ARSAC

Azienda Regionale per lo Sviluppo
dell'Agricoltura Calabrese

REGOLAMENTO SULLA GESTIONE E PROTEZIONE DEI DATI PERSONALI

Approvato con deliberazione n. 123/cs *del* 07 OTT. 2024

INDICE-SOMMARIO

CAPO I – DISPOSIZIONI GENERALI

Art. 1 - Oggetto e finalità

1. Il presente Regolamento disciplina i processi interni di attuazione del Reg. UE 2016/679 (GDPR) ai fini del trattamento di dati personali per finalità istituzionali nell'Ente e, pertanto, integra il vigente Regolamento sull'organizzazione degli uffici e dei servizi. Scopo precipuo del presente Regolamento è la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal Titolare, nel rispetto di quanto previsto dal GDPR.

2. Ai fini del presente Regolamento, per funzioni istituzionali si intendono quelle:
a) previste dalla legge, dallo statuto dell'Ente e dai suoi regolamenti;
b) esercitate in attuazione di convenzioni, accordi nonché sulla base degli strumenti di programmazione e pianificazione previsti dalla legislazione vigente;
c) svolte per l'esercizio dell'autonomia organizzativa, amministrativa e finanziaria dell'Ente;
d) in esecuzione di un contratto con i soggetti interessati;
e) in casi eccezionali, per finalità specifiche e diverse dai punti precedenti.

3. Il Titolare garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

4. Ai fini della tutela dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali, tutti i processi, inclusi i procedimenti amministrativi di competenza del Titolare, devono essere gestiti conformemente alle disposizioni del Codice in materia di dati personali di cui al d.lgs. n. 196/2003 e successive modificazioni, del GDPR e del presente Regolamento.

Art. 2 - Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali (D.lgs. n. 196/2003) e ss.mm.;
- Regolamento UE 679/2016 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR) e ss. mm.;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (*databreach notification*) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di Trasparenza del trattamento - WP 260 rev.01 Versione emendata adottata l'11 aprile 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Parere del WP29 8 giugno 2017 sul trattamento dati sul posto di lavoro;
- Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea (Regolamento (UE) 2016/679) - Elaborato per il programma "T4DATA" finanziato dall'UE versione approvata dalla Commissione, luglio 2019;
- Linee Guida dell'EDPS n. 7/2020 sui concetti di titolare del trattamento e responsabile del trattamento nel GDPR – Adottate il 2 settembre 2020;

- Linee Guida dell'EDPB n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 Adottate il 29 gennaio 2020;
- DECISIONE DI ESECUZIONE (UE) 2021/914 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio;
- DECISIONE DI ESECUZIONE (UE) 2021/915 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio;
- Linee Guida dell'Autorità Garante per la protezione dei dati personali in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (Registro dei provvedimenti n. 243 del 15 maggio 2014);
- Provvedimento in materia di videosorveglianza 08/04/2010 emesso dell'Autorità Garante per la protezione dei dati personali;
- Linee guida dell'European Data Protection Board n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video;
- Ulteriori Linee guida, Provvedimenti e raccomandazioni *ratione materiae* dell'Autorità Garante per la protezione dei dati personali.

CAPO II – PRINCIPI IN MATERIA DI PROTEZIONE DATI PERSONALI

Art. 3 – Principi

1. Per le finalità indicate nell'art. 1, l'Azienda Regionale per lo Sviluppo dell'Agricoltura in Calabria (di seguito, "ARSAC"), Titolare del trattamento dei dati, svolge il trattamento nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche.

2. Vengono, pertanto, integralmente recepiti, nell'ordinamento interno di ARSAC, i principi del GDPR, per effetto del quale i dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati in base al principio di "minimizzazione dei dati";
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati base del principio di "esattezza";
- 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, del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato in base al principio di "limitazione della conservazione";
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali in base ai principi di "integrità e riservatezza";
- configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo in caso di necessità ("principio di necessità")[1].

[1] Art. 5, par. 1, GDPR.

3. Il Titolare è competente per il rispetto dei principi sopra declinati ed è in grado di comprovarlo in base al principio di accountability ("responsabilizzazione")[2].

4. Collegati *all'accountability* sono i principi di *privacy by design*: sia al momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso, il Titolare mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati[3], nonché di *privacy by default*: il Titolare mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento[4].

Art. 4 – Categorie di dati trattati e liceità del trattamento

1 Il Titolare, nell'esercizio delle sue funzioni istituzionali, tratta, in modo manuale e automatizzato, in presenza di idonea base giuridica, le seguenti categorie di dati personali:

- dati personali di tipo "comune", quali dati identificativi (ossia quelle informazioni che consentono di risalire all'identità dell'interessato, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *on line* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, fisica, economica, culturale o sociale), anagrafici e di contatto;
- categorie particolari di dati personali, ossia 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[5];
- dati personali relativi a condanne penali e reati[6].

