risarcimento.

Art. 32 Sicurezza di documenti ed archivi aziendali

Gli archivi analogici e digitali contenenti dati personali devono essere gestiti in modo da garantirne riservatezza, integrità, disponibilità, reperibilità, conservazione e scarto secondo le norme applicabili.

Gli archivi cartacei devono essere collocati in locali idonei, protetti da accessi non autorizzati, rischi ambientali, dispersione, furto o consultazione indebita. L'accesso ai locali di archivio è consentito solo a personale autorizzato e deve essere tracciato quando il rischio o la natura dei dati lo richiede.

La documentazione sanitaria, amministrativa e del personale deve essere conservata per il tempo previsto dalla normativa, dai massimari di scarto, dagli obblighi di conservazione e dalle esigenze di tutela dei diritti. Decorso il termine, si procede allo scarto o alla cancellazione secondo procedure documentate.

I supporti informatici, magnetici, ottici, dispositivi rimovibili, immagini diagnostiche, videoregistrazioni cliniche e ogni altro supporto contenente dati personali devono essere custoditi con misure adeguate e, quando dismessi, cancellati o distrutti in modo sicuro.

La conservazione digitale dei documenti informatici avviene nel rispetto del Codice dell'amministrazione digitale, delle linee guida AgID e delle norme di settore. Se affidata a conservatori o fornitori esterni, deve essere regolata da contratto e nomina a responsabile del trattamento, ove applicabile.

Il trasferimento di archivi dalle Aziende cessate ad Ats Liguria deve essere documentato e gestito con misure idonee a garantire continuità, integrità, tracciabilità e corretta attribuzione delle responsabilità.

Art. 33 Violazione dei dati personali

Per violazione dei dati personali si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati.

Ogni autorizzato, soggetto designato, amministratore di sistema, responsabile esterno o sub-responsabile che venga a conoscenza di una violazione o di un sospetto incidente deve segnalarlo senza ingiustificato ritardo mediante i canali aziendali previsti, fornendo tutte le informazioni disponibili.

Esempi di violazione sono: invio di referto al destinatario errato, perdita di documenti o dispositivi, accesso indebito a cartelle o applicativi, pubblicazione online non autorizzata, ransomware, furto di credenziali, disclosure a soggetto non legittimato, alterazione di dati clinici, indisponibilità prolungata di sistemi critici con impatto su dati personali.

Ats Liguria per l'Area Sociosanitaria Locale 5 con la collaborazione del componente del team del RPD di Area valuta natura, categorie e volume dei dati, numero di interessati, facilità di identificazione, conseguenze probabili, misure già adottate, rischio per diritti e libertà e necessità di notificare la violazione al Garante o comunicarla agli interessati.

Quando la violazione presenta un rischio per i diritti e le libertà delle persone fisiche, Ats Liguria notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza. Se la notifica avviene oltre 72 ore, sono indicati i motivi del ritardo.

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati, Ats Liguria comunica la violazione agli interessati senza ingiustificato ritardo, salvo i casi in cui ricorrano le condizioni di esonero previste dall'art. 34 GDPR.

La notifica al Garante e la comunicazione agli interessati indicano, nei limiti delle informazioni disponibili, natura della violazione, categorie e numero approssimativo di interessati e registrazioni, dati di contatto del RPD, probabili conseguenze, misure adottate o proposte per rimediare e attenuare gli effetti negativi.

Ats Liguria documenta tutte le violazioni, anche quelle non notificate, in apposito registro, indicando circostanze, valutazioni, decisioni, motivazioni, misure adottate, comunicazioni effettuate e azioni correttive.

Non spetta alle singole Aree effettuare notifiche di violazioni al Garante e/o agli interessati.

Art. 34 Limiti alla conservazione dei dati

I dati personali sono conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati, salvo obblighi di legge, esigenze di archiviazione nel pubblico interesse, ricerca scientifica o statistica, tutela della salute pubblica, difesa in giudizio o altri motivi legittimi previsti dalla normativa.

Per la documentazione sanitaria, le cartelle cliniche, i referti, gli atti amministrativi, la documentazione del personale, gli atti contabili, i documenti contrattuali e gli archivi pubblici si applicano i termini previsti dalle norme di settore, dai massimari di conservazione e scarto, dalle regole archivistiche e dalle procedure aziendali.

