RedigoPASkills

LA PRIVACY NEI CONTRATTI PUBBLICI

Avv. Alessandra Lezzi

RedigoPA Skills

Privacy, appalti, PNRR, PON, formazione

Avv. Alessandra Lezzi

RedigoPA Skills

I nostri Servizi

Incarico DPO

Supporto al RUP

Gestione amministrativa progetti: PNRR, PON, FESR, FSE, PNSD

Formazione del personale

GDPR 2016/679: cos'è ?

GDPR (General Data Protection Regulation) in italiano RGPD (Regolamento Generale sulla Protezione dei Dati):

- È un regolamento attraverso il quale la Commissione Europea ha inteso rafforzare la protezione dei dati personali dei cittadini dell'Unione Europea. Il Regolamento a differenza delle direttive (che sono recepite con norme interne dagli Stati membri) è direttamente applicabile all'interno degli Stati membri.
- Si applica alle **persone fisiche**, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali (***persone giuridiche (C14)? Trattamento personale o domestico senza connessione con un'attività commerciale o professionale (C18)? Dati anonimi (C26)?***)
- **Deve essere rispettato da tutte le aziende pubbliche e private nonché dalle Pubbliche Amministrazioni con sede nell'Unione Europea e dalle aziende con sede fuori UE che elaborano e trattano dati dei cittadini di uno degli Stati membri (p.e. si pensi alle società che offrono beni o servizi agli interessati in uno o più Stati membri dell'Unione** e che effettuano un monitoraggio del comportamento degli interessati attraverso tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali. C.23 e 24 GDPR)
- Si applica a qualsiasi **trattamento automatizzato e non (p.e dati contenuti in un archivio) di dati personali**

Entrata in vigore e applicazione

- Il Regolamento UE 2016/679 è entrato in vigore il 24 maggio 2016
- Ha visto applicazione in via diretta in tutti i paesi UE a partire dal 25 maggio 2018
- Ha abrogato la direttiva privacy EU 95/46
- È stato recepito in Italia con il **D. Lgs. 101/2018** del 10 Agosto che è entrato in vigore il 19 Settembre 2018 adeguando e modificando il D. Lgs. 196/2003 (Codice della Privacy) alle disposizioni del prevalente UE (GDPR).
- Le disposizioni nazionali devono, comunque, essere interpretate ed applicate alla luce di quanto prescritto dal Regolamento Ue 2016/679 in materia di protezione dei dati personali (art. 288 TFUE)

D. LGS. 101/2018 cos'è?

- Art. 13 Legge di delegazione europea 25 ottobre 2017 n.163 per la modifica del Codice privacy
- Ha abrogato numerose disposizioni del D.LGS n. 196/2003 non compatibili con il Regolamento
- Ha introdotto nuove disposizioni all'interno del D.LGS n. 196/2003
- Ha eliminato alcune sanzioni penali: «ne bis in idem» (p.e. Eliminazione del reato di cui all'art. 169 del previgente Codice, "Misure di sicurezza")
- Inasprimento dell'impianto sanzionatorio con **sanzioni amministrative** (sanzioni fino a 10 milioni di euro nel caso di mancata designazione del DPO- sanzioni fino a 20 milioni di euro per inosservanza dei principi base del trattamento), **penali** (p.e. le sanzioni penali prevedono la reclusione fino a sei anni nel caso di comunicazione o diffusione illecita di dati personali oggetto di trattamento su larga scala) **e civili** (risarcimento del danno materiale o immateriale)
- Attribuzione di maggiori poteri all'Autorità di controllo nazionale

D. L. 8 ottobre 2021, n.139

Disposizioni urgenti per l'accesso alle attivita' culturali, sportive e ricreative, nonche' per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.

- Ha introdotto disposizioni in materia di protezione dei dati personali
- All'articolo 2-ter dopo il comma 1, e' inserito il seguente:

"1-bis Il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, *e' anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti.*

La finalita' del trattamento, se non espressamente prevista da una norma di legge o di regolamento, e' indicata dall'amministrazione, in coerenza al compito svolto o al potere esercitato, assicurando adeguata pubblicita' all'identita' del titolare del trattamento, alle finalita' del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.";

Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso ai pubblici poteri

Il **D.L. n. 139/2021,** convertito in legge n. 205/2021, ha introdotto importanti modifiche alla disciplina del D.Lgs. n. 196/2003:

a) Da un lato, ha ampliato la base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: **oltre alla legge e al regolamento, vi è anche l'atto amministrativo generale (art. 2-ter, c. 1)**.

b) dall'altro ha previsto che il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, è anche consentito se **il trattamento è necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti**.**(art. 2-ter, c. 1-bis)**.

Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso ai pubblici poteri

ATTO AMMINISTRATIVO GENERALE:

- Atto amministrativo operante nei confronti di una generalità indeterminata di destinatari e volto a risolvere specifici problemi già disciplinati in astratto dall'ordinamento *(cit. Aldo M. Sandulli)*
- Atto adottato da una pubblica amministrazione in quanto autorità. Si distingue dagli accordi, dalle convenzioni, dai contratti, che la pubblica amministrazione conclude non in posizione di autorità, ma in posizione di sostanziale parità nei confronti dell'amministrato. *(enciclopedia Treccani)*

Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso ai pubblici poteri

ATTO AMMINISTRATIVO GENERALE

In altri termini, l'atto amministrativo generale, a differenza di quello regolamentare, **non pone alcuna disciplina generale e astratta dei rapporti giuridici e non innova l'ordinamento giuridico.**

L'atto amministrativo generale è espressione di una **"potestà amministrativa di natura gestionale"** ed è rivolto alla "cura concreta d'interessi pubblici, seppure a destinatari indeterminati".

Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso ai pubblici poteri

ATTO AMMINISTRATIVO GENERALE

Nell'ordinamento italiano, tipici esempi di atto amministrativo generale sono il **bando di gara** e il **bando di concorso**.

La protezione dei dati personali

- Garantisce la veridicità e affidabilità dei dati utilizzati. Essa rappresenta una condizione indispensabile per garantire la riservatezza, la libertà di autodeterminazione.
- Nasce come risposta alla rapidità dell'evoluzione tecnologica.

Rinunciare alla protezione dei dati personali significa perdere ogni forma di libertà.

Concetto di **dato personale**

- Qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»).
- Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo anagrafico (**nome**), un numero di identificazione **(cod. fiscale),** dati relativi all'ubicazione **(residenza/domicilio**), dato di contatto **(numeri telefonici)** un identificativo online **(mail o pec)** o a uno o più elementi caratteristici della sua identità fisica **(fisionomia),** caratteristiche psichica **(carattere o patologia),** economica, culturale o sociale; (**art. 4, paragrafo 1**)

Categorie di dati personali:

Dati comuni-identificativi:

- di persone fisiche: nome e cognome, indirizzo, residenza anagrafica, numero telefonico, pec, mail, codice fiscale, partita iva ecc. e comunque i dati pubblici in genere.
- di enti (sia pubblici che privati), associazioni e società: sede legale, indirizzo, numero di telefono ecc. NON si dovrebbe applicare il regolamento (C.14 GDPR), però quando si trattano le fatture di persone giuridiche si hanno come riferimento dei dati di contatto di persone fisiche della società/azienda come la mail o tel., quindi si applica il regolamento europeo.

Categorie di dati personali:

Dati particolari:

- **Ex Dati sensibili:** (ART. 9 GDPR)dati che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose/filosofiche, appartenenza sindacale, orientamento sessuale, relativi alla salute..
- **Dati genetici** (C34 GDPR): sono relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica (esami DNA,RNA).
- **Dati biometrici** (C51 GDPR): sono ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dati giudiziari** (ART. 10 GDPR): possono rivelare l'esistenza di determinati provvedimenti giudiziari penali (*ad esempio*, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Dati particolari

Art.9 GDPR.