2. Il trattamento di dati personali di tipo "comune" 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 (base giuridica, tuttavia, "residuale" in ambito pubblico);
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;
d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona;
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[7];
f. il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi (base giuridica, tuttavia, non applicabile in ambito pubblico)[8].
La base su cui si fonda il trattamento dei dati di cui all'art. 6, par. 1, lettere c) ed e), deve essere stabilita: a) dal diritto dell'Unione Europea; o b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento[9]. In tal senso, il Codice privacy chiarisce che la base giuridica, prevista dall'articolo 6, paragrafo 3, lettera b), GDPR, è costituita esclusivamente da una norma di legge o di regolamento o da atti amministrativi generali[10].

3. In ordine, invece, alla liceità del trattamento delle "categorie particolari" di dati personali indicate nell'articolo 9, par. 1, del GDPR, vige il divieto generale di trattamento, dunque, il Titolare può trattare tali tipi di dati personali soltanto al ricorrere di una delle eccezioni previste dal GDPR[11]. Ciò avviene, in particolare, in ambito pubblico, qualora il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione Europea o degli Stati membri; il trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato). Il legislatore italiano ha elencato, nel Codice[12], i

---

[2] Art. 24, par. 1, GDPR.
[3] Art. 25, par. 1, GDPR.
[4] Art. 25, par. 2, GDPR.
[5] Art. 9, GDPR.
[6] Art. 10, GDPR.
[7] Come confermato dall'art. 1, comma 1-bis, Codice privacy.
[8] Art. 6, par. 1, GDPR.
[9] Art. 6, par. 3, GDPR.
[10] Art. 2-ter, comma 1, Codice privacy.
[11] Art. 9, par.2, GDPR.
[12] Art. 2-sexies, comma 2, Codice privacy, in particolare le lettere bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario; cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento

casi in cui si considera rilevante l'interesse pubblico, mentre, per i dati relativi alla salute assume centralità l'articolo 2-septies, Codice privacy.

4. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati[13]. Fatto salvo quanto previsto dal decreto legislativo 18 maggio 2018, n. 51, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, GDPR, che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati[14]. Il Codice privacy elenca i casi[15] in cui è consentito il trattamento di dati personali relativi alle condanne penali e ai reati, se autorizzato da una norma di legge o di regolamento, comunque applicando le disposizioni previste dall'articolo 2-sexies del Codice[16].

Art. 5 – Principio di correttezza e trasparenza nei confronti dell'interessato. L'informativa.

1. Il Titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi dei soggetti delegati o autorizzati, apposita informativa secondo le modalità previste dagli articoli 12, 13 e 14, GDPR, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

2. L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi on line, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra, qualora l'interessato lo richieda espressamente, previa verifica dell'identità dell'interessato[17]. L'informativa può essere fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati, in cui sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti;
- avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del Titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il Titolare;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure.

3. Il momento del rilascio dell'informativa è:
a) in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, il momento della raccolta dei dati;
b) in caso di dati personali non ottenuti presso l'interessato:
- entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati;
- nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione;
- se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.

4. Il contenuto minimo dell'informativa[18] è il seguente:

- l'identità e i dati di contatto del Titolare;
- i dati di contatto del RPD/DPO nominato dal Titolare;
- le finalità del trattamento e, per ognuna di queste, la base giuridica del trattamento;

---

e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan); dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

[13] Art. 10, par.1, GDPR.

[14] Art. 2-octies, comma 1, Codice privacy.

[15] Art. 2-octies, comma 3, Codice privacy.

[16] Art. 2-octies, comma 3, Codice privacy.

[17] Art. 12, par. 1, GDPR.

[18] Art. 13, GDPR.

- le categorie di dati trattati e le modalità del trattamento (in particolare, se esiste un processo decisionale automatizzato, compresa la profilazione, eventualmente, le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato);
- le categorie di responsabili del trattamento e, in generale, i destinatari dei dati (comunicazione e diffusione);
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- se il Titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
- il diritto dell'interessato di chiedere al titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo all'autorità di controllo.

5. Nel caso i dati personali non siano raccolti direttamente presso l'interessato, il Titolare deve informare l'interessato in merito alla fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico. L'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato[19].

6. Apposite informative devono essere inserite negli avvisi pubblici e nella documentazione di affidamento dei contratti pubblici, in accordi o convenzioni, bandi di concorso pubblico, segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali. In tal senso, in caso di dubbi, è opportuno contattare, con congruo preavviso, il RPD/DPO per adeguata consulenza. Non è necessario fornire l'informativa nel caso in cui l'interessato disponga già di tutte le informazioni necessarie o nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.

Art. 6 - Sensibilizzazione e formazione in materia di protezione dati personali

1. Ai fini della corretta applicazione della disciplina relativa alla protezione dei dati personali, il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza e migliorare la qualità del servizio[20]. Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data a ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente i riferimenti per la consultazione del presente regolamento, pubblicato sul sito del Titolare. Il dipendente si impegna ad acquisire il Regolamento, prenderne visione e attenersi alle sue prescrizioni.

2. Nell'ambito della formazione continua e obbligatoria del personale, il Titolare organizza, con il coordinamento del RPD/DPO, specifici interventi di formazione e di aggiornamento, con la collaborazione del Responsabile per la Prevenzione Corruzione e della Trasparenza (RPCT), del Responsabile per la Transizione Digitale (RTD) e del Servizio Informatico dell