Il periodo di conservazione o i criteri usati per determinarlo devono essere indicati nel Registro delle attività di trattamento e nelle informative, ove possibile.

Alla scadenza dei termini, i dati devono essere cancellati, anonimizzati, distrutti o sottoposti a scarto secondo procedure documentate e sicure. I supporti informatici devono essere cancellati in modo tale da impedire il recupero dei dati o distrutti quando non sia possibile una cancellazione sicura.

Il riuso di apparati, supporti o dispositivi deve avvenire solo dopo cancellazione sicura o bonifica. La dismissione di beni informatici è gestita con procedure che impediscano l'accesso a dati personali residui.

La conservazione dei log deve essere proporzionata alla finalità di sicurezza, audit, verifica degli accessi, tutela dei diritti e adempimenti normativi. Tempi più lunghi richiedono una motivazione documentata e una base giuridica idonea.

Art. 35 Controllo a distanza

Ats Liguria applica ai sistemi che possono comportare controllo a distanza dei lavoratori il principio di proporzionalità, necessità, trasparenza e minimizzazione, nel rispetto dell'art. 4 della L. 300/1970, del GDPR, del Codice privacy e dei provvedimenti del Garante.

Prima dell'attivazione di sistemi di videosorveglianza, tracciamento, log applicativi, controllo accessi, geolocalizzazione, posta elettronica, strumenti di collaborazione, badge, dispositivi mobili o altri strumenti dai quali possa derivare controllo dell'attività lavorativa, Ats Liguria verifica finalità, base giuridica, necessità, alternative meno invasive, tempi di conservazione, informative e adempimenti sindacali o autorizzativi ove richiesti.

Gli strumenti informatici e i log possono essere usati per esigenze organizzative, produttive, di sicurezza del lavoro, tutela del patrimonio aziendale, sicurezza informatica e accertamento di illeciti, nei limiti di legge e delle informative rese ai lavoratori.

È vietato l'uso di sistemi occulti, generalizzati o sproporzionati di controllo dell'attività dei lavoratori. Le verifiche devono essere mirate, motivate, autorizzate e documentate secondo le procedure aziendali.

La conservazione dei metadati di posta elettronica e degli altri log dei lavoratori deve essere limitata a quanto necessario per le finalità tecniche e di sicurezza, salvo specifiche esigenze documentate e rispetto delle garanzie previste dalla normativa lavoristica.

Art. 36 Attività di verifica e controllo

Ats Liguria anche per l'Area Sociosanitaria Locale 5 svolge verifiche periodiche sull'applicazione del presente regolamento, delle procedure privacy, delle misure di sicurezza, delle autorizzazioni, delle nomine dei responsabili esterni, della gestione dei diritti e della gestione dei data breach.

Le verifiche possono essere programmate o avviate a seguito di reclami, richieste degli interessati, incidenti, rilievi del RPD, audit interni, segnalazioni, modifiche organizzative, controlli di autorità o esigenze di miglioramento del Sistema Privacy Aziendale.

Gli audit possono riguardare strutture sanitarie, amministrative e tecniche, sistemi informativi, archivi, fornitori, applicativi, log, processi di pubblicazione, gestione di consensi, oscuramenti, accessi, comunicazioni a terzi e misure fisiche di sicurezza.

Le strutture e i fornitori interessati devono collaborare, fornire la documentazione richiesta, rendere disponibili i referenti, attuare le azioni correttive e comunicare l'avanzamento degli interventi.

Gli esiti delle verifiche sono documentati e, ove necessario, trasmessi alla Direzione competente, al RPD e alle funzioni interessate per l'adozione delle misure correttive.

Art. 37 Videosorveglianza, riprese in sala operatoria, telefonia, postazioni informatiche e posta aziendale

Le attività di videosorveglianza, le eventuali riprese in sala operatoria, l'uso della telefonia, delle postazioni informatiche, della posta elettronica aziendale, degli strumenti di collaborazione e delle piattaforme digitali sono disciplinati da specifici regolamenti, procedure e informative aziendali.