Divieto di trattamento di dati personali *“che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.”*

Il divieto è derogabile in presenza di una delle condizioni:

- **consenso esplicito**
- trattamenti dati nel rapporto di lavoro (Serv. San. per visite fiscali o organi preposti alla vigilanza igienico-sanitaria)
- trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria
- **trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art 9, paragrafo 1 e paragrafo 2, lett. g) GDPR; art. 2 sexies novellato D.LGS 196/2003)
- dati personali resi manifestamente pubblici dall’interessato
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro ecc.

Trattamento dati: cos’è?

Qualsiasi operazione fatta su un dato o su un insieme di dati personali, compiuta con o senza l'ausilio di processi automatizzati (art. 4 GDPR)

Alcuni esempi di trattamenti:

- Raccolta dati (raccogliere dati dall’interessato)
- Conservazione dei dati (tenuti in archivio)
- Adattamento dei dati (modifica dei dati)
- Raffronto dei dati (confronto dati diversi raccolti da più fonti)
- Messa a disposizione dei dati (metterli a favore di terzi autorizzati)
- Estrazione dei dati (tirar fuori)
- Cancellazione o distruzione dei dati (non più disponibili a terzi)

Principi applicabili al trattamento di dati personali

- **Liceità, correttezza e trasparenza**. In particolare i dati dovranno essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
- **Limitazione della finalità**, ossia per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
- **Minimizzazione dei dati**, ovvero in maniera adeguata, pertinente e limitata a quanto necessario rispetto alle finalità per le quali sono trattati.
- **Esattezza**, e cioè in modo esatto e, se necessario, con i dovuti aggiornamenti; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
- **Limitazione della conservazione**, ossia conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.
- **Integrità e riservatezza.** I dati infine dovranno essere trattati in maniera da garantire, mediante misure tecniche e organizzative adeguate, un'idonea sicurezza, compresa la protezione, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Il nuovo Principio di Responsabilizzazione o di *Accountability*

E’ il cardine del Regolamento e consiste nell’obbligo del Titolare del Trattamento di giustificare il proprio comportamento e quindi di dimostrare il rispetto dei principi di trattamento dei dati attraverso l’adozione di adeguate misure di sicurezza fisiche, tecniche e organizzative .

.

Accountability

- E’ stata tradotta impropriamente come responsabilizzazione
- Responsabilità incondizionata in capo a un soggetto del risultato conseguito da un’organizzazione, sulla base delle proprie capacità, abilità ed etica. Tale responsabilità richiede giudizio e capacità decisionale, e si realizza nei confronti di uno o più portatori di interessi con conseguenze positive (premi) o negative (sanzioni), a seconda che i risultati desiderati siano raggiunti o disattesi. L’accento non è posto sulla responsabilità delle attività svolte per raggiungere un determinato risultato, ma sulla definizione specifica e trasparente dei risultati attesi che formano le aspettative, su cui la responsabilità stessa si basa e sarà valutata. La definizione degli obiettivi costituisce, dunque, un mezzo per assicurare l’accountability (fonte Treccani)

Accountability

- Insieme al concetto di responsabilità presuppone quelli di **trasparenza** e di **compliance**. La prima è intesa come accesso alle informazioni concernenti ogni aspetto dell'organizzazione volto a rendere visibili decisioni, attività e risultati. La seconda si riferisce al rispetto delle norme ed è intesa sia come garanzia della legittimità dell'azione sia come adeguamento dell'azione agli standard stabiliti da leggi, regolamenti, linee guida etiche o codici di condotta.
- Sotto questi aspetti, l'*accountability* può anche essere definita come **l'obbligo di spiegare e giustificare il proprio comportamento.**

Fonte: treccani.it

Il nuovo Principio di Responsabilizzazione o di *Accountability*

Corte dei Conti, sezione giurisdizionale per il Trentino Alto Adige, sentenza n.1 del 9 gennaio 2024

Condanna per danno erariale da violazione della privacy irrogata ad un funzionaria del Comune, avendo quest'ultima posto in essere trattamenti di dati personali dei dipendenti relativa alla navigazione in internet, in assenza dei presupposti e di idonea informativa (sanzione irrogata: 4200 euro)

Privacy by design e by default

Il Titolare quindi dovrà trattare i dati:

- secondo un approccio basato sulla protezione e sul **controllo del dato utilizzato** e che richiede una corretta valutazione dei rischi per i diritti e le libertà degli utenti. (rafforzamento dei diritti del soggetto interessato)
- con una protezione dei dati fin dalla progettazione (**privacy by design**)
- secondo una impostazione predefinita e nella misura necessaria e sufficiente per le finalità previste e per il periodo di conservazione strettamente necessario a tali fini (**privacy by default**)

Privacy by design

Già in fase di progettazione dei sistemi informativi e dei mezzi per il trattamento, devono essere individuate le **misure tecniche e organizzative adeguate** in relazione agli obblighi imposti dal Regolamento e connessi alla tipologia di dati trattati, all'ambito del trattamento, alle finalità e ai rischi del trattamento, alle tipologie di interessati.

Fermo restando il **principio di minimizzazione** *(*Art.5 punto c:*"limitati a quanto necessario rispetto alle finalità per le quali sono trattati"*) tra le misure adeguate e necessarie previste dal Regolamento abbiamo:

- **Pseudonimizzazione**(Art.4, punto5:*"trattamento dei dati personali in modo tale che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive"*).È una misura di sicurezza dei dati personali.
- **Cifratura dei dati** (Riferimento *Considerando 83* del GDPR). È una misura di sicurezza dei dati personali.
- **Anonimizzazione** (Riferimento *Considerando 26* del GDPR). È una tecnica per far perdere ai dati la qualifica di dato personale.

Privacy by design (sistemi informatici)

- Password per tutte le postazioni degli uffici, possibilmente non conservate sotto la tastiera del computer. Le password, di ogni singola postazione, devono essere conservate oltre che dal dipendente, anche dal Referente privacy o Amministratore di sistema (in busta chiusa e custodite con riservatezza). Inoltre, procedere alla modifica delle stesse con una frequenza trimestrale/semestrale. Qualora per esigenze d'ufficio, le credenziali sono cedute ad altri assistenti, diversi da chi è solitamente assegnato a quella postazione, il giorno dopo, chi rientra alla sua postazione lavorativa deve modificare la password, onde evitare un eventuale accesso abusivo a sistema informatico da parte di terzi non autorizzati.
- antivirus aggiornati su tutti i pc;
- gruppo di continuità;
- sistema di backup dei dati (possibilmente in cloud);

Privacy by design (sistemi informatici)

- Dominio windows;
- Reti internet separate fisicamente o logicamente
- Firewall
- Stampanti multifunzione: quando questa dovesse essere allocata in una zona di passaggio e non vigilata fisicamente, per garantire la riservatezza dei documenti, soprattutto quelli contenenti dati particolari, si consiglia di aver un apposito pin e di digitarlo quando di è fisicamente vicino alla stampante, ovviamente, sempre e solo dopo aver lanciata la stampa dalla postazione dell'ufficio, in modo tale da scaricare il documento solo quando si è vicini alla stessa.

Privacy by design (pratiche amm.ve)

- Per garantire una maggiore riservatezza e disciplinare meglio gli accessi agli uffici, sarebbe opportuno anche utilizzare un front office o di predisporlo, se possibile, per garantire un filtro ulteriore ai fini della riservatezza dei dati trattati. Si potrebbe garantire una maggiore riservatezza, delimitando una distanza con una linea segnaletica (es. ufficio postale)

Privacy by design (pratiche amm.ve)

- Il salvataggio di dati, documenti e cartelle deve avvenire su server o in cloud. È opportuno seguire il **principio di clear screen** (“schermo pulito”), evitando di conservare i file sul desktop del PC per assicurare la disponibilità degli stessi in caso di malfunzionamento o compromissione della macchina.
- Evitare di scaricare o salvare file potenzialmente dannosi o di origine incerta sul PC o di aprire e condividere e-mail da mittenti sconosciuti o appartenenti a catene e mail lists.
- Controllare l’indirizzo mail del destinatario prima di procedere alla comunicazione di dati e/o documenti contenenti dati personali e particolari.
- Effettuare il log out dai programmi utilizzati e spegnere correttamente tutte le attrezzature utilizzate (PC, Lim, notebook, tablet, proiettori, ecc.) al termine della sessione di lavoro, non solo per evitare accessi non autorizzati ma anche per garantire il corretto funzionamento delle stesse.

