SCHEMA RIASSUNTIVO · MATERIA

Privacy e GDPR

Reg. UE 2016/679 e d.lgs. 196/2003: trattamento dati personali, ruoli, diritti dell'interessato.

Studia questa materia sul sito →

8 argomenti · 55 lezioni

Lezioni principali

Diritti dell'interessato (artt. 15-22 GDPR)

Il GDPR riconosce all'interessato otto diritti fondamentali. Una PA che tratta dati deve garantirne l'esercizio con tempi rapidi e modalità chiare.

I principi del GDPR applicati alla PL

Liceità, finalità, minimizzazione, accountability. Come operare nel rispetto del Regolamento UE 2016/679.

DPO e DPIA: ruoli e strumenti del GDPR

Il GDPR impone la nomina di un Data Protection Officer in molte PA e la Valutazione d'Impatto (DPIA) per trattamenti ad alto rischio. Ruoli chiave per la compliance.

Videosorveglianza pubblica (GDPR + Garante)

La videosorveglianza pubblica è disciplinata da: GDPR (Reg. UE 2016/679) + Codice Privacy (D.Lgs. 196/2003 modif. D.Lgs. 101/2018) + Provvedimenti Garante (in particolare 8/4/2010 e successivi aggiornamenti) + L. 38/2009 e D.L. 14/2017 (sicurezza urbana). Requisiti: finalità specifica (sicurezza, traffico, decoro), DPIA (valutazione impatto privacy ex art. 35 GDPR), cartelli informativi ben visibili, conservazione delle immagini per il tempo strettamente necessario, normalmente breve, con durata motivata in base alla finalità e al rischio, accesso ai filmati solo personale autorizzato (PL, AG su richiesta). Privacy by design: zone sensibili oscurate (interno abitazioni, ingressi privati). Per la PL: gestione operativa centrali, accesso filmati per indagini PG, comunicazione AG, rispetto rigoroso normativa privacy. Sanzioni Garante elevate per violazioni.

Trasferimento dati fuori dall'UE

Il GDPR consente il trasferimento di dati personali fuori dall'UE solo se il Paese di destinazione garantisce un livello di protezione adeguato. Cloud USA, schemi Privacy Framework e clausole contrattuali.

Fondamenti del GDPR

GDPR (Reg. UE 2016/679) — struttura e applicazione

Il GDPR (Regolamento UE 2016/679) è la norma europea sulla protezione dei dati personali. In vigore dal 25 maggio 2018. Direttamente applicabile in tutti gli Stati UE. 99 articoli + 173 considerando. Principio: tutela diritti fondamentali. In Italia integrato dal Codice privacy novellato (D.lgs. 196/2003 modificato da D.lgs. 101/2018).

Definizioni chiave del GDPR (art. 4)

L'art. 4 GDPR definisce i concetti fondamentali: dato personale, trattamento, interessato, titolare, responsabile, consenso, data breach. Comprensione di queste definizioni è essenziale per l'applicazione corretta del Regolamento.

Basi giuridiche del trattamento (art. 6 GDPR)

L'art. 6 GDPR elenca 6 basi giuridiche alternative per il trattamento di dati personali: a) consenso, b) esecuzione contratto, c) obbligo legale, d) vitali interessi, e) interesse pubblico/esercizio pubblici poteri, f) interesse legittimo. Per la PA italiana: le basi più rilevanti sono lett. c (obbligo legale) e lett. e (interesse pubblico/esercizio pubblici poteri) — il consenso è raramente utilizzato dalla PA (lett. a) e l'interesse legittimo non si applica (lett. f). Tipicamente la PL si basa su norme di legge specifiche (CdS, D.Lgs. 114/1998, TUA, ecc.) che fissano obblighi legali o funzioni pubbliche. Per categorie particolari (art. 9): deroghe specifiche, tipicamente lett. g (interesse pubblico rilevante) e lett. b (obbligo legale rilevante).

Consenso al trattamento (art. 7 GDPR)

Il consenso (art. 7 GDPR) deve essere libero, specifico, informato e inequivocabile. Dimostrabile dal titolare. Revocabile in qualsiasi momento (senza pregiudicare trattamenti pregressi). Non valido se pre-selezionato, da condizioni inique, imposto. Requisiti stringenti per dati particolari (consenso esplicito).

Informativa privacy (artt. 13-14 GDPR)

L'informativa (artt. 13-14 GDPR) è obbligatoria: prima della raccolta (art. 13) o al momento della raccolta indiretta (art. 14). Deve essere concisa, trasparente, intelligibile, accessibile, scritta. Contenuti obbligatori: identità titolare, DPO, finalità, base giuridica, destinatari, tempi, diritti. Omissione = sanzione.

Privacy by design e by default (art. 25 GDPR)

L'art. 25 GDPR impone privacy by design (protezione fin dalla progettazione) e by default (impostazioni predefinite più restrittive). Il titolare implementa misure tecniche e organizzative adeguate. Pseudonimizzazione, minimizzazione, trasparenza. Certificazioni (art. 42) possono aiutare.

Registro delle attività di trattamento (art. 30)

L'art. 30 GDPR impone ai titolari di tenere un registro delle attività di trattamento. Obbligatorio per PA (sempre), imprese 250 dipendenti, o trattamenti a rischio. Contenuti: finalità, categorie interessati e dati, destinatari, trasferimenti extra-UE, tempi conservazione, misure sicurezza. Strumento di accountability.

Misure di sicurezza (art. 32 GDPR)

L'art. 32 GDPR impone misure tecniche e organizzative adeguate al rischio per la sicurezza dei dati personali. Pseudonimizzazione, crittografia, capacità ripristino, test periodici. Misure proporzionate al rischio. Responsabile esterno deve garantire stesse misure. Valutazione continua.

Data breach — notifica (artt. 33-34 GDPR)

L'art. 33 GDPR impone la notifica al Garante entro 72 ore da quando si è venuti a conoscenza della violazione di dati personali. Se alto rischio,

Soggetti e responsabilità GDPR

Titolare del trattamento — ruolo e obblighi

Il titolare del trattamento (art. 4 n. 7 GDPR) è chi determina finalità e mezzi del trattamento. Responsabile primario della compliance. Obblighi: informativa, registro, misure sicurezza, DPIA, DPO (se obbligato), gestione diritti interessati, data breach. Sanzioni elevate. Persona fisica/giuridica.

Responsabile del trattamento (art. 28)

Il responsabile del trattamento (art. 28 GDPR) tratta dati per conto del titolare. Relazione regolata da contratto scritto obbligatorio. Contenuto: oggetto, durata, natura, finalità, tipi dati, obblighi, misure sicurezza. Sub-responsabili solo con autorizzazione. Responsabilità solidale con titolare in caso di violazioni.

DPO — Data Protection Officer (artt. 37-39)

Il DPO (Responsabile Protezione Dati, artt. 37-39 GDPR) è figura obbligatoria per: PA, trattamenti che richiedono monitoraggio sistematico su larga scala, dati particolari su larga scala. Requisiti: competenze specifiche, indipendenza, risorse. Funzioni: consulenza, sorveglianza, cooperazione con Garante. Non sanzionato personalmente.

Diritti dell'interessato (artt. 15-22 GDPR)

Gli artt. 15-22 GDPR elencano i diritti dell'interessato: art. 15 accesso (sapere quali dati sono trattati e ottenerne copia); art. 16 rettifica; art. 17 cancellazione ("diritto all'oblio"); art. 18 limitazione; art. 19 notifica delle modifiche/cancellazioni; art. 20 portabilità (limitato per PA); art. 21 opposizione; art. 22 no decisioni automatizzate. Tempi di risposta: 30 giorni (estendibili a 60-90 in casi complessi). Limitazioni rilevanti: alcuni diritti possono essere limitati quando il trattamento riguarda indagini, sicurezza pubblica o attività di polizia giudiziaria (D.Lgs. 51/2018 LED + art. 23 GDPR + art. 2-quinquiesdecies Codice Privacy). Per la PL: gestione delle richieste degli interessati con valutazione caso per caso, motivazione delle eventuali limitazioni, coordinamento con DPO.