Le procedure adottate dalle Aziende cessate restano applicabili solo se compatibili con il nuovo assetto, con il GDPR, con il Codice privacy, con la normativa sul lavoro e con i provvedimenti del Garante, fino alla loro revisione o sostituzione con atti unitari di Ats Liguria.

La videosorveglianza è ammessa per finalità determinate e legittime, quali sicurezza delle persone, tutela del patrimonio, gestione di aree sensibili o esigenze organizzative, nel rispetto di minimizzazione, limitazione degli angoli di ripresa, cartellonistica, tempi di conservazione, accessi autorizzati e garanzie lavoristiche.

Le riprese in sala operatoria o in altri contesti clinici sono ammesse solo quando fondate su una base giuridica idonea e su una finalità lecita, documentata e proporzionata, come cura, documentazione clinica, formazione o tutela giudiziaria nei casi previsti. Devono essere definite informative, consensi ove richiesti, accessi, conservazione, oscuramenti e misure di sicurezza.

Per la posta elettronica aziendale e i servizi connessi, Ats Liguria tiene conto del documento di indirizzo del Garante del 6 giugno 2024 sui metadati nel contesto lavorativo. La conservazione dei metadati deve essere proporzionata, configurata in modo consapevole e non trasformarsi in controllo generalizzato dell'attività dei lavoratori.

Le postazioni informatiche sono strumenti di lavoro. Il loro uso deve rispettare le procedure aziendali, le misure di sicurezza, le regole di conservazione dei dati, i divieti di installazione non autorizzata e le istruzioni su Internet, e-mail, dispositivi rimovibili, cloud e strumenti di messaggistica.

Art. 38 Redazione degli atti

Nella redazione di deliberazioni, determinazioni, decreti, provvedimenti, note, verbali, relazioni, atti istruttori e allegati, le strutture devono applicare i principi di minimizzazione, pertinenza, non eccedenza, esattezza e limitazione della finalità.

I dati personali devono essere inseriti negli atti solo quando necessari alla motivazione, al dispositivo, all'identificazione del procedimento o all'adempimento di un obbligo di legge. Quando il dato non è necessario, deve essere omesso, generalizzato, pseudonimizzato o riportato in allegato non pubblicabile.

È vietato inserire nell'oggetto o nel dispositivo dell'atto dati relativi alla salute, disabilità, permessi, idoneità, infortuni, maternità, dipendenze, salute mentale, procedimenti disciplinari, dati giudiziari o altre informazioni delicate se non strettamente necessario e previsto dalla legge.

Quando il provvedimento si fonda su documenti contenenti dati particolari, dati giudiziari o dati soggetti a maggior tutela, la motivazione può richiamare gli atti istruttori conservati nel fascicolo, evitando di riprodurre nel testo pubblicabile informazioni eccedenti.

Gli allegati contenenti dati personali devono essere classificati correttamente, indicando se siano pubblicabili, non pubblicabili o pubblicabili previa anonimizzazione. La struttura proponente è responsabile della verifica preliminare dei dati contenuti nell'atto e negli allegati.

Gli atti destinati alla pubblicazione devono essere predisposti già in fase di redazione in una versione conforme alla disciplina sulla protezione dei dati, evitando interventi correttivi tardivi e rischi di pubblicazione indebita.

Art. 39 Pubblicazione degli atti

La pubblicazione di atti, documenti e informazioni sul sito istituzionale, sull'albo online, nella sezione Amministrazione trasparente o in altre piattaforme deve avvenire nel rispetto del GDPR, del Codice privacy, del D.lgs. 33/2013 e delle Linee guida del Garante in materia di trasparenza e pubblicazione online da parte dei soggetti pubblici.

Prima della pubblicazione la struttura competente verifica: obbligo normativo di pubblicazione, durata della pubblicazione, dati da pubblicare, eventuali dati da oscurare, presenza di categorie particolari di dati, dati giudiziari, dati di minori, dati relativi a soggetti vulnerabili, dati non pertinenti o eccedenti.

La pubblicazione all'albo online non comporta automaticamente l'obbligo di pubblicazione nella sezione Amministrazione trasparente. Ogni pubblicazione deve avere una specifica base normativa e deve rispettare tempi e limiti propri.