Privacy by design (progettazione strutturale)

- Antifurto e Videosorveglianza;
- Grate alle finestre e alle porte;
- Armadi chiusi a chiave;
- Casseforti e/o armadi blindati;
- Dispositivi antincendio.

Privacy by design (gestione dati)

- Custodire i documenti cartacei e i supporti informatici removibili in scaffali, cassetti e armadi chiusi a chiave e, al termine dell'orario di lavoro, riporre tutti i documenti presenti sulla scrivania in cassetti chiusi a chiave, soprattutto quando la pulizia degli uffici è affidata a ditte esterne.
- Accertarsi, durante i trattamenti, che i documenti contenenti dati personali non siano alla portata di vista di persone non autorizzate
- Si suggerisce inoltre di separare i dati particolari e/o giudiziari, contenuti in supporti informatici e in faldoni, da quelli non particolari e/o giudiziari in partizioni differenti nonché applicare controlli di sicurezza diversi ai dati particolari, ad esempio attraverso codici di anonimizzazione o pseudonimizzazione
- Garantire la sicurezza dei dati attraverso la distruzione di documenti o fotocopie non più utilizzati

Privacy by design (gestione dati)

- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del Reg. Ue 2016/679, utilizzando i moduli appositamente predisposti
- Effettuare le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) in forma riservata.
- Nel trattare i dati dei lavoratori il Titolare deve adottare misure tecniche e organizzative per prevenire la conoscibilità ingiustificata di dati personali dei propri dipendenti da parte di soggetti terzi, al fine di evitare la comunicazione illecita di informazioni personali (ad es., riguardanti informazioni particolarmente delicate come lo stato di salute del lavoratore o l'assunzione di provvedimenti di carattere disciplinare o valutativo)

Privacy by default

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Il principio di *privacy by default* stabilisce che per impostazione predefinita si dovrebbero trattare solo i dati personali nella misura **necessaria** e sufficiente per le **finalità previste** e per il **periodo strettamente necessario** a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

Privacy by default

Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti (**PRINCIPIO DI MINIMIZZAZIONE**□ trattare i dati in maniera adeguata, pertinente e limitata a quanto necessario rispetto alle finalità per le quali sono trattati)

Privacy by default
Ordinanza ingiunzione Garante Privacy

Con l'**Ordinanza ingiunzione n.190 del 13.05.2021,** il Garante ha rilevato lamentata la violazione dei principi di liceità, correttezza e minimizzazione nel trattamento dei dati personali dei dipendenti del Comune X, atteso che **il sistema di registrazione degli accessi ad Internet impiegato dall'Ente consentiva di "controllare, tracciare, filtrare in maniera massiva, costante e indiscriminata** […] **la cronologia dei siti internet visitati e il tempo di navigazione di per ciascun sito"** (cfr. reclamo, p. 6), **nonché la memorizzazione e la conservazione di tali dati associati a ciascun dipendente per un lungo periodo di tempo**. Ciò avrebbe, dunque, reso possibile, inoltrando specifica richiesta all'Ufficio servizi informatici dell'Ente, la verifica sui singoli siti visitati dall'interessato, mediante estrazione di reportistica (cfr. report relativi al reclamante all. n. 4 al reclamo), tradottasi in un "controllo a distanza ingiustamente lesivo della libertà e della dignità […] nonché vietato dall'art. 4 della l. 300 del 1970" .

SANZIONE APPLICATA:euro 84.000,00 (ottantaquattromila), in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice

Privacy by default (videosorveglianza)

- Premesso che il **GDPR non si applica**:

a) **telecamere false** (cioè quelle che non registrano video o immagini) poiché non vengono elaborati dati personali;

b) **video registrazioni ad alta quota** (perché le immagini non possono essere agganciate ad un soggetto preciso);

c) **videocamera a bassa risoluzione**, non in grado di raccogliere alcuna informazione relativa ad una specifica persona fisica (come targhe o informazioni che potrebbero identificare i passanti).

d) **videocamera per fini domestici e personali**. (installazione di videosorveglianza nel proprio giardino, un turista che registra un video per documentare la vacanza rendendolo accessibili ad amici e parenti)

Privacy by default (videosorveglianza)

- L'installazione di sistemi di videosorveglianza nell'edificio deve in ogni caso garantire:
- **"il diritto del lavoratore alla riservatezza"** (art. 4, L. 300/1970)
- Inoltre, è necessario individuare:

a)**le finalità di trattamento**. (tutelare l'edificio e i beni in esso contenuti da atti vandalici. Protezione della proprietà e di altri beni);

b)**la base giuridica del trattamento** (Articolo 6, paragrafo 1, lettera e), GDPR per lo svolgimento delle funzioni istituzionali.

Privacy by default (videosorveglianza)

c) se è necessario e indispensabile il trattamento (**extrema ratio**).

Ad esempio, l'**EDPB**(European Data Protection Board) suggerisce che se la finalità è quella di prevenire i reati connessi alla proprietà, invece di installare un sistema di videosorveglianza, il titolare potrebbe anche adottare misure di sicurezza alternative quali assumere personale di sicurezza.

Il principio di minimizzazione viene garantito anche con l'eliminazione automatica del filmato dopo un certo periodo o rendendolo accessibile solo in caso di incidente.

Privacy by default (videosorveglianza)

Provvedimento in materia di videosorveglianza - 8 aprile 2010

SETTORI SPECIFICI

RAPPORTI DI LAVORO

Nelle attività di sorveglianza occorre rispettare il **divieto di controllo a distanza dell´attività lavorativa**, pertanto è vietata l´installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l´osservanza dei doveri di diligenza stabiliti per il rispetto dell´orario di lavoro e la correttezza nell´esecuzione della prestazione lavorativa **(ad es. orientando la telecamera sul *badge*).**

Vanno poi osservate le **garanzie previste in materia di lavoro** quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell´**art. 4 della l. n. 300/1970**, gli impianti e le apparecchiature,

"*dai quali può derivare anche la possibilità di controllo a distanza dell´attività dei lavoratori, possono essere installati soltanto* ***previo accordo con le rappresentanze sindacali aziendali,*** *oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l´****Ispettorato del lavoro,*** *dettando, ove occorra, le modalità per l´uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).*

Privacy by default (videosorveglianza)

SETTORI SPECIFICI

RAPPORTI DI LAVORO

Tali garanzie vanno osservate sia all´interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, **nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone.** In tali casi le telecamere non devono riprendere in modo stabile la postazione di guida, le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull´attività lavorativa degli addetti.

Privacy by default (videosorveglianza)

SETTORI SPECIFICI

SICUREZZA NEL TRASPORTO PUBBLICO

L'installazione **di sistemi di videosorveglianza sia su mezzi di trasporto pubblici,** sia presso le f**ermate dei predetti mezzi** può avvenire nel rispetto d**elle seguenti garanzie**:

1. la **localizzazione delle telecamere** e le modalità di ripresa devono essere determinate nel rispetto dei richiamati principi di necessità, proporzionalità e finalità (ad es.presso le aree di fermata l´angolo visuale delle apparecchiature di ripresa deve essere strettamente circoscritto all´area di permanenza);
2. occorre **evitare riprese particolareggiate** nei casi in cui le stesse non sono indispensabili in relazione alle finalità perseguite;
3. **informativa agli utenti del servizio di trasporto urbano (semplificata ed estesa)**;

Privacy by default (videosorveglianza)

- Obbligo di fornire un'adeguata **informativa agli interessati in forma semplificata** che dovrà contenere: - **i** dettagli delle finalità del trattamento; - l'identità del Titolare; - l'elencazione dei diritti dell'interessato; - le informazioni sugli impatti del trattamento (ad esempio la base giuridica del trattamento); - l'indicazione del DPO.
- **Obbligo di fornire un'informativa ai sensi dell'art.13** del Regolamento 679/2016 e deve essere esposta all'interno dell'edificio, in prossimità del front office, e pubblicata nella sezione privacy del sito istituzionale.