Garante per la protezione dei dati personali

Il Garante per la protezione dei dati personali è l'autorità amministrativa indipendente che vigila sull'attuazione del GDPR e del Codice Privacy in Italia. È composto da membri eletti dal Parlamento (due dalla Camera, due dal Senato), con mandato di 7 anni non rinnovabile. Funzioni: vigilanza, controllo, provvedimenti correttivi e sanzionatori (anche elevatissimi), pareri su atti normativi, gestione reclami degli interessati, cooperazione UE (con altre autorità di protezione dati). Sede: Roma. Sito: www.garanteprivacy.it. Per la PL: autorità di riferimento per reclami dei cittadini, notifiche data breach (entro 72h), provvedimenti su videosorveglianza, body-cam, fototrappole, banche dati. Sanzioni: pecuniarie elevate (fino 20 mln € o 4% fatturato per casi gravi), applicabili anche alle PA con criteri specifici.

Sanzioni GDPR (art. 83)

Le sanzioni del GDPR (art. 83) sono pecuniarie amministrative di entità significativa. Due fasce: violazioni meno gravi fino a 10 milioni di € o 2% del fatturato (per le imprese); violazioni più gravi fino a 20 milioni di € o 4% del fatturato. Anche le PA possono essere destinatarie di provvedimenti correttivi e sanzioni secondo il GDPR e il Codice Privacy italiano (D.Lgs. 196/2003 modif. D.Lgs. 101/2018). I criteri di applicazione tengono conto di: gravità, durata, natura intenzionale o colposa, dimensione PA, misure adottate, recidiva, cooperazione con il Garante. Sanzioni accessorie: ordini di limitazione/cancellazione, ammonimenti, pubblicazione del provvedimento. Per la PL: rischio sanzionatorio reale per violazioni di videosorveglianza, banche dati, comunicazioni illegittime, conservazione eccessiva. Cooperazione costruttiva con Garante mitiga le sanzioni.

Codice privacy (D.lgs. 196/2003) — novellato

Applicazione pratica e PL

Videosorveglianza e body-cam della Polizia Locale

Le body-cam sono telecamere indossate dagli operatori PL: utilizzabili solo se previste da adeguata base normativa/regolamentare interna, con: DPIA (art. 35 GDPR), informativa ai cittadini coinvolti, limiti chiari di attivazione (eventi specifici, no riprese continue), istruzioni operative scritte ai designati. Provvedimenti del Garante (es. 13/12/2017) hanno fornito linee guida specifiche. La videosorveglianza generale della PL (telecamere fisse nella zona urbana) segue regole simili: regolamento, DPIA, cartelli informativi, conservazione per il tempo strettamente necessario, normalmente breve, motivato. NO uso ordinario di body-cam senza base regolamentare adeguata. Per la PL: strumento valido se gestito correttamente; cooperazione con DPO + sindacati per implementazione conforme.

Controlli sul lavoro e privacy dei dipendenti

I controlli a distanza sui lavoratori sono disciplinati dall'art. 4 L. 300/1970 (Statuto lavoratori) novellato dal D.lgs. 151/2015 (Jobs Act). Impianti audiovisivi e strumenti controllo: solo per esigenze organizzative, produttive, sicurezza, previa accordo sindacale o autorizzazione ITL. Dati utilizzabili a fini disciplinari SOLO con informativa ex art. 13 GDPR. PL datore: segue stesse regole.

Cookie e trattamenti online (siti PA e PL)

I cookie sono regolati dalla Direttiva ePrivacy 2002/58/CE, art. 122 Codice privacy, Linee guida Garante 10 giugno 2021. Distinzione tra tecnici (no consenso), analitici (consenso salvo anonimizzazione), profilazione (consenso esplicito). Banner cookie con parità scelta accetta/rifiuta. Siti PA e PL: obbligo conformità; preferibili solo cookie tecnici.

Marketing, telemarketing e registro opposizioni

Il marketing e il telemarketing sono disciplinati da GDPR + Codice Privacy + Codice Consumo (D.Lgs. 206/2005) + L. 5/2018 (Registro Pubblico Opposizioni — RPO). Competenze primarie: AGCM (Autorità Garante Concorrenza e Mercato per pratiche scorrette), Garante Privacy (per uso illecito dati). Il Registro Pubblico Opposizioni consente ai cittadini di opporsi al telemarketing. Per la Polizia Locale: tema poco utile per concorso e operatività quotidiana — la PL può essere coinvolta solo per pubblicità abusiva locale (volantini in strada, manifesti senza autorizzazione, insegne illegittime). Argomento di sfondo culturale, non centrale; priorità a verbali, banche dati, videosorveglianza, atti PG.

Privacy nelle scuole e in sanità

La privacy nelle scuole e in sanità è materia ampia. Scuole: dati di minori (tutela rafforzata art. 8 GDPR + art. 2-quinquies Codice Privacy), trattamenti del personale docente, fotografie e video di iniziative scolastiche. Sanità: dati sanitari = particolari art. 9 GDPR, FSE (Fascicolo Sanitario Elettronico), referti, cartelle cliniche, procedure HIPAA-like nazionali. Competenze primarie: dirigenti scolastici, ASL, strutture sanitarie. Per la Polizia Locale: argomento non centrale per concorso; il focus operativo PL è su: minori nei sinistri o procedimenti (oscuramento, identificazione con genitori), TSO (esecuzione ordinanza Sindaco), sinistri con feriti (dati sanitari trattati con cautele), dati sanitari nei procedimenti (referti acquisiti). Argomento ridotto rispetto a verbali, banche dati, videosorveglianza.

Accesso agli atti vs privacy — bilanciamento

Il diritto d'accesso (L. 241/1990), accesso civico (D.lgs. 33/2013), FOIA (D.lgs. 97/2016) possono confliggere con la privacy. Bilanciamento: accesso prevale se interesse concreto e attuale del richiedente; privacy prevale per dati sensibili senza necessità difesa. Linee guida ANAC 2017 e Garante su accesso civico. PL: frequenti richieste su verbali, incidenti, segnalazioni.

Pubblicazioni di trasparenza e limiti privacy

Privacy PL: basi operative

Dati personali, particolari e giudiziari

Il GDPR distingue tre categorie principali di dati: dati personali (art. 4 n. 1: qualsiasi informazione riguardante persona fisica identificata o identificabile — nome, indirizzo, codice fiscale, targa, immagine); dati particolari ex art. 9 GDPR (origine razziale/etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici, biometrici per identificazione, dati sanitari, vita sessuale); dati relativi a condanne penali e reati ex art. 10 GDPR (dati giudiziari). Trattamento più rigoroso: per particolari serve base giuridica rinforzata + misure di sicurezza specifiche; per giudiziari serve base normativa specifica. Esempi PL: verbale CdS (dati personali); referto sanitario in sinistro (dati particolari sanitari); CNR/atto PG (dati giudiziari); foto ambito identificativo (potenzialmente biometrici).

GDPR vs D.Lgs. 51/2018 (LED): quale si applica alla PL?

La PL svolge attività con due nature diverse, soggette a regimi privacy distinti: il GDPR (Reg. UE 2016/679) si applica all'attività amministrativa (es. verbali CdS, sanzioni amministrative, gestione SCIA, ordinanze, banche dati anagrafiche); il D.Lgs. 51/2018 (recepimento Direttiva LED — Law Enforcement Directive 2016/680/UE) si applica alle finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (es. CNR, atti di PG, sequestri, identificazioni di indiziati). Esempio cardine: lo stesso operatore PL applica GDPR quando redige verbale CdS, LED quando redige CNR per reato. Conseguenze pratiche: basi giuridiche diverse, diritti dell'interessato modulati, conservazione dati con criteri specifici. Per la PL: distinzione fondamentale per concorso e operatività.

Accesso alle banche dati della PL

L'accesso alle banche dati da parte della PL è uno dei trattamenti più sensibili. Principi cardine: accesso solo per finalità di servizio (mai per curiosità o per uso privato); credenziali personali e non cedibili (no condivisione); tracciamento obbligatorio degli accessi (chi, quando, quale dato consultato); principio di necessità e minimizzazione (non consultare oltre il necessario per il caso). Banche dati tipiche: CED interforze SDI (Sistema di Indagine), ANPR (anagrafe nazionale), PRA (Pubblico Registro Automobilistico), MCTC (motorizzazione), casellario giudiziale, anagrafe tributaria (limitato), banca dati Albo Gestori Ambientali. Abuso: responsabilità disciplinare + civile + PENALE (art. 615-ter c.p. accesso abusivo a sistema informatico, fino 3 anni; art. 326 c.p. rivelazione segreto d'ufficio).