È vietata la diffusione di dati relativi alla salute. Devono essere omessi o oscurati anche dati idonei a rivelare indirettamente lo stato di salute, quali causali di assenza, codici di patologia, riferimenti a visite, certificazioni, invalidità, disabilità, permessi o benefici connessi a condizioni sanitarie, se non ricorra una specifica disposizione di legge che ne imponga la pubblicazione nei limiti strettamente necessari.

Devono essere adottate misure tecniche e organizzative per evitare indicizzazione indebita da parte dei motori di ricerca quando non necessaria, permanenza oltre i termini, duplicazione incontrollata, pubblicazione di allegati errati o versioni non oscurate.

In caso di pubblicazione errata o eccedente, la struttura deve attivarsi immediatamente per la rimozione o l'oscuramento, segnalando l'evento secondo la procedura data breach quando vi sia una violazione dei dati personali.

Art. 40 Regole di comportamento da adottare a tutela della privacy

Il personale e i collaboratori di Ats Liguria anche per l'Area Sociosanitaria Locale 5 devono adottare comportamenti coerenti con il segreto professionale, il segreto d'ufficio, il dovere di riservatezza, il presente regolamento e le istruzioni ricevute.

La documentazione cartacea contenente dati personali deve essere custodita in armadi, cassetti, locali o contenitori chiusi. Al termine dell'attività, i documenti non devono restare su scrivanie, banconi, stampanti, fotocopiatrici, carrelli o aree accessibili a utenti, visitatori o personale non autorizzato.

Il trasporto interno di cartelle cliniche, referti o altra documentazione sanitaria deve avvenire con buste, contenitori o modalità che impediscano la lettura accidentale o l'accesso non autorizzato.

La distruzione di documenti cartacei contenenti dati personali deve avvenire tramite strumenti o servizi che impediscano la ricostruzione dei documenti. È vietato gettare documenti leggibili nei normali cestini.

Le tabelle di presenza, elenchi pazienti, agende, turni, richieste, referti e informazioni cliniche non devono essere esposti in luoghi visibili al pubblico, salvo che siano adottate modalità non identificative o strettamente necessarie.

Le informazioni sulla presenza di un paziente presso una struttura possono essere fornite solo nei limiti della volontà dell'interessato e delle procedure aziendali. Se l'interessato ha chiesto riservatezza, la presenza non deve essere confermata.

Le informazioni sullo stato di salute possono essere comunicate a familiari, caregiver o terzi solo se autorizzati dall'interessato, legittimati dalla legge o necessari in situazioni di emergenza, incapacità o tutela della salute. La comunicazione deve essere limitata a quanto necessario.

Le richieste delle forze dell'ordine o di altre autorità sono gestite dalle funzioni competenti, previa identificazione del richiedente, verifica dei poteri e acquisizione della richiesta formale quando necessaria. Il personale non deve consegnare documenti o informazioni sulla base di richieste informali non verificate.

Le conversazioni con utenti, pazienti e colleghi devono svolgersi con prudenza, evitando che terzi ascoltino diagnosi, terapie, dati personali, condizioni economiche, informazioni familiari o altri dati riservati. Negli ambienti condivisi si usano toni, spazi e modalità adeguati.

Al telefono si forniscono dati personali solo dopo ragionevole verifica dell'identità del chiamante e della sua legittimazione. In caso di dubbio, è preferibile richiamare un recapito già noto o indirizzare l'interessato verso canali sicuri.

L'uso di fax, ove ancora previsto, deve essere limitato ai casi in cui non siano disponibili canali più sicuri e compatibili con la normativa. Nelle comunicazioni tra pubbliche amministrazioni si applicano le regole del Codice dell'amministrazione digitale, privilegiando strumenti telematici idonei e tracciabili.

Prima di inviare e-mail, PEC o messaggi tramite piattaforme autorizzate, l'operatore verifica destinatari, allegati, oggetto, contenuto e necessità dell'invio. Per dati sanitari o particolarmente delicati si adottano canali protetti, cifratura o portali autenticati quando disponibili.

È vietato usare account personali, servizi cloud personali, applicazioni di messaggistica non autorizzate o strumenti non approvati per trattare o trasmettere dati sanitari o dati aziendali.