Privacy by default (videosorveglianza) TEMPI DI CONSERVAZIONE

- La conservazione deve essere limitata a **poche ore o, al massimo, alle ventiquattro ore** successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione **a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell´autorità giudiziaria o di polizia giudiziaria.**
- S**olo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto)** o per la particolare rischiosità dell´attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l´esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, **si ritiene non debba comunque superare la settimana**.
- **Per i comuni e nelle sole ipotesi in cui l´attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana**, alla luce delle recenti disposizioni normative(12), **il termine massimo di durata** della conservazione dei dati è limitato ***"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l´uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"***.
- Deve essere assicurato agli interessati identificabili l´**effettivo esercizio dei propri diritti** in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.

Quali sono gli adempimenti privacy?

I PRINCIPALI ADEMPIMENTI
Informativa

- L'INFORMATIVA: **art. 13 del Regolamento** – **atto unilaterale da pubblicare**. Occorre una prova dell'avvenuta produzione (ad esempio all'interno del bando di gara). Se emergono nuove ipotesi di trattamento è opportuno integrare l'informativa
- IL CONSENSO: Le autorità pubbliche non hanno bisogno di consenso quando il trattamento avviene per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Art. 2-ter del novellato Codice Privacy. In tali casi la base giuridica del trattamento è costituita da una norma di legge, di regolamento o da un atto amministrativo generale.
- La comunicazione tra Titolari che effettuano il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa solo se prevista da una norma di legge, di regolamento o da un atto amministrativo generale (comunicazione e diffusione).

I PRINCIPALI ADEMPIMENTI
Informativa

DICITURA PRIVACY DA INSERIRE NEL BANDO DI GARA

I dati personali di tutti i soggetti coinvolti nella presente procedura saranno trattati nel rispetto del D.Lgs. n. 196/2003 e ss.mm.ii e del Regolamento UE 679/2016. In particolare:

- Soggetto attivo della raccolta e del trattamento dei dati richiesti, anche particolari in quanto a carattere giudiziario, è il _____;

- Le finalità cui sono destinati i dati forniti dai partecipanti alla gara e le modalità del loro trattamento si riferiscono esclusivamente al procedimento instaurato con la presente gara;

- L'Ente potrà comunicare i dati raccolti al proprio personale interno coinvolto nel procedimento ed ad ogni altro soggetto che abbia interesse ai sensi della L- 241/90;
- Il soggetto interessato richiedente potrà esercitare in ogni momento i suoi diritti nei confronti del titolare del trattamento identificabile nell'_____

- Nel sito web dell'Ente è disponibile l'informativa estesa sulle modalità del trattamento dei dati consultabile al seguente indirizzo: _____.

informativa

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento

informativa

Il titolare **DEVE SEMPRE** specificare:

- i **dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer);**
- **le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;**
- **gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;**
- **se trasferisce i dati personali in Paesi terzi** e **attraverso quali strumenti;**
- il **periodo di conservazione** dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto di presentare un reclamo all'autorità di controllo.

informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** dei dati a terzi o all'interessato.

informativa

L'informativa deve essere data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico.**

E' importante richiamare nella documentazione di gara (ad esempio nel capitolato tecnico) l'informativa privacy contenente le modalità di trattamento dei dati personali dell'operatore economico.

Consenso/ autorizzazione

- Di regola le PP.AA. non devono richiedere il consenso per il trattamento dei dati personali in quanto sono le norme che individuano gli ambiti di trattamento *(Vd considerando 43 del REG., Linee Guida sul consenso del Gruppo di Lavoro articolo 29 del 10 aprile 2018).*
- Ciò in quanto il trattamento dei dati da parte delle PP.AA. avviene prevalentemente per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio dei pubblici poteri di cui è investito il Titolare del Trattamento .

Basi giuridiche del trattamento

- E' il presupposto necessario per poter trattare lecitamente i dati

Ai sensi dell'art. 6 del GDPR il trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- **e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;**
- f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Consenso

CONSENSO E PP.AA

Quando **il trattamento si fonda sul consenso dell'interessato**, il Titolare deve sempre essere in grado di dimostrare (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso(Accountability). Il consenso è valido se:

- all'interessato è stata resa **l'informazione sul trattamento dei dati personali** (articoli 13 o 14 del Regolamento);
- è stato espresso dall'interessato **liberamente**, in modo **specifico**, **inequivocabile,** e se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre **revocabile**.

Consenso

(C43) Per assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un **evidente squilibrio tra l'interessato e il titolare del trattamento**, **specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica.**

Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

Consenso

Il Gruppo di lavoro Articolo 29 sottolinea che sia **improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento** in quanto *«quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento.*

Tuttavia, non esclude completamente il consenso quale base giuridica per il trattamento dei dati da parte delle autorità pubbliche che può risultare appropriato in casi specifici.

Consenso

Esempio: Un comune sta pianificando l'esecuzione di lavori di manutenzione stradale. Poiché i lavori possono perturbare il traffico per parecchio tempo, il comune offre ai cittadini la possibilità di iscriversi a una mailing list per ricevere aggiornamenti sull'avanzamento dei lavori e sui ritardi previsti.

Il comune chiarisce che **la partecipazione non è obbligatoria e chiede il consenso a utilizzare gli indirizzi di posta elettronica per questa finalità (esclusiva).**

I cittadini che non acconsentono non perderanno l'accesso ad alcun servizio fondamentale del comune né alcun diritto, di conseguenza possono esprimere o rifiutare liberamente il loro consenso a questo uso dei dati.

Tutte le informazioni sui lavori stradali saranno disponibili anche sul sito web del comune.

Consenso

Esempio: Una troupe cinematografica filmerà una determinata area di un ufficio. Il datore di lavoro chiede a tutti i dipendenti che hanno la scrivania in quella zona il consenso a essere ripresi, in quanto potrebbero apparire sullo sfondo del video. Chi non vuole essere filmato non viene penalizzato in alcun modo e ottiene invece una scrivania altrove nell'edificio per l'intera durata delle riprese.

Consenso

Come evidenziato dal Comitato in diversi pareri, il consenso è valido soltanto se l'interessato è in grado di operare realmente una scelta e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative (ad es. costi aggiuntivi sostanziali) in caso di rifiuto a prestare il consenso

SICUREZZA

Le misure di sicurezza passano da «minime» ad «adeguate»

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell' oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** al rischio.

SICUREZZA

Le misure di sicurezza adeguate al rischio possono includere:

- la **pseudonimizzazione** e la **cifratura** dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Misure di sicurezza: Rischi

distruzione, perdita, modifica, divulgazione non autorizzata, derivanti dall'accesso in modo accidentale o illegale

Provvedimenti del Garante

DATA	ACCADUTO	ELEMENTI VALUTABILI DAL GARANTE AI FINI DEL QUANTUM
13.05.2021	violazione dei principi di liceità, correttezza e minimizzazione nel trattamento dei dati personali dei dipendenti del Comune, atteso che il sistema di registrazione degli accessi ad Internet impiegato dall'Ente consente di "controllare, tracciare, filtrare in maniera massiva, costante e indiscriminata […] la cronologia dei siti internet visitati e il tempo di navigazione di per ciascun sito" (cfr. reclamo, p. 6), nonché la memorizzazione e la conservazione di tali dati associati a ciascun dipendente per un lungo periodo di tempo.	il Comune ha manifestato una particolarmente collaborazione nel corso dell'istruttoria provvedendo ad apportare, già a seguito della prima richiesta di elementi dell'Ufficio, taluni primi correttivi ai trattamenti oggetto di reclamo e ad avviare, in pari tempo, i necessari approfondimenti funzionali alla progressiva adozione anche delle misure tecniche e organizzative che, ancorché non sufficienti ad assicurare la piena conformità dei trattamenti alle disposizioni in materia di protezione dei dati, denotano tuttavia, un particolare impegno nell'attenuare gli effetti negativi del trattamento nei confronti dei dipendenti.
PROVVEDIMENTO		**SANZIONE AMMINISTRATIVA APPLICABILE**
Ordinanza di ingiunzione nei confronti di un COMUNE		ART 162,COMMA 2 BIS Codice Privacy Sanzione amministrativa del pagamento di una somma da euro 10.000,00 (diecimila) a euro 120.000,00 (centoventimila)
VIOLAZIONE		**SANZIONE AMMINISTRATIVA COMMINATA**
artt. 5, 6, 9, 88 e 35 del Regolamento, nonché 113 e 114 del Codice		la somma di euro 84.000,00 (ottantaquattromila) a titolo di sanzione amministrativa pecuniaria ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento e 166, comma 2, del Codice, di pagare

Titolare e Responsabile del Trattamento

Il **«titolare del trattamento»** (controller) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4, punto 7 GDPR)

Il titolare è quindi il soggetto che tratta i dati forniti dall'interessato (che restano di proprietà dell'interessato) per i suoi scopi.