Privacy nei verbali della Polizia Locale

I verbali della PL contengono inevitabilmente dati personali — il loro trattamento è soggetto al GDPR (per illeciti amministrativi) o al D.Lgs. 51/2018 (per atti di PG). Dati tipici: trasgressore (nome, cognome, indirizzo, codice fiscale), proprietario veicolo (se distinto), targa, descrizione del fatto, luogo, data/ora, eventuali testimoni. Principio di minimizzazione (art. 5 GDPR): inserire solo i dati necessari alla finalità del verbale; non includere dati eccedenti (es. informazioni sanitarie irrilevanti, opinioni personali, dati di terzi non coinvolti). Notifiche: solo all'interessato e a soggetti normativamente previsti; busta chiusa + PEC per evitare visibilità a terzi. Pubblicazione: i verbali individuali NON si pubblicano salvo casi specifici e con anonimizzazione. Per la PL: cura particolare nella redazione + nelle notifiche.

Privacy nei sinistri stradali

I sinistri stradali comportano un trattamento particolarmente delicato perché coinvolgono spesso dati sanitari (referti, condizioni feriti — dati particolari art. 9 GDPR), dati assicurativi (compagnie, polizze, franchigie), foto/video di persone e veicoli (immagini = dati personali). Verbale di sinistro: redatto dalla PL, contiene tutti questi dati con base giuridica obbligo legale + interesse pubblico. Accesso agli atti (art. 11 CdS + accesso ex L. 241/1990): consentito agli aventi diritto (parti coinvolte, eredi, assicurazioni mandatarie); terzi: solo con motivazione

Privacy: tecnologie e comunicazione

Fototrappole ambientali — privacy

Le fototrappole ambientali sono telecamere autonome con sensori di movimento utilizzate dalla PL per il contrasto agli abbandoni di rifiuti, scarichi abusivi, altri illeciti ambientali. Trattano dati personali (immagini di persone, targhe veicoli) → GDPR + D.Lgs. 51/2018 se per finalità penali. Requisiti di legittimità: 1) base regolamentare (regolamento comunale); 2) finalità specifica (ambientale, sicurezza urbana); 3) DPIA (valutazione impatto privacy ex art. 35 GDPR); 4) informativa (cartelli ove previsti, anche generici per zone con fototrappole nascoste); 5) minimizzazione (registrazione solo a movimento, ripresa mirata); 6) conservazione delle immagini per il tempo strettamente necessario, normalmente breve, motivato in base alla finalità; 7) accesso limitato al personale autorizzato. Utilizzo nel verbale: prove se acquisite legittimamente. Per la PL: strumento centrale ma soggetto a cautele.

ZTL, autovelox, varchi elettronici

I sistemi di rilevamento elettronico della PL — autovelox (controllo velocità), ZTL (Zone a Traffico Limitato), varchi elettronici (accesso aree riservate) — trattano massicciamente dati personali: targhe, immagini dei veicoli, eventualmente del conducente. Base giuridica: obbligo legale (CdS, regolamenti comunali) + interesse pubblico. Conservazione: solo per il tempo necessario alla notifica del verbale e all'eventuale procedimento (di norma alcuni mesi/anni a seconda della tipologia, con tempi specifici per Comune); dati di passaggi non sanzionati vanno eliminati prima. Accesso alle foto: solo all'interessato (sanzionato/proprietario veicolo) + autorità competente; oscuramento dei terzi (passeggeri, persone in foto) obbligatorio nelle copie diffuse. Cartelli informativi: obbligatori (omologazione + segnalazione varco/ZTL).

Conservazione dei dati nella PA

La conservazione dei dati personali è uno dei principi cardine del GDPR (art. 5 par. 1 lett. e: "limitazione della conservazione"). Regola generale: i dati devono essere conservati per un tempo non superiore a quello necessario al conseguimento delle finalità per cui sono trattati. Tempi specifici sono spesso fissati da norme di settore (es. 5 anni verbali CdS per riscossione, 10 anni atti contabili, 30 gg di norma per immagini videosorveglianza, prescrizioni per atti di PG). Criteri: necessità, proporzionalità, motivazione del periodo. Documentazione: registro dei trattamenti deve indicare i tempi (art. 30 GDPR). Distruzione: con procedure sicure (no semplice cestino, distruzione documentale + cancellazione digitale certificata). Per la PL: ogni tipologia di dato ha tempo proprio; politiche di conservazione del Comune.

Comunicazione e diffusione dei dati

Il GDPR distingue comunicazione (dare conoscenza a soggetti determinati) da diffusione (dare conoscenza a soggetti indeterminati). Per la PL: la comunicazione tra uffici comunali e con altre amministrazioni (Prefettura per CdS, Motorizzazione, Procura per CNR, assicurazioni in casi specifici) è legittima se ha base giuridica (norma di legge o interesse pubblico) e rispetta principio di minimizzazione. La diffusione online (pubblicazione su siti, social, ecc.) è vietata salvo base normativa specifica (es. Albo Pretorio per atti dovuti, Amministrazione Trasparente con limiti). Differenza chiave: comunicare ≠ pubblicare. Per la PL: cura particolare nelle comunicazioni a soggetti diversi dal Comune, valutazione caso per caso, sempre minimizzazione.

Pubblicazione online di atti comunali

La pubblicazione online di atti comunali segue due binari: Albo Pretorio online (D.Lgs. 267/2000 TUEL + L. 69/2009: pubblicazione legale di atti per dare loro efficacia) e Amministrazione Trasparente (D.Lgs. 33/2013: trasparenza dell'attività amministrativa). Principio: solo i dati necessari alla finalità di pubblicazione; dati eccedenti devono essere oscurati

Privacy: soggetti e responsabilità

Privacy di minori e soggetti vulnerabili

I minori e i soggetti vulnerabili (anziani non autosufficienti, persone con disabilità, vittime di reati gravi) godono di tutela rafforzata nel trattamento dei dati personali. Per i minori: art. 8 GDPR (consenso digitale: 16 anni in UE, 14 anni in Italia); art. 2-quinquies Codice Privacy. Per la PL: incidenti stradali con minori richiedono cautela estrema (oscuramento volti, dati pseudonimizzati nelle copie diffuse); scuole: rapporti con istituti per controlli, manifestazioni, attraversamenti — minimizzazione massima; vittime di reati: tutela rafforzata (artt. 6-9 D.Lgs. 51/2018 LED); TSO: dati sanitari particolari + cautele. Mai pubblicare identificativi di minori in atti diffusi (Albo, social, comunicati). Mai diffondere foto identificabili di vittime fragili senza consenso/base normativa.

Responsabilità del dipendente pubblico in materia privacy

Il dipendente pubblico che viola la normativa privacy può essere soggetto a triplice responsabilità: disciplinare (procedimento ex D.P.R. 3/57 + CCNL: dal richiamo al licenziamento), civile (risarcimento danni ex art. 82 GDPR + eventuale rivalsa dell'amministrazione), PENALE. Reati specifici: art. 615-ter c.p. (accesso abusivo a sistema informatico, fino 5 anni se commesso da PU); art. 326 c.p. (rivelazione e utilizzazione di segreti d'ufficio, fino 3 anni); art. 167 D.Lgs. 196/2003 (trattamento illecito di dati personali per profitto/danno, fino 3 anni); art. 167-bis (comunicazione/diffusione illecita su larga scala). Altri reati possibili: art. 314 (peculato d'uso), art. 323 (abuso d'ufficio), art. 479 (falso ideologico). Per la PL: cautela massima nell'uso di banche dati e nei trattamenti.

Autorizzati al trattamento (designati)

Gli autorizzati al trattamento (in italiano anche "designati", art. 2-quaterdecies Codice Privacy + art. 29 GDPR) sono i dipendenti o collaboratori che operano sotto l'autorità del titolare/responsabile del trattamento e che trattano materialmente i dati personali. Per la PL: tutti gli agenti, ufficiali, dipendenti amministrativi che accedono a verbali, banche dati, archivi. Nomina formale: atto del Comune (Sindaco/dirigente) che li designa, individua le istruzioni operative scritte, l'ambito autorizzato (quali dati, quali finalità), i limiti, la durata. Formazione obbligatoria sulla privacy. Tracciamento degli accessi. Responsabilità: il designato risponde personalmente delle violazioni (disciplinare, civile, penale). Per la PL: ogni operatore deve essere formalmente designato + ricevere istruzioni scritte.