È vietato caricare referti, immagini diagnostiche, cartelle cliniche, dati di pazienti, dati di lavoratori o documenti aziendali contenenti dati personali su piattaforme di intelligenza artificiale generativa o altri servizi online non autorizzati da Ats Liguria. Eventuali strumenti basati su IA possono essere impiegati solo se approvati, valutati sotto il profilo privacy e sicurezza, e regolati da istruzioni aziendali.

Le stampe e le fotocopie devono essere ritirate immediatamente. Non deve essere usata carta riciclata che contenga dati personali leggibili. Le stampanti condivise devono essere configurate, ove possibile, con rilascio sicuro della stampa.

Il personale deve segnalare subito errori di invio, smarrimento di documenti, accessi indebiti, uso improprio di credenziali, furto di dispositivi, malware, pubblicazioni errate o ogni altra situazione che possa costituire violazione di dati personali.

Art. 41 Comportamenti individuali e sanzionabilità

La violazione delle norme in materia di protezione dei dati personali, del segreto d'ufficio, del segreto professionale, delle istruzioni aziendali o del presente regolamento può comportare responsabilità disciplinare, civile, amministrativa o penale secondo la gravità del fatto e le norme applicabili.

Sono condotte particolarmente rilevanti: accesso a dati senza ragione di servizio; consultazione di dati di familiari, colleghi o personaggi noti per curiosità; comunicazione non autorizzata di dati sanitari; pubblicazione indebita; invio a destinatario errato per negligenza; cessione di credenziali; uso di strumenti non autorizzati; mancata segnalazione di data breach; conservazione non autorizzata di copie; estrazione di dati per finalità personali; uso di dati aziendali per attività estranee al servizio.

Resta fermo l'obbligo dei dipendenti pubblici di osservare il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali, secondo il codice di comportamento, i contratti collettivi, i regolamenti aziendali e le disposizioni vigenti.

Le strutture competenti valutano le condotte, acquisiscono gli elementi necessari, assicurano il contraddittorio nei procedimenti disciplinari e adottano le misure organizzative o correttive necessarie a evitare il ripetersi dell'evento.

La sanzionabilità del comportamento individuale non esclude l'obbligo dell'Azienda di valutare eventuali carenze organizzative, formative, tecniche o procedurali che abbiano contribuito all'evento.

Art. 42 Norme transitorie e finali

Per quanto non espressamente previsto dal presente regolamento si applicano il GDPR, il Codice privacy, la normativa sanitaria e sociosanitaria, le norme sull'amministrazione digitale, la disciplina su accesso e trasparenza, i provvedimenti del Garante, gli orientamenti EDPB pertinenti e le procedure aziendali di Ats Liguria.

A decorrere dal 1 gennaio 2026, i riferimenti contenuti nei precedenti regolamenti, informative, moduli, atti di designazione, nomine, procedure, contratti e istruzioni alle Aziende sociosanitarie 1, 2, 3, 4, 5 e a Liguria Salute devono intendersi riferiti ad Ats Liguria, nei limiti di compatibilità con il nuovo assetto organizzativo e salvo revisione espressa.

Le autorizzazioni, designazioni interne, nomine a responsabile esterno, informative, consensi, procedure, regolamenti e misure adottati dalle Aziende cessate restano efficaci se compatibili con il presente regolamento e con il nuovo titolare, fino alla loro revisione, sostituzione o cessazione.

Ats Liguria programma l'armonizzazione progressiva del Sistema Privacy Aziendale.

Le strutture dell'Area Sociosanitaria Locale 5 continuano a erogare servizi e prestazioni in continuità territoriale con la cessata Azienda, applicando il presente regolamento e segnalando alla Direzione, al RPD e al suo team e alle funzioni competenti ogni criticità derivante dal passaggio al nuovo assetto.

Ats Liguria si riserva di modificare o integrare il presente regolamento in caso di sopravvenienze normative, provvedimenti dell'Autorità Garante, orientamenti EDPB, modifiche organizzative, innovazioni tecnologiche, audit, data breach o esigenze operative. Le modifiche sono comunicate alle strutture interessate e rese disponibili con modalità idonee.