Il Titolare è la Stazione Appaltante nel suo complesso.

Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del RGPD: "liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza."

Titolare del Trattamento

- Il **«titolare del trattamento»** (controller) quindi dovrà trattare i dati nel rispetto dei suindicati principi e mettere in atto misure adeguate ed efficaci allo scopo di **dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure stesse**.
- Per essere **Compliance** il Titolare deve:

a) rispettare i principi del trattamento (art. 5) e della privacy by design e by default

b) avere effettuare, nei casi previsti, la valutazione di impatto e consultazioni preventive

c) adottare le procedure di sicurezza (misure necessarie ed adeguate)

d) effettuare la valutazione dei rischi

e) predisporre il registro dei trattamenti con analisi dei rischi

f) definire le procedure la gestione e notifica dei data breach

g) designare il Data Protection Officer (DPO)

h) Prevedere un sistema di audit

Responsabile del Trattamento

Il **«responsabile del trattamento»** (processor) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto del titolare del trattamento** (art. 4, punto 8; art. 28 GDPR);

Quando e chi nominare Responsabile del Trattamento interno e/o esterno ?

- Ha **accesso a dati personali la cui titolarità spetta alla Stazione appaltante;**
- **Il servizio prestato ha natura continuativa;**
- **Presenza di contratto o altro atto giuridico equivalente.**

Il Responsabile del Trattamento

Il responsabile del trattamento, la cui **nomina dovrà avere forma scritta**, sia quale atto autonomo che con l'inserimento di clausole ad hoc all'interno di un contratto di servizio, dovrà presentare garanzie sufficienti a **mettere in atto misure tecniche e organizzative adeguate** affinché il trattamento affidato garantisca la tutela dei diritti dell'interessato.

Il Responsabile ha **obblighi di trasparenza, di garantire la sicurezza dei dati e di avvisare, assistere e consigliare il titolare**

La responsabilità del Responsabile: art. 82 del Regolamento.

Il responsabile del trattamento risponde per il danno causato dal trattamento quando:

a) non ha adempiuto agli obblighi che il Regolamento prevede per i Responsabili

b) se ha agito in modo difforme o contrario alle istruzione del Titolare.

Sussiste **responsabilità solidale dei Titolare e dei Responsabili** nel caso in i medesimi siano coinvolti nello stesso trattamento e siano responsabili del danno causato dal trattamento.

Il Responsabile del Trattamento

CLAUSOLE DA INSERIRE NEL CONTRATTO:

ART. __ Trattamento dei dati personali

- Ai sensi della normativa in materia di privacy ed, in particolare, ai sensi del Reg. Ue n. 679/2016 (di seguito, anche «GDPR») e del D.lgs n. 196/2003, come modificato dal D. Lgs n. 101 del 10 agosto 2018, contenente disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 e, da ultimo, dal D.L. n. 139/2021 (di seguito, anche «Codice della Privacy»),il Titolare del Trattamento è _____ in persona del legale rappresentante pro-tempore, dott./ssa _____
- Con la sottoscrizione del presente contratto, la Stazione Appaltante (di seguito, anche «Concedente») autorizza l'Operatore economico affidatario (di seguito anche «Concessionario») a trattare i dati personali soltanto nella misura e nei limiti previsti dal presente accordo, nonchè nomina il Concessionario quale «Responsabile del trattamento» ai sensi e per gli effetti dell'art. 28 del GDPR sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, per tutta la durata del Contratto. A tal fine, il Concessionario, accettando l'incarico, dichiara di essere a conoscenza, di rispettare e di essere conforme al Regolamento UE 2016/679, nonché di rispettare tutte, nessuna esclusa, le prescrizioni in materia di protezione e di sicurezza dei dati personali e, in particolare di:
- utilizzare per conto del Titolare i dati personali di cui verrà a conoscenza nel corso dell'esecuzione dello stesso contratto per i soli scopi ivi previsti;

Il Responsabile del Trattamento

CLAUSOLE DA INSERIRE NEL CONTRATTO:

ART. __ Trattamento dei dati personali

- di non comunicare e diffondere a terzi non autorizzati le informazioni e i dati personali trattati;
- vigilare affinché il trattamento dei dati da parte del personale posto alle dirette dipendenze o delle società controllate e/o partecipate avvenga in modo lecito e secondo correttezza; nonché infine di custodire – nel rispetto delle misure di sicurezza individuate dal Regolamento- i dati personali trattati in modo tale da evitare rischi derivanti dalla violazione di tali dati;
- non diffondere i dati personali acquisiti a Paesi Terzi (extra Ue), se non solo nei casi tassativi previsti dagli artt. 45 e ss del GDPR, in merito al Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali
- adottare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure («privacy by design»), nonché adottare misure tecniche e organizzative adeguate a garantire che i dati personali siano trattati in conformità al principio di necessità, ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse («privacy by default»).
-

Il "Titolare" del trattamento,inoltre, in conformità all'articolo 13 del GDPR, Le comunica che tutte le informazioni estese sulle finalità di trattamento dei Suoi dati, sulle modalità di trattamento, sulla obbligatorietà o meno del consenso, sul periodo di conservazione, sulla comunicazioni e diffusione dei suoi dati personali, nonché sui diritti dell'interessato sono contenute nell'informativa redatta in formato elettronico e pubblicata sul sito istituzionale _____, nella sezione Privacy, consultabile al seguente link: _____

Autorizzati al Trattamento
(ex incaricati del trattamento)

- Il Titolare del trattamento è tenuto ai sensi dell'**articolo 29 del GDPR** 2016/679 ad istruire e formare adeguatamente il personale autorizzato al trattamento dei dati. (**obbligo di formazione per il Titolare**) Art. 4, n.10 GDPR
- L'art. 2- quaterdecies, comma 2, del novellato D.LGS 196/2003 dispone che siano il Titolare o il Responsabile ad individuare le ***"modalità più opportune per autorizzare le persone che operano sotto la propria autorità diretta".***

Organigramma Privacy

- L’organigramma privacy è un modello organizzativo che ha la funzione di assicurare un adeguato ordinamento e classificazione dei dati personali e un corretto utilizzo delle informazioni e dei dati
- La definizione dei ruoli, delle responsabilità e dei settori di competenza di ciascun soggetto dell’organizzazione costituiscono elementi imprescindibili di un sistema di gestione dei dati

RPD /DPO

La nomina del responsabile della protezione dati (RPD) o Data Protection Officer (DPO) è una delle vere novità del regolamento e va comunicata al Garante (invio telematico)

La funzione del RDP è quella di **vigilare** in via generale sui trattamenti posti in essere dal titolare

l DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la protezione dei dati nonché sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento;

La responsabilità principale del DPO è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e la loro protezione) all'interno dell'Ente, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

RPD /DPO

L'articolo 39 del Regolamento specifica nel dettaglio quali sono i compiti minimi del DPO:

- informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento o dalle altre disposizioni legislative interne o europee in materia di protezione dati;
- sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento
- fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo fungendo da punto di contatto per questioni connesse al trattamento, effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

RPD /DPO

- **Conoscenza specialistica** della normativa e delle prassi,
- capacità di essere **coinvolto in modo tempestivo e adeguato**,
- capacità di **lavorare in autonomia** senza ricevere istruzioni, in grado di **riferire direttamente al vertice gerarchico**, di **interloquire con gli interessati**, di **informare e fornire consulenza** al titolare o al responsabile nonché ai dipendenti,
- Capacità di **sorvegliare l'osservanza** del presente regolamento, nonché delle politiche interne, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale,
- Capacità di **fornire un parere in merito alla valutazione d'impatto e sorvegliarne lo svolgimento**, di **cooperare e fungere da punto di contatto con l'autorità di controllo**.