Responsabili esterni del trattamento applicati alla PL

Il responsabile esterno del trattamento (art. 28 GDPR) è il soggetto terzo (di norma un'azienda) che tratta dati personali per conto del titolare (il Comune). Per la PL: numerosi servizi sono affidati a fornitori esterni che diventano responsabili: software house del gestionale verbali, gestori del sistema ZTL, gestori della videosorveglianza, cloud comunale (storage dati), società di stampa e notifica dei verbali, gestori siti web con dati di cittadini. Obblighi: contratto scritto specifico (DPA — Data Processing Agreement) che regoli oggetto, durata, finalità, categorie dati, obblighi del responsabile (sicurezza, riservatezza, sub-responsabili, restituzione/cancellazione a fine contratto, supporto ai diritti dell'interessato, notifica data breach al titolare, audit). Il Comune resta titolare e responsabile delle scelte; il responsabile esterno risponde direttamente per propri inadempimenti.

Informativa privacy nei procedimenti della PL

L'informativa privacy (artt. 13-14 GDPR) è l'atto con cui il titolare comunica all'interessato come tratta i suoi dati. Obbligatoria in tutti i trattamenti, ma con modulazioni per attività di PG (D.Lgs. 51/2018). Per la PL: deve essere predisposta per ogni procedimento — verbali CdS (informativa sintetica nel verbale + estesa online), accesso ZTL (cartelli + estesa online), istanze dei cittadini (al momento della presentazione),

Privacy: casi pratici e schema operativo PL

Data breach nella PA — casistica pratica

Il data breach (violazione dei dati personali) nella PA si manifesta con casistiche frequenti: invio PEC al destinatario sbagliato (errore battitura), smarrimento di un fascicolo cartaceo, furto/smarrimento di un dispositivo aziendale (laptop, USB), accesso abusivo a banca dati (interno o esterno), errore di sistema che espone dati pubblicamente. Procedura obbligatoria (artt. 33-34 GDPR): 1) Rilevazione del breach (chiunque rileva, segnala al DPO/Titolare); 2) Valutazione del rischio per i diritti e libertà degli interessati; 3) Notifica al Garante entro 72 ore se rischio non basso (art. 33); 4) Comunicazione agli interessati se rischio elevato (art. 34); 5) Misure di contenimento e correttive; 6) Registrazione nel registro data breach interno. Per la PL: ogni operatore deve sapere riconoscere e segnalare immediatamente.

Schema operativo del trattamento dati nella PL

Lo schema operativo del trattamento dati personali nella PL può essere riassunto in 9 fasi: 1) identificazione del dato (categoria: personale, particolare, giudiziario); 2) identificazione della base giuridica (obbligo legale, interesse pubblico, consenso, ecc.); 3) identificazione del regime applicabile (GDPR amministrativa o LED per finalità penali); 4) trattamento vero e proprio (verbale, sinistro, video, banche dati); 5) conservazione per il tempo necessario; 6) accesso/comunicazione secondo principi di minimizzazione e con base giuridica; 7) misure di sicurezza (tecniche e organizzative); 8) gestione data breach se accade (artt. 33-34); 9) responsabilità in caso di violazione (triplice). Per la PL: schema cardine da memorizzare per concorso, ricorrente in ogni atto operativo.

Body-cam: condizioni di legittimità

Le body-cam (telecamere indossate dagli operatori PL) sono strumenti utili per documentare interventi, ma il loro utilizzo è delicato: trattano dati personali (immagini, voce di cittadini) e particolari (eventuali condizioni sanitarie visibili). Sono utilizzabili solo se previste da adeguata base normativa/regolamentare interna, con: DPIA (valutazione impatto privacy), informativa ai cittadini coinvolti (cartelli + segnalazione vocale all'attivazione), limiti chiari di attivazione (eventi specifici, no riprese continue), istruzioni operative scritte ai designati. NO uso ordinario senza base regolamentare. Conservazione delle riprese per il tempo strettamente necessario, normalmente breve. Provvedimenti del Garante (es. 2017, 2020 e successivi) hanno fornito linee guida specifiche. Per la PL: strumento valido se gestito correttamente.

Dati sanitari nei procedimenti della PL

I dati sanitari sono dati particolari ex art. 9 GDPR — il loro trattamento è di norma vietato, salvo specifiche deroghe. Per la PL si presentano in: sinistri stradali con feriti (referti, condizioni cliniche), TSO (Trattamento Sanitario Obbligatorio), interventi su soggetti vulnerabili (anziani, disabili, persone in stato di alterazione), vittime di reati (lesioni, violenze), identificazione di persone con problematiche sanitarie evidenti. Base giuridica ex art. 9 par. 2: tipicamente interesse pubblico rilevante (lett. g), obbligo legale rilevante (lett. b), finalità di sanità (lett. h), vitali interessi (lett. c). Cautele estreme: minimizzazione assoluta, cifratura, accesso limitatissimo, comunicazione solo a soggetti autorizzati con base specifica, no diffusione mai. Comunicazione a compagnia assicurativa: solo con consenso o base normativa specifica.

Privacy negli atti di PG (regime LED)

Gli atti di Polizia Giudiziaria sono soggetti al regime privacy del D.Lgs. 51/2018 (LED — recepimento Direttiva 2016/680/UE), distinto dal GDPR. Atti tipici PL ricompresi: CNR (Comunicazione Notizia di Reato, art. 347 c.p.p.), identificazione (art. 349 c.p.p.), sommarie informazioni (artt. 350-351), sequestri probatori (art. 354 c.p.p.), fermi e arresti. Caratteristiche LED: base giuridica = norma di legge (no consenso); diritti dell'interessato modulati (artt. 8-10 D.Lgs. 51/2018, possibili

Mappa concettuale

Privacy e GDPR · argomenti e lezioni collegate

Privacy e GDPR

Lezioni principali

Diritti dell'interessato (artt. 15-22 GDPR)

Il GDPR riconosce all'interessato otto diritti fondamentali. Una PA che tratta dati deve garantirne l'esercizio con tempi rapidi e modalità chiare.

I principi del GDPR applicati alla PL

Liceità, finalità, minimizzazione, accountability. Come operare nel rispetto del Regolamento UE 2016/679.

DPO e DPIA: ruoli e strumenti del GDPR

Il GDPR impone la nomina di un Data Protection Officer in molte PA e la Valutazione d'Impatto (DPIA) per trattamenti ad alto rischio. Ruoli chiave per la compliance.

Videosorveglianza pubblica (GDPR + Garante)

La videosorveglianza pubblica è disciplinata da: GDPR (Reg. UE 2016/679) + Codice Privacy (D.Lgs. 196/2003 modif. D.Lgs. 101/2018) + Provvedimenti Garante (in particolare 8/4/2010 e successivi aggiornamenti) + L. 38/2009 e D.L. 14/2017 (sicurezza urbana). Requisiti: finalità specifica (sicurezza, traffico, decoro), DPIA (valutazione impatto privacy ex art. 35 GDPR), cartelli informativi ben visibili, conservazione delle immagini per il tempo strettamente necessario, normalmente breve, con durata motivata in base alla finalità e al rischio, accesso ai filmati solo personale autorizzato (PL, AG su richiesta). Privacy by design: zone sensibili oscurate (interno abitazioni, ingressi privati). Per la PL: gestione operativa centrali, accesso filmati per indagini PG, comunicazione AG, rispetto rigoroso normativa privacy. Sanzioni Garante elevate per violazioni.

Trasferimento dati fuori dall'UE

Il GDPR consente il trasferimento di dati personali fuori dall'UE solo se il Paese di destinazione garantisce un livello di protezione adeguato. Cloud USA, schemi Privacy Framework e clausole contrattuali.

Fondamenti del GDPR

GDPR (Reg. UE 2016/679) — struttura e applicazione

Il GDPR (Regolamento UE 2016/679) è la norma europea sulla protezione dei dati personali. In vigore dal 25 maggio 2018. Direttamente applicabile in tutti gli Stati UE. 99 articoli + 173 considerando. Principio: tutela diritti fondamentali. In Italia integrato dal Codice privacy novellato (D.lgs. 196/2003 modificato da D.lgs. 101/2018).

Definizioni chiave del GDPR (art. 4)

L'art. 4 GDPR definisce i concetti fondamentali: dato personale, trattamento, interessato, titolare, responsabile, consenso, data breach. Comprensione di queste definizioni è essenziale per l'applicazione corretta del Regolamento.