RPD /DPO

I dati di contatto del DPO devono essere comunicati, da parte del titolare o del responsabile, all'autorità di controllo competente

Il registro dei trattamenti deve contenere il nome e i contatti del responsabile della protezione dei dati personali

L'informativa privacy deve riportare i riferimenti del DPO (trasparenza e accountability)

Privacy o trasparenza?

Necessità di coordinare la disciplina in materia di protezione dei dati personali (REG. UE 2016/679; novellato D.LGS 196/2003) con quella di trasparenza amministrativa (D.LGS 33/2013, L. 241/1990).

Privacy o trasparenza?

- **Con l'adozione di apposite Linee guida (provvedimento del 15 maggio 2014), il Garante è intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul web di atti e documenti.**
- **Le linee guida hanno lo scopo di individuare le cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa.**

Privacy o trasparenza?

- Per finalità di trasparenza vanno pubblicati gli atti e documenti per i quali è previsto un **obbligo di pubblicazione.**
- Laddove l'Amministrazione riscontri l'esistenza di un **obbligo normativo** che impone la pubblicazione dell'atto o del documento nel proprio sito web istituzionale è necessario **selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni.**

Privacy o trasparenza?

PRINCIPIO DI NECESSITA' E DI MINIMIZZAZIONE

- I dati devono essere adeguati, limitati e pertinenti a quanto necessario rispetto alle finalità per le quali sono trattati.
- Pertanto, anche in presenza degli obblighi di pubblicazione di atti o documenti contenuti nel d. lgs. n. 33/2013, i soggetti chiamati a darvi attuazione **devono rendere non intelligibili i dati personali non pertinenti o, se sensibili e non giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione (art. 7 bis, comma 4, D.Lgs 33/2013)**

Privacy o trasparenza?

Di conseguenza, i dati personali che esulano dalle finalità di pertinenza - non eccedenza non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione online.

In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti.

sottrarre all´indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari..

FAQ su Trasparenza online della P.A. e privacy del GPDP

Privacy o trasparenza?

QUALI SONO GLI ATTI CHE NON VANNO PUBBLICATI ONLINE?

È vietato diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l´esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici. Il Garante ha più volte ribadito la necessità di garantire il rispetto della dignità delle persone, facendo oscurare, ad esempio, dai siti web di diversi Comuni italiani i dati personali contenuti nelle ordinanze con le quali i sindaci disponevano il trattamento sanitario obbligatorio per determinati cittadini ***(FAQ GARANTE PRIVACY Trasparenza online della P.A. e privacy)***

Privacy o trasparenza?

Diritti complementari e non speculari

*"**il diritto alla protezione dei dati personali** non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va **contemperato con gli altri diritti fondamentali in ossequio al principio di proporzionalità**" (C.4 GDPR)*

"l'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali, contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico, dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti", il quale deve ***"conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali" (C. 154 GDPR)***

Fonti

- **D.Lgs 33/2013** come modificato dal D.Lgs 97/2016, c.d. Decreto Trasparenza (**art. 37 del D.Lgs 36/2023**)
- **L. n.190/2012,** c.d. Legge anticorruzione
- **Linee guida AGID** sulla pubblicità legale dei documenti e sulla conservazione dei siti web delle PA del maggio 2016
- **PNA 2022 Delibera Anac n. 7 del 17 gennaio 2023 e, in particolare, la parte relativa alla "Trasparenza in materia dei contratti pubblici"** (allegato 9 Obblighi di trasparenza contratti)
- **Delibera n. 261 del 20 giugno 2023** - Provvedimento Art 23 - BDNCP
- **Delibera n. 264 del 20 giugno 2023 (come modificata e integrata con delibera n. 601 del 19 dicembre 2023)e Allegato I-** *Individuazione delle informazioni e dei dati relativi alla programmazione di lavori, servizi e forniture*
- **Delibera n. 582 del 13.12.2023 - Adozione comunicato relativo avvio processo di digitalizzazione**
- **Comunicato Anac del 10 gennaio 2024-** Indicazioni di carattere transitorio per l'acquisizione del CIG di importo inferiore a 5.000 euro
- **Avviso ANAC del 5 gennaio 2024,** Adempimenti Legge 190/2012 art. 1, comma 32
- **REG. UE 2016/679 e D.Lgs 196/2003 e ss.mm.ii**

OBBLIGHI DI PUBBLICAZIONE DEI CONTRATTI PUBBLICI DI LAVORI, SERVIZI E FORNITURE

L'art. 37 del D.Lgs 33/2013 (c.d. Decreto Trasparenza), come sostituito dall'articolo 224, comma 4 del codice, prevede che

a) *"Fermo restando quanto previsto dall'articolo 9-bis e fermi restando gli obblighi di pubblicità legale,* ***le pubbliche amministrazioni e le stazioni appaltanti/gli enti concedenti pubblicano i dati, gli atti e le informazioni secondo quanto previsto dall'articolo 28 del codice dei contratti pubblici****"*

b) ai sensi dell'articolo 9-bis, **gli obblighi di pubblicazione di cui al comma 1 si intendono assolti attraverso l'invio dei medesimi dati alla BDNCP presso l'ANAC e alla banca dati delle amministrazioni pubbliche** ai sensi dell'articolo 2 del decreto legislativo 29 dicembre 2011, n. 229, **limitatamente alla parte lavori**

PRINCIPI IN MATERIA DI TRASPARENZA

Art. 20 del D.Lgs 36/2023 (Codice Contratti pubblici)

*"**Fermi restando gli obblighi di pubblicità legale, a fini di trasparenza i dati, le informazioni e gli atti relativi ai contratti pubblici sono indicati nell'articolo 28 e sono pubblicati secondo quanto stabilito dal decreto legislativo 14 marzo 2013, n. 33. 2.** Le comunicazioni e l'interscambio di dati per le finalità di conoscenza e di trasparenza avvengono nel rispetto del **principio di unicità del luogo di pubblicazione e dell'invio delle informazioni**".*

TRASPARENZA DEI CONTRATTI PUBBLICI

Art. 28 del D.Lgs 36/2023 (Codice Contratti pubblici)

1. **Le informazioni e i dati relativi alla programmazione di lavori, servizi e forniture, nonché alle procedure del ciclo di vita dei contratti pubblici, ove non considerati riservati ai sensi dell'articolo 35 ovvero secretati ai sensi dell'articolo 139, sono trasmessi tempestivamente alla Banca dati nazionale dei contratti pubblici attraverso le piattaforme digitali di cui all'articolo 25.**

2. **Le stazioni appaltanti e gli enti concedenti assicurano il collegamento tra la sezione «Amministrazione trasparente» del sito istituzionale e la Banca dati nazionale dei contratti pubblici**, secondo le disposizioni di cui al decreto legislativo 14 marzo 2013, n. 33. **Sono pubblicati nella predetta sezione di cui al primo periodo la composizione della commissione giudicatrice e i curricula dei suoi componenti, nonché i resoconti della gestione finanziaria dei contratti al termine della loro esecuzione.**

3. Per la trasparenza dei contratti pubblici fanno fede i dati trasmessi alla Banca dati nazionale dei contratti pubblici presso l'ANAC, la quale assicura la tempestiva pubblicazione sul proprio portale dei dati ricevuti, anche attraverso la piattaforma unica della trasparenza, e la periodica pubblicazione degli stessi in formato aperto. **In particolare, sono pubblicati la struttura proponente, l'oggetto del bando, l'elenco degli operatori invitati a presentare offerte, l'aggiudicatario, l'importo di aggiudicazione, i tempi di completamento dei lavori, servizi o forniture e l'importo delle somme liquidate**.

4. L'ANAC, entro sessanta giorni dalla data di entrata in vigore del codice, individua con proprio provvedimento le informazioni, i dati e le relative modalità di trasmissione per l'attuazione del presente articolo.

ART. 28 TRASPARENZA DEI CONTRATTI PUBBLICI

La **trasparenza dei contratti pubblici** viene assicurata mediante la **trasmissione tempestiva** delle informazioni e dei dati relativi alla programmazione di lavori, servizi e forniture, nonché alle procedure del ciclo di vita dei contratti pubblici, **ove non considerati riservati ai sensi dell'articolo 35 ovvero secretati ai sensi dell'articolo 139, alla Banca dati nazionale dei contratti pubblici attraverso le piattaforme digitali di cui all'articolo 25.**

ART. 28 TRASPARENZA DEI CONTRATTI PUBBLICI

Quali sono le Informazioni che le stazioni appaltanti e gli enti concedenti sono tenuti a trasmettere alla BDNCP tramite le piattaforme di approvvigionamento ? ***(vd DELIBERA ANAC N. 261 del 20 giugno 2023)***

FASE DI PROGRAMMAZIONE

a) Il programma triennale ed elenchi annuali dei lavori;
b) **Il programma triennale degli acquisti di servizi e forniture** da pubblicare mediante la piattaforma Servizio Contratti Pubblici (SCP) del MIT in quanto inclusa nell'ambito dell'ecosistema di approvvigionamento digitale di cui all'articolo 22 del Codice Appalti ***(VD Delibera ANAC 582 del 13.12.2023, articolo 223, comma 10 del Codice)***

FASE DI PROGETTAZIONE e PUBBLICAZIONE

a) gli avvisi di pre-informazione
b) i bandi e gli avvisi di gara
c) avvisi relativi alla costituzione di elenchi di operatori economici

ART. 28 TRASPARENZA DEI CONTRATTI PUBBLICI

Quali sono le Informazioni che le stazioni appaltanti e gli enti concedenti sono tenuti a trasmettere alla BDNCP tramite le piattaforme di approvvigionamento ? ***(vd DELIBERA ANAC N. 261 del 20 giugno 2023)***

FASE DI AFFIDAMENTO

a) gli avvisi di aggiudicazione ovvero i dati di aggiudicazione per gli affidamenti non soggetti a pubblicità
b) **gli affidamenti diretti**

ART. 28 TRASPARENZA DEI CONTRATTI PUBBLICI

Quali sono le Informazioni che le stazioni appaltanti e gli enti concedenti sono tenuti a trasmettere alla BDNCP tramite le piattaforme di approvvigionamento ? ***(vd DELIBERA ANAC N. 261 del 20 giugno 2023)***

FASE DI ESECUZIONE

a) **La stipula e l'avvio del contratto**
b) **gli stati di avanzamento**
c) i subappalti
d) **le modifiche contrattuali e le proroghe**
e) le sospensioni dell'esecuzione
f) gli accordi bonari
g) le istanze di recesso
h) **la conclusione del contratto**
i) **il collaudo finale**

ART. 28 TRASPARENZA DEI CONTRATTI PUBBLICI

Quali sono le Informazioni che le stazioni appaltanti e gli enti concedenti sono tenuti a trasmettere alla BDNCP tramite le piattaforme di approvvigionamento ? ***(vd DELIBERA ANAC N. 261 del 20 giugno 2023)***

Ogni altra informazione che dovesse rendersi utile per l'assolvimento dei compiti assegnati all'ANAC dal codice e da successive modifiche e integrazioni

PUBBLICAZIONE DATI AI FINI DELLA TRASPARENZA

DELIBERA ANAC N. 264 del 30 giugno 2023

Quali sono le gli atti, le informazioni e i dati relativi al ciclo di vita dei contratti pubblici oggetto di trasparenza ?

Al fine di assolvere gli obblighi di pubblicazione in materia di contratti pubblici di cui all'articolo 37 del decreto trasparenza, le stazioni appaltanti e gli enti concedenti comunicano tempestivamente alla BDNCP tutti i dati e le informazioni, individuati nell'articolo 10 del provvedimento di cui all'articolo 23 del codice (*VD DELIBERA ANAC 261/2023)*

Ai fini della trasparenza fanno fede i dati trasmessi alla BDNCP per il tramite della PCP.

Le stazioni appaltanti e gli enti concedenti inseriscono sul sito istituzionale, nella sezione "Amministrazione trasparente", un collegamento ipertestuale che rinvia ai dati relativi all'intero ciclo di vita del contratto contenuti nella BDNCP secondo le regole tecniche di cui al provvedimento adottato da ANAC ai sensi dell'articolo 23 del codice.

Le specifiche tecniche dei servizi di interoperabilità e i tracciati di trasmissione delle informazioni di cui al punto 10.1 sono pubblicati sul portale Developers Italia https://developers.italia.it/ nella sezione dedicata alla PCP e raggiungibili attraverso il portale internet dell'ANAC;

PUBBLICAZIONE DATI AI FINI DELLA TRASPARENZA

DELIBERA ANAC N. 264 del 30 giugno 2023

Quali sono le gli atti, le informazioni e i dati relativi al ciclo di vita dei contratti pubblici oggetto di trasparenza ?

Le stazioni appaltanti e gli enti concedenti pubblicano nella sezione "Amministrazione Trasparente" del proprio sito istituzionale gli atti, i dati e le informazioni che non devono essere comunicati alla BDNCP e che sono oggetto di pubblicazione obbligatoria come individuati nell'Allegato 1) al presente provvedimento.

PUBBLICAZIONE DATI AI FINI DELLA TRASPARENZA

ALLEGATO 1 della DELIBERA ANAC N. 264 del 30 giugno 2023

Quali sono le gli atti, le informazioni e i dati relativi al ciclo di vita dei contratti pubblici oggetto di trasparenza ?

Art. 82, d.lgs. 36/2023
Documenti di gara

Documenti di gara. Che comprendono, almeno:
Delibera a contrarre
Bando/avviso di gara/lettera di invito
Disciplinare di gara
Capitolato speciale
Condizioni contrattuali proposte
Aggiornamento: TEMPESTIVO

Art. 85, co. 4, d.lgs. 36/2023

Pubblicazione a livello nazionale (cfr. anche l'Allegato II.7)

PUBBLICAZIONE DATI AI FINI DELLA TRASPARENZA

ALLEGATO 1 della DELIBERA ANAC N. 264 del 30 giugno 2023

Quali sono le gli atti, le informazioni e i dati relativi al ciclo di vita dei contratti pubblici oggetto di trasparenza ?

Art. 28, d.lgs. 36/2023

Trasparenza dei contratti pubblici

Composizione delle commissioni giudicatrici e CV dei componenti

N.B. ATTENZIONE AI DATI PRESENTI NEL CVE!

PUBBLICAZIONE DATI AI FINI DELLA TRASPARENZA

DELIBERA ANAC N. 264 del 30 giugno 2023 adottata in attuazione di quanto previsto dall'art. 28,comma 4 del D.Lgs 36/2023.

Durata della pubblicazione

I dati, gli atti e le informazioni oggetto di pubblicazione ai sensi del decreto trasparenza rimangono pubblicati in BDNCP e nella sezione "Amministrazione trasparente" della stazione appaltante e dell'ente concedente per un periodo almeno di cinque anni e, comunque, nel rispetto delle previsioni dell'articolo 8, comma 3, del decreto trasparenza.