Basi giuridiche del trattamento (art. 6 GDPR)

L'art. 6 GDPR elenca 6 basi giuridiche alternative per il trattamento di dati personali: a) consenso, b) esecuzione contratto, c) obbligo legale, d) vitali interessi, e) interesse pubblico/esercizio pubblici poteri, f) interesse legittimo. Per la PA italiana: le basi più rilevanti sono lett. c (obbligo legale) e lett. e (interesse pubblico/esercizio pubblici poteri) — il consenso è raramente utilizzato dalla PA (lett. a) e l'interesse legittimo non si applica (lett. f). Tipicamente la PL si basa su norme di legge specifiche (CdS, D.Lgs. 114/1998, TUA, ecc.) che fissano obblighi legali o funzioni pubbliche. Per categorie particolari (art. 9): deroghe specifiche, tipicamente lett. g (interesse pubblico rilevante) e lett. b (obbligo legale rilevante).

Consenso al trattamento (art. 7 GDPR)

Il consenso (art. 7 GDPR) deve essere libero, specifico, informato e inequivocabile. Dimostrabile dal titolare. Revocabile in qualsiasi momento (senza pregiudicare trattamenti pregressi). Non valido se pre-selezionato, da condizioni inique, imposto. Requisiti stringenti per dati particolari (consenso esplicito).

Informativa privacy (artt. 13-14 GDPR)

L'informativa (artt. 13-14 GDPR) è obbligatoria: prima della raccolta (art. 13) o al momento della raccolta indiretta (art. 14). Deve essere concisa, trasparente, intelligibile, accessibile, scritta. Contenuti obbligatori: identità titolare, DPO, finalità, base giuridica, destinatari, tempi, diritti. Omissione = sanzione.

Privacy by design e by default (art. 25 GDPR)

L'art. 25 GDPR impone privacy by design (protezione fin dalla progettazione) e by default (impostazioni predefinite più restrittive). Il titolare implementa misure tecniche e organizzative adeguate. Pseudonimizzazione, minimizzazione, trasparenza. Certificazioni (art. 42) possono aiutare.

Registro delle attività di trattamento (art. 30)

L'art. 30 GDPR impone ai titolari di tenere un registro delle attività di trattamento. Obbligatorio per PA (sempre), imprese 250 dipendenti, o trattamenti a rischio. Contenuti: finalità, categorie interessati e dati, destinatari, trasferimenti extra-UE, tempi conservazione, misure sicurezza. Strumento di accountability.

Misure di sicurezza (art. 32 GDPR)

L'art. 32 GDPR impone misure tecniche e organizzative adeguate al rischio per la sicurezza dei dati personali. Pseudonimizzazione, crittografia, capacità ripristino, test periodici. Misure proporzionate al rischio. Responsabile esterno deve garantire stesse misure. Valutazione continua.

Data breach — notifica (artt. 33-34 GDPR)

L'art. 33 GDPR impone la notifica al Garante entro 72 ore da quando si è venuti a conoscenza della violazione di dati personali. Se alto rischio, anche comunicazione agli interessati (art. 34). Documentazione obbligatoria di tutte le violazioni. Sanzioni severe per omessa notifica.

DPIA — Valutazione Impatto (art. 35)

La DPIA (Data Protection Impact Assessment, art. 35 GDPR) è la valutazione d'impatto sulla protezione dati. Obbligatoria per trattamenti ad alto rischio: profilazione sistematica, dati particolari su larga scala, monitoraggio sistematico. Contenuto: descrizione, necessità, rischi, misure. Prima del trattamento. Consultazione Garante se rischio non mitigato.

Soggetti e responsabilità GDPR

Titolare del trattamento — ruolo e obblighi

Il titolare del trattamento (art. 4 n. 7 GDPR) è chi determina finalità e mezzi del trattamento. Responsabile primario della compliance. Obblighi: informativa, registro, misure sicurezza, DPIA, DPO (se obbligato), gestione diritti interessati, data breach. Sanzioni elevate. Persona fisica/giuridica.

Responsabile del trattamento (art. 28)

Il responsabile del trattamento (art. 28 GDPR) tratta dati per conto del titolare. Relazione regolata da contratto scritto obbligatorio. Contenuto: oggetto, durata, natura, finalità, tipi dati, obblighi, misure sicurezza. Sub-responsabili solo con autorizzazione. Responsabilità solidale con titolare in caso di violazioni.

DPO — Data Protection Officer (artt. 37-39)

Il DPO (Responsabile Protezione Dati, artt. 37-39 GDPR) è figura obbligatoria per: PA, trattamenti che richiedono monitoraggio sistematico su larga scala, dati particolari su larga scala. Requisiti: competenze specifiche, indipendenza, risorse. Funzioni: consulenza, sorveglianza, cooperazione con Garante. Non sanzionato personalmente.

Diritti dell'interessato (artt. 15-22 GDPR)

Gli artt. 15-22 GDPR elencano i diritti dell'interessato: art. 15 accesso (sapere quali dati sono trattati e ottenerne copia); art. 16 rettifica; art. 17 cancellazione ("diritto all'oblio"); art. 18 limitazione; art. 19 notifica delle modifiche/cancellazioni; art. 20 portabilità (limitato per PA); art. 21 opposizione; art. 22 no decisioni automatizzate. Tempi di risposta: 30 giorni (estendibili a 60-90 in casi complessi). Limitazioni rilevanti: alcuni diritti possono essere limitati quando il trattamento riguarda indagini, sicurezza pubblica o attività di polizia giudiziaria (D.Lgs. 51/2018 LED + art. 23 GDPR + art. 2-quinquiesdecies Codice Privacy). Per la PL: gestione delle richieste degli interessati con valutazione caso per caso, motivazione delle eventuali limitazioni, coordinamento con DPO.

Garante per la protezione dei dati personali

Il Garante per la protezione dei dati personali è l'autorità amministrativa indipendente che vigila sull'attuazione del GDPR e del Codice Privacy in Italia. È composto da membri eletti dal Parlamento (due dalla Camera, due dal Senato), con mandato di 7 anni non rinnovabile. Funzioni: vigilanza, controllo, provvedimenti correttivi e sanzionatori (anche elevatissimi), pareri su atti normativi, gestione reclami degli interessati, cooperazione UE (con altre autorità di protezione dati). Sede: Roma. Sito: www.garanteprivacy.it. Per la PL: autorità di riferimento per reclami dei cittadini, notifiche data breach (entro 72h), provvedimenti su videosorveglianza, body-cam, fototrappole, banche dati. Sanzioni: pecuniarie elevate (fino 20 mln € o 4% fatturato per casi gravi), applicabili anche alle PA con criteri specifici.

Sanzioni GDPR (art. 83)

Le sanzioni del GDPR (art. 83) sono pecuniarie amministrative di entità significativa. Due fasce: violazioni meno gravi fino a 10 milioni di € o 2% del fatturato (per le imprese); violazioni più gravi fino a 20 milioni di € o 4% del fatturato. Anche le PA possono essere destinatarie di provvedimenti correttivi e sanzioni secondo il GDPR e il Codice Privacy italiano (D.Lgs. 196/2003 modif. D.Lgs. 101/2018). I criteri di applicazione tengono conto di: gravità, durata, natura intenzionale o colposa, dimensione PA, misure adottate, recidiva, cooperazione con il Garante. Sanzioni accessorie: ordini di limitazione/cancellazione, ammonimenti, pubblicazione del provvedimento. Per la PL: rischio sanzionatorio reale per violazioni di videosorveglianza, banche dati, comunicazioni illegittime, conservazione eccessiva. Cooperazione costruttiva con Garante mitiga le sanzioni.

Codice privacy (D.lgs. 196/2003) — novellato

Il D.lgs. 196/2003 (Codice privacy) è stato novellato dal D.lgs. 101/2018 per adattarsi al GDPR. Mantiene norme specifiche italiane: sanzioni penali (artt. 167 ss.), PA (art. 166), settore sanitario, lavoro, minori, giornalismo. Complementa GDPR (direttamente applicabile) con specifiche nazionali.

Trasferimenti di dati extra-UE (artt. 44-50)

Il trasferimento di dati personali fuori dall'UE è disciplinato dagli artt. 44-50 GDPR: necessita di decisione di adeguatezza della Commissione UE (paesi con livello adeguato di protezione), oppure di garanzie adeguate (clausole contrattuali standard CCS, BCR — Binding Corporate Rules), oppure di deroghe specifiche (consenso esplicito, vitali interessi, ecc.). Sentenza Schrems II (CGUE 2020): ha invalidato il Privacy Shield USA-UE, imponendo verifiche ulteriori per trasferimenti USA. Per la Polizia Locale: argomento avanzato non centrale per concorso PL; rilevante in pratica solo per scelte sul cloud comunale fuori UE (es. AWS, Google Cloud, Microsoft Azure) — cura del DPO + DPA con clausole contrattuali standard + valutazione Schrems II. Approfondimento secondario rispetto a verbali, banche dati, videosorveglianza, atti PG.

Direttiva LED e Polizia Giudiziaria (D.lgs. 51/2018)

La Direttiva UE 2016/680 (Law Enforcement Directive, LED) disciplina i trattamenti di dati personali da parte delle autorità per prevenzione, indagine, perseguimento reati. Recepita in Italia dal D.lgs. 51/2018. Principi simili a GDPR ma regime specifico per polizia/giustizia. PL con qualifica PG applica LED.

Responsabilità civile e diritto al risarcimento (art. 82 GDPR)

L'art. 82 GDPR riconosce all'interessato il diritto al risarcimento del danno materiale o immateriale subito per violazione del Regolamento. Titolare e responsabile sono responsabili in solido; possono esonerarsi provando di non aver alcuna responsabilità. Competenza del giudice ordinario; azione anche collettiva.

Applicazione pratica e PL

Videosorveglianza e body-cam della Polizia Locale

Le body-cam sono telecamere indossate dagli operatori PL: utilizzabili solo se previste da adeguata base normativa/regolamentare interna, con: DPIA (art. 35 GDPR), informativa ai cittadini coinvolti, limiti chiari di attivazione (eventi specifici, no riprese continue), istruzioni operative scritte ai designati. Provvedimenti del Garante (es. 13/12/2017) hanno fornito linee guida specifiche. La videosorveglianza generale della PL (telecamere fisse nella zona urbana) segue regole simili: regolamento, DPIA, cartelli informativi, conservazione per il tempo strettamente necessario, normalmente breve, motivato. NO uso ordinario di body-cam senza base regolamentare adeguata. Per la PL: strumento valido se gestito correttamente; cooperazione con DPO + sindacati per implementazione conforme.

Controlli sul lavoro e privacy dei dipendenti

I controlli a distanza sui lavoratori sono disciplinati dall'art. 4 L. 300/1970 (Statuto lavoratori) novellato dal D.lgs. 151/2015 (Jobs Act). Impianti audiovisivi e strumenti controllo: solo per esigenze organizzative, produttive, sicurezza, previa accordo sindacale o autorizzazione ITL. Dati utilizzabili a fini disciplinari SOLO con informativa ex art. 13 GDPR. PL datore: segue stesse regole.

Cookie e trattamenti online (siti PA e PL)

I cookie sono regolati dalla Direttiva ePrivacy 2002/58/CE, art. 122 Codice privacy, Linee guida Garante 10 giugno 2021. Distinzione tra tecnici (no consenso), analitici (consenso salvo anonimizzazione), profilazione (consenso esplicito). Banner cookie con parità scelta accetta/rifiuta. Siti PA e PL: obbligo conformità; preferibili solo cookie tecnici.

Marketing, telemarketing e registro opposizioni

Il marketing e il telemarketing sono disciplinati da GDPR + Codice Privacy + Codice Consumo (D.Lgs. 206/2005) + L. 5/2018 (Registro Pubblico Opposizioni — RPO). Competenze primarie: AGCM (Autorità Garante Concorrenza e Mercato per pratiche scorrette), Garante Privacy (per uso illecito dati). Il Registro Pubblico Opposizioni consente ai cittadini di opporsi al telemarketing. Per la Polizia Locale: tema poco utile per concorso e operatività quotidiana — la PL può essere coinvolta solo per pubblicità abusiva locale (volantini in strada, manifesti senza autorizzazione, insegne illegittime). Argomento di sfondo culturale, non centrale; priorità a verbali, banche dati, videosorveglianza, atti PG.

Privacy nelle scuole e in sanità

La privacy nelle scuole e in sanità è materia ampia. Scuole: dati di minori (tutela rafforzata art. 8 GDPR + art. 2-quinquies Codice Privacy), trattamenti del personale docente, fotografie e video di iniziative scolastiche. Sanità: dati sanitari = particolari art. 9 GDPR, FSE (Fascicolo Sanitario Elettronico), referti, cartelle cliniche, procedure HIPAA-like nazionali. Competenze primarie: dirigenti scolastici, ASL, strutture sanitarie. Per la Polizia Locale: argomento non centrale per concorso; il focus operativo PL è su: minori nei sinistri o procedimenti (oscuramento, identificazione con genitori), TSO (esecuzione ordinanza Sindaco), sinistri con feriti (dati sanitari trattati con cautele), dati sanitari nei procedimenti (referti acquisiti). Argomento ridotto rispetto a verbali, banche dati, videosorveglianza.

Accesso agli atti vs privacy — bilanciamento

Il diritto d'accesso (L. 241/1990), accesso civico (D.lgs. 33/2013), FOIA (D.lgs. 97/2016) possono confliggere con la privacy. Bilanciamento: accesso prevale se interesse concreto e attuale del richiedente; privacy prevale per dati sensibili senza necessità difesa. Linee guida ANAC 2017 e Garante su accesso civico. PL: frequenti richieste su verbali, incidenti, segnalazioni.

Pubblicazioni di trasparenza e limiti privacy

Il D.lgs. 33/2013 prevede pubblicazioni obbligatorie su Amministrazione Trasparente. Limiti: solo dati strettamente necessari (art. 7-bis c. 4); dati personali pseudonimizzati/oscurati quando non indispensabili; vietati dati particolari (salute, vita sessuale) e giudiziari salvo deroghe. Corte Cost. 20/2019 e 84/2022 hanno ridimensionato obblighi per dirigenti.

GDPR e operatività PL — casistica

La PL tratta dati personali in ogni attività: identificazione, verbalizzazione, informazioni al PM, banche dati. Cornice applicabile: GDPR o D.lgs. 51/2018 (LED) a seconda della natura del trattamento. Principi chiave: minimizzazione, accuracy, retention. Sistemi usati: SDI, VERALI, SISTER, banche dati regionali. Accessi tracciati e autorizzati.

GDPR nei rapporti internazionali e cooperazione PL

La cooperazione internazionale di polizia è regolata dalla Convenzione Schengen, SIS II (sistema informativo), Reg. UE 1862/2018, Direttiva LED. Trasferimenti extra-UE per finalità di law enforcement seguono regole speciali. Europol e Interpol con procedure proprie. PL partecipa marginalmente ma riceve richieste via Prefettura/PG nazionale.

Giurisprudenza GDPR — casi paradigmatici

La giurisprudenza in materia GDPR include sentenze rilevanti come: Schrems I (CGUE 2015) che invalidò il Safe Harbor; Schrems II (CGUE 2020) che invalidò il Privacy Shield e impone verifiche per trasferimenti extra-UE; Cassazione italiana su accessi abusivi a banche dati pubbliche da parte di pubblici ufficiali (art. 615-ter c.p. aggravato); provvedimenti del Garante su videosorveglianza, body-cam, app di tracciamento, ecc. Per la Polizia Locale: tema avanzato non prioritario per concorso; conoscenza generale dei principi giurisprudenziali consigliata, ma il focus operativo resta su atti quotidiani (verbali, banche dati, videosorveglianza). Argomento di approfondimento finale, non

sostitutivo delle materie centrali. Aggiornamento continuo necessario.

Privacy PL: basi operative

Dati personali, particolari e giudiziari

Il GDPR distingue tre categorie principali di dati: dati personali (art. 4 n. 1: qualsiasi informazione riguardante persona fisica identificata o identificabile — nome, indirizzo, codice fiscale, targa, immagine); dati particolari ex art. 9 GDPR (origine razziale/etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici, biometrici per identificazione, dati sanitari, vita sessuale); dati relativi a condanne penali e reati ex art. 10 GDPR (dati giudiziari). Trattamento più rigoroso: per particolari serve base giuridica rinforzata + misure di sicurezza specifiche; per giudiziari serve base normativa specifica. Esempi PL: verbale CdS (dati personali); referto sanitario in sinistro (dati particolari sanitari); CNR/atto PG (dati giudiziari); foto ambito identificativo (potenzialmente biometrici).

GDPR vs D.Lgs. 51/2018 (LED): quale si applica alla PL?