PUBBLICAZIONE DATI AI FINI DELLA TRASPARENZA

DELIBERA ANAC N. 264 del 30 giugno 2023 adottata in attuazione di quanto previsto dall'art. 28,comma 4 del D.Lgs 36/2023.

Accesso civico semplice

In caso di mancata pubblicazione dei dati, atti e informazioni nella BDNCP o in "Amministrazione Trasparente" della stazione appaltante e dell'ente concedente si applica la disciplina sull'accesso civico semplice di cui all'articolo 5, comma 1, decreto trasparenza

Nel caso in cui sia stata omessa la pubblicazione nella BDNCP, la richiesta di accesso civico di cui al comma 1 del presente articolo è presentata al RPCT della stazione appaltante/ente concedente al fine di verificare se tale omissione sia imputabile ai soggetti tenuti all'elaborazione o trasmissione dei dati.

Ove sia appurato che la stazione appaltante/ente concedente abbia effettivamente trasmesso i dati alla BDNCP per il tramite della PCP, la richiesta di accesso di cui al precedente comma è presentata al RPCT di ANAC, in qualità di amministrazione titolare della BDNCP.

Adempimenti Legge 190/2012 art. 1, comma 32

AVVISO ANAC 5 GENNAIO 2024

Con il nuovo Codice dei contratti pubblici, che ha abrogato l'art.1 comma 32 della legge n.190/2012, dal 2024, **gli enti e le pubbliche amministrazioni non dovranno più compilare e pubblicare il file XML contenente il riepilogo dei contratti in essere nell'anno precedente, né inviare entro il 31 gennaio ad ANAC via PEC la dichiarazione di avvenuta pubblicazione del file nella propria sezione Amministrazione Trasparente.**

Considerato che la BDNCP assicura la pubblicazione dei dati di cui all'art. 28, comma del Codice Appalti tra cui quelli già previsti dall'art. 1, co. 32, della legge 190/2012 pertanto abrogato dal nuovo codice ed, in particolare, dei seguenti dati: la struttura proponente, l'oggetto del bando, l'elenco degli operatori invitati a presentare offerte, l'aggiudicatario, l'importo di aggiudicazione, i tempi di completamento dei lavori, servizi o forniture e l'importo delle somme liquidate.

Non è più prevista, per alcuna procedura contrattuale, la predisposizione del file XML e l'invio ad ANAC della PEC, entro il 31 gennaio,

Adempimenti Legge 190/2012 art. 1, comma 32

AVVISO ANAC 5 GENNAIO 2024

Per i contratti conclusi entro il 2023: gli obblighi di pubblicazione dei dati in questione risultano adempiuti pubblicando nella sezione “Amministrazione trasparente” sottosezione “Bandi di gara e contratti” le informazioni di cui all’art. 4 della delibera 39/2016 in formato digitale standard aperto, secondo le modalità indicate dalla stessa delibera.

Per i contratti non conclusi entro il 2023: la trasparenza degli stessi dati già previsti dall’art. 1, co. 32 della l. 190/2012 e ora indicati nell’art. 28, co. 3 del nuovo codice, **è assolta mediante comunicazione tempestiva degli stessi, cioè nell’immediatezza della loro produzione, alla BDNCP tramite SIMOG** (cfr. Comunicato congiunto ANAC-MIT, delibera 582 del 13 dicembre 2023). Le stazioni appaltanti pubblicano in “Amministrazione Trasparente”, sottosezione “Bandi di gara e contratti”, il **link** tramite il quale si accede alla sezione della BDNCP dove sono pubblicate, per ogni procedura di affidamento associata a un CIG, tutte le informazioni che le stazioni appaltanti hanno trasmesso attraverso SIMOG.

Adempimenti Legge 190/2012 art. 1, comma 32

AVVISO ANAC 5 GENNAIO 2024

Per i contratti la cui procedura si avvia dal 1° gennaio 2024: la trasparenza dei dati già previsti dall'art. 1, co. 32 della l. 190/2012, e ora indicati nell'art. 28 co. 3 del nuovo codice, **è assolta mediante la trasmissione degli stessi dati alla BDNCP attraverso le piattaforme di approvvigionamento digitale certificate. Le stazioni appaltanti e gli enti concedenti inseriscono sul sito istituzionale, nella sezione "Amministrazione trasparente", un collegamento ipertestuale che rinvia ai dati relativi all'intero ciclo di vita** del contratto e che includono anche quelli indicati all'art. 28, co. 3 del nuovo codice.

Per informazioni e chiarimenti

avvalessandralezzi@eduservice.it

info@eduservice.it

ACCESSO AGLI ATTI E RISERVATEZZA

Art. 35 del D.Lgs 36/2023 (Codice Contratti pubblici)

Le stazioni appaltanti e gli enti concedenti assicurano in modalità digitale l'accesso agli atti delle procedure di affidamento e di esecuzione dei contratti pubblici, mediante acquisizione diretta dei dati e delle informazioni inseriti nelle piattaforme, ai sensi degli articoli 3-bis e 22 e seguenti della legge 7 agosto 1990, n. 241 e degli articoli 5 e 5-bis del decreto legislativo 14 marzo 2013, n. 33.

Art 5 bis. Esclusioni e limiti all'accesso civico.

L'accesso di cui all'articolo 5, comma 2, è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia;
b) la libertà e la segretezza della corrispondenza;
c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

ART. 25 D.LGS 36/2023 PIATTAFORME DI APPROVVIGIONAMENTO DIGITALE

Le piattaforme di approvvigionamento digitale assicurano **la piena digitalizzazione dell'intero ciclo di vita dei contratti pubblici. Esse infatti sono** sono costituite dall'insieme **dei servizi e dei sistemi informatici, interconnessi e interoperanti**, utilizzati dalle stazioni appaltanti e dagli enti concedenti per svolgere una o più **attività di cui all'articolo 21, comma 1, (programmazione, progettazione, pubblicazione, affidamento ed esecuzione)**

Le **Piattaforme di approvvigionamento digitale** interoperano con i servizi erogati dalla **BDNCP mediante i servizi della (PCP)**, secondo le regole tecniche stabilite da AgID nel provvedimento "Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale" adottate ai sensi dell'articolo 26 del codice.

PRINCIPI IN MATERIA DI TRASPARENZA

Art. 19,comma 2 del D.Lgs 36/2023

"In attuazione del **principio dell'unicità dell'invio**, ciascun dato è fornito una sola volta a un solo sistema informativo. **Tale principio si applica** ai dati relativi a programmazione di lavori, opere, servizi e forniture, nonché **a tutte le procedure di affidamento e di realizzazione di contratti pubblici soggette al presente codice** e a quelle da esso escluse, in tutto o in parte, **ogni qualvolta siano imposti obblighi di comunicazione a una banca dati o a un sistema informativo"**

ART. 23 BANCA DATI NAZIONALE DEI CONTRATTI PUBBLICI

Art. 23 D.Lgs 36/2023) La Banca dati nazionale dei contratti pubblici (BDNCP) è istituita dall'articolo 62 bis del codice dell'Amministrazione Digitale di cui al decreto legislativo 7 marzo 2005, n. 82 ed è disciplinata dagli articoli 23 e 222, comma 8 del codice dei contratti pubblici.

La **BDNCP** si articola nelle seguenti sezioni:

a) **Anagrafe Unica delle Stazioni Appaltanti (AUSA)**

b) **Piattaforma contratti pubblici (PCP)** è il complesso dei servizi web attraverso i quali le piattaforme di approvvigionamento digitale delle stazioni appaltanti interoperano con la BDNCP per la gestione digitale del ciclo di vita dei contratti pubblici

c) **Piattaforma per la pubblicità legale degli atti** –> Tipo di procedura? Importo? Per la pubblicità legale degli atti ai sensi degli articoli 84 e 85 relativi agli appalti aggiudicati di importo pari o superiore alle soglie di cui all'art. 14.

d) **Fascicolo virtuale dell'operatore economico (FVOE)**

e) **Casellario Informatico**

f) **Anagrafe degli operatori economici**