La PL svolge attività con due nature diverse, soggette a regimi privacy distinti: il GDPR (Reg. UE 2016/679) si applica all'attività amministrativa (es. verbali CdS, sanzioni amministrative, gestione SCIA, ordinanze, banche dati anagrafiche); il D.Lgs. 51/2018 (recepimento Direttiva LED — Law Enforcement Directive 2016/680/UE) si applica alle finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (es. CNR, atti di PG, sequestri, identificazioni di indiziati). Esempio cardine: lo stesso operatore PL applica GDPR quando redige verbale CdS, LED quando redige CNR per reato. Conseguenze pratiche: basi giuridiche diverse, diritti dell'interessato modulati, conservazione dati con criteri specifici. Per la PL: distinzione fondamentale per concorso e operatività.

Accesso alle banche dati della PL

L'accesso alle banche dati da parte della PL è uno dei trattamenti più sensibili. Principi cardine: accesso solo per finalità di servizio (mai per curiosità o per uso privato); credenziali personali e non cedibili (no condivisione); tracciamento obbligatorio degli accessi (chi, quando, quale dato consultato); principio di necessità e minimizzazione (non consultare oltre il necessario per il caso). Banche dati tipiche: CED interforze SDI (Sistema di Indagine), ANPR (anagrafe nazionale), PRA (Pubblico Registro Automobilistico), MCTC (motorizzazione), casellario giudiziale, anagrafe tributaria (limitato), banca dati Albo Gestori Ambientali. Abuso: responsabilità disciplinare + civile + PENALE (art. 615-ter c.p. accesso abusivo a sistema informatico, fino 3 anni; art. 326 c.p. rivelazione segreto d'ufficio).

Privacy nei verbali della Polizia Locale

I verbali della PL contengono inevitabilmente dati personali — il loro trattamento è soggetto al GDPR (per illeciti amministrativi) o al D.Lgs. 51/2018 (per atti di PG). Dati tipici: trasgressore (nome, cognome, indirizzo, codice fiscale), proprietario veicolo (se distinto), targa, descrizione del fatto, luogo, data/ora, eventuali testimoni. Principio di minimizzazione (art. 5 GDPR): inserire solo i dati necessari alla finalità del verbale; non includere dati eccedenti (es. informazioni sanitarie irrilevanti, opinioni personali, dati di terzi non coinvolti). Notifiche: solo all'interessato e a soggetti normativamente previsti; busta chiusa + PEC per evitare visibilità a terzi. Pubblicazione: i verbali individuali NON si pubblicano salvo casi specifici e con anonimizzazione. Per la PL: cura particolare nella redazione + nelle notifiche.

Privacy nei sinistri stradali

I sinistri stradali comportano un trattamento particolarmente delicato perché coinvolgono spesso dati sanitari (referti, condizioni feriti — dati particolari art. 9 GDPR), dati assicurativi (compagnie, polizze, franchigie), foto/video di persone e veicoli (immagini = dati personali). Verbale di sinistro: redatto dalla PL, contiene tutti questi dati con base giuridica obbligo legale + interesse pubblico. Accesso agli atti (art. 11 CdS + accesso ex L. 241/1990): consentito agli aventi diritto (parti coinvolte, eredi, assicurazioni mandatarie); terzi: solo con motivazione qualificata; dati di altri soggetti sempre oscurati se non strettamente pertinenti. Sinistro con feriti: scatta anche D.Lgs. 51/2018 (LED) per profilo penale (artt. 589, 590-bis c.p.). Eventuale CNR in caso di reato (omicidio/lesioni stradali, fuga, omissione soccorso).

Privacy: tecnologie e comunicazione

Fototrappole ambientali — privacy

Le fototrappole ambientali sono telecamere autonome con sensori di movimento utilizzate dalla PL per il contrasto agli abbandoni di rifiuti, scarichi abusivi, altri illeciti ambientali. Trattano dati personali (immagini di persone, targhe veicoli) → GDPR + D.Lgs. 51/2018 se per finalità penali. Requisiti di legittimità: 1) base regolamentare (regolamento comunale); 2) finalità specifica (ambientale, sicurezza urbana); 3) DPIA (valutazione impatto privacy ex art. 35 GDPR); 4) informativa (cartelli ove previsti, anche generici per zone con fototrappole nascoste); 5) minimizzazione (registrazione solo a movimento, ripresa mirata); 6) conservazione delle immagini per il tempo strettamente necessario, normalmente breve, motivato in base alla finalità; 7) accesso limitato al personale autorizzato. Utilizzo nel verbale: prove se acquisite legittimamente. Per la PL: strumento centrale ma soggetto a cautele.

ZTL, autovelox, varchi elettronici

I sistemi di rilevamento elettronico della PL — autovelox (controllo velocità), ZTL (Zone a Traffico Limitato), varchi elettronici (accesso aree riservate) — trattano massicciamente dati personali: targhe, immagini dei veicoli, eventualmente del conducente. Base giuridica: obbligo legale (CdS, regolamenti comunali) + interesse pubblico. Conservazione: solo per il tempo necessario alla notifica del verbale e all'eventuale procedimento (di norma alcuni mesi/anni a seconda della tipologia, con tempi specifici per Comune); dati di passaggi non sanzionati vanno eliminati prima. Accesso alle foto: solo all'interessato (sanzionato/proprietario veicolo) + autorità competente; oscuramento dei terzi (passeggeri, persone in foto) obbligatorio nelle copie diffuse. Cartelli informativi: obbligatori (omologazione + segnalazione varco/ZTL).

Conservazione dei dati nella PA

La conservazione dei dati personali è uno dei principi cardine del GDPR (art. 5 par. 1 lett. e: "limitazione della conservazione"). Regola generale: i dati devono essere conservati per un tempo non superiore a quello necessario al conseguimento delle finalità per cui sono trattati. Tempi specifici sono spesso fissati da norme di settore (es. 5 anni verbali CdS per riscossione, 10 anni atti contabili, 30 gg di norma per immagini videosorveglianza, prescrizioni per atti di PG). Criteri: necessità, proporzionalità, motivazione del periodo. Documentazione: registro dei trattamenti deve indicare i tempi (art. 30 GDPR). Distruzione: con procedure sicure (no semplice cestino, distruzione documentale + cancellazione digitale certificata). Per la PL: ogni tipologia di dato ha tempo proprio; politiche di conservazione del Comune.

Comunicazione e diffusione dei dati

Il GDPR distingue comunicazione (dare conoscenza a soggetti determinati) da diffusione (dare conoscenza a soggetti indeterminati). Per la PL: la comunicazione tra uffici comunali e con altre amministrazioni (Prefettura per CdS, Motorizzazione, Procura per CNR, assicurazioni in casi specifici) è legittima se ha base giuridica (norma di legge o interesse pubblico) e rispetta principio di minimizzazione. La diffusione online (pubblicazione su siti, social, ecc.) è vietata salvo base normativa specifica (es. Albo Pretorio per atti dovuti, Amministrazione Trasparente con limiti). Differenza chiave: comunicare ≠ pubblicare. Per la PL: cura particolare nelle comunicazioni a soggetti diversi dal Comune, valutazione caso per caso, sempre minimizzazione.

Pubblicazione online di atti comunali

La pubblicazione online di atti comunali segue due binari: Albo Pretorio online (D.Lgs. 267/2000 TUEL + L. 69/2009: pubblicazione legale di atti per dare loro efficacia) e Amministrazione Trasparente (D.Lgs. 33/2013: trasparenza dell'attività amministrativa). Principio: solo i dati necessari alla finalità di pubblicazione; dati eccedenti devono essere oscurati prima della pubblicazione. Da oscurare obbligatoriamente: dati di minori, dati sanitari, dati giudiziari, dati eccedenti rispetto alla finalità di trasparenza. Durata della pubblicazione: limitata da norme specifiche (Albo: di norma 15 gg per atti generali; Trasparenza: variabile per categoria, di norma 5 anni). Provvedimento Garante 15/5/2014 "Linee guida pubbl. online atti PA" + aggiornamenti. Per la PL: cura nella preparazione di atti destinati a pubblicazione.

Privacy: soggetti e responsabilità

Privacy di minori e soggetti vulnerabili

I minori e i soggetti vulnerabili (anziani non autosufficienti, persone con disabilità, vittime di reati gravi) godono di tutela rafforzata nel trattamento dei dati personali. Per i minori: art. 8 GDPR (consenso digitale: 16 anni in UE, 14 anni in Italia); art. 2-quinquies Codice Privacy. Per la PL: incidenti stradali con minori richiedono cautela estrema (oscuramento volti, dati pseudonimizzati nelle copie diffuse); scuole: rapporti con istituti per controlli, manifestazioni, attraversamenti — minimizzazione massima; vittime di reati: tutela rafforzata (artt. 6-9 D.Lgs. 51/2018 LED); TSO: dati sanitari particolari + cautele. Mai pubblicare identificativi di minori in atti diffusi (Albo, social, comunicati). Mai diffondere foto identificabili di vittime fragili senza consenso/base normativa.

Responsabilità del dipendente pubblico in materia privacy

Il dipendente pubblico che viola la normativa privacy può essere soggetto a triplice responsabilità: disciplinare (procedimento ex D.P.R. 3/57 + CCNL: dal richiamo al licenziamento), civile (risarcimento danni ex art. 82 GDPR + eventuale rivalsa dell'amministrazione), PENALE. Reati specifici: art. 615-ter c.p. (accesso abusivo a sistema informatico, fino 5 anni se commesso da PU); art. 326 c.p. (rivelazione e utilizzazione di segreti d'ufficio, fino 3 anni); art. 167 D.Lgs. 196/2003 (trattamento illecito di dati personali per profitto/danno, fino 3 anni); art. 167-bis (comunicazione/diffusione illecita su larga scala). Altri reati possibili: art. 314 (peculato d'uso), art. 323 (abuso d'ufficio), art. 479 (falso ideologico). Per la PL: cautela massima nell'uso di banche dati e nei trattamenti.

Autorizzati al trattamento (designati)

Gli autorizzati al trattamento (in italiano anche "designati", art. 2-quaterdecies Codice Privacy + art. 29 GDPR) sono i dipendenti o collaboratori che operano sotto l'autorità del titolare/responsabile del trattamento e che trattano materialmente i dati personali. Per la PL: tutti gli agenti, ufficiali, dipendenti amministrativi che accedono a verbali, banche dati, archivi. Nomina formale: atto del Comune (Sindaco/dirigente) che li designa, individua le istruzioni operative scritte, l'ambito autorizzato (quali dati, quali finalità), i limiti, la durata. Formazione obbligatoria sulla privacy. Tracciamento degli accessi. Responsabilità: il designato risponde personalmente delle violazioni (disciplinare, civile, penale). Per la PL: ogni operatore deve essere formalmente designato + ricevere istruzioni scritte.

Responsabili esterni del trattamento applicati alla PL

Il responsabile esterno del trattamento (art. 28 GDPR) è il soggetto terzo (di norma un'azienda) che tratta dati personali per conto del titolare (il Comune). Per la PL: numerosi servizi sono affidati a fornitori esterni che diventano responsabili: software house del gestionale verbali, gestori del sistema ZTL, gestori della videosorveglianza, cloud comunale (storage dati), società di stampa e notifica dei verbali, gestori siti web con dati di cittadini. Obblighi: contratto scritto specifico (DPA — Data Processing Agreement) che regoli oggetto, durata, finalità, categorie dati, obblighi del responsabile (sicurezza, riservatezza, sub-responsabili, restituzione/cancellazione a fine contratto, supporto ai diritti dell'interessato, notifica data breach al titolare, audit). Il Comune resta titolare e responsabile delle scelte; il responsabile esterno risponde direttamente per propri inadempimenti.

Informativa privacy nei procedimenti della PL

L'informativa privacy (artt. 13-14 GDPR) è l'atto con cui il titolare comunica all'interessato come tratta i suoi dati. Obbligatoria in tutti i trattamenti, ma con modulazioni per attività di PG (D.Lgs. 51/2018). Per la PL: deve essere predisposta per ogni procedimento — verbali CdS (informativa sintetica nel verbale + estesa online), accesso ZTL (cartelli + estesa online), istanze dei cittadini (al momento della presentazione), segnalazioni/esposti (al ricevimento), videosorveglianza (cartelli e DPIA). Modello consigliato: informativa breve "stratificata" (essenziali su atto/cartello) + informativa completa (online o presso uffici). Contenuto obbligatorio (art. 13): identità titolare, contatti DPO, finalità, base giuridica, destinatari, conservazione, diritti, reclamo Garante, processo decisionale automatizzato.

Privacy: casi pratici e schema operativo PL

Data breach nella PA — casistica pratica

Il data breach (violazione dei dati personali) nella PA si manifesta con casistiche frequenti: invio PEC al destinatario sbagliato (errore battitura), smarrimento di un fascicolo cartaceo, furto/smarrimento di un dispositivo aziendale (laptop, USB), accesso abusivo a banca dati (interno o esterno), errore di sistema che espone dati pubblicamente. Procedura obbligatoria (artt. 33-34 GDPR): 1) Rilevazione del breach (chiunque rileva, segnala al DPO/Titolare); 2) Valutazione del rischio per i diritti e libertà degli interessati; 3) Notifica al Garante entro 72 ore se rischio non basso (art. 33); 4) Comunicazione agli interessati se rischio elevato (art. 34); 5) Misure di contenimento e correttive; 6) Registrazione nel registro data breach interno. Per la PL: ogni operatore deve sapere riconoscere e segnalare immediatamente.

Schema operativo del trattamento dati nella PL

Lo schema operativo del trattamento dati personali nella PL può essere riassunto in 9 fasi: 1) identificazione del dato (categoria: personale, particolare, giudiziario); 2) identificazione della base giuridica (obbligo legale, interesse pubblico, consenso, ecc.); 3) identificazione del regime applicabile (GDPR amministrativa o LED per finalità penali); 4) trattamento vero e proprio (verbale, sinistro, video, banche dati); 5) conservazione per il tempo necessario; 6) accesso/comunicazione secondo principi di minimizzazione e con base giuridica; 7) misure di sicurezza (tecniche e organizzative); 8) gestione data breach se accade (artt. 33-34); 9) responsabilità in caso di violazione (triplice). Per la PL: schema cardine da memorizzare per concorso, ricorrente in ogni atto operativo.

Body-cam: condizioni di legittimità

Le body-cam (telecamere indossate dagli operatori PL) sono strumenti utili per documentare interventi, ma il loro utilizzo è delicato: trattano dati personali (immagini, voce di cittadini) e particolari (eventuali condizioni sanitarie visibili). Sono utilizzabili solo se previste da adeguata base normativa/regolamentare interna, con: DPIA (valutazione impatto privacy), informativa ai cittadini coinvolti (cartelli + segnalazione vocale all'attivazione), limiti chiari di attivazione (eventi specifici, no riprese continue), istruzioni operative scritte ai designati. NO uso ordinario senza base regolamentare. Conservazione delle riprese per il tempo strettamente necessario, normalmente breve. Provvedimenti del Garante (es. 2017, 2020 e successivi) hanno fornito linee guida specifiche. Per la PL: strumento valido se gestito correttamente.

Dati sanitari nei procedimenti della PL

I dati sanitari sono dati particolari ex art. 9 GDPR — il loro trattamento è di norma vietato, salvo specifiche deroghe. Per la PL si presentano in: sinistri stradali con feriti (referti, condizioni cliniche), TSO (Trattamento Sanitario Obbligatorio), interventi su soggetti vulnerabili (anziani, disabili, persone in stato di alterazione), vittime di reati (lesioni, violenze), identificazione di persone con problematiche sanitarie evidenti. Base giuridica ex art. 9 par. 2: tipicamente interesse pubblico rilevante (lett. g), obbligo legale rilevante (lett. b), finalità di sanità (lett. h), vitali interessi (lett. c). Cautele estreme: minimizzazione assoluta, cifratura, accesso limitatissimo, comunicazione solo a soggetti autorizzati con base specifica, no diffusione mai. Comunicazione a compagnia assicurativa: solo con consenso o base normativa specifica.

Privacy negli atti di PG (regime LED)

Gli atti di Polizia Giudiziaria sono soggetti al regime privacy del D.Lgs. 51/2018 (LED — recepimento Direttiva 2016/680/UE), distinto dal GDPR. Atti tipici PL ricompresi: CNR (Comunicazione Notizia di Reato, art. 347 c.p.p.), identificazione (art. 349 c.p.p.), sommarie informazioni (artt. 350-351), sequestri probatori (art. 354 c.p.p.), fermi e arresti. Caratteristiche LED: base giuridica = norma di legge (no consenso); diritti dell'interessato modulati (artt. 8-10 D.Lgs. 51/2018, possibili limitazioni per indagini in corso); conservazione secondo prescrizione del reato; categorie particolari trattate solo se strettamente necessarie + adeguate garanzie; comunicazione primariamente all'AG; divieto di trasferimento extra-UE non autorizzato. Per la PL: distinzione regime fondamentale + cautela rinforzata negli atti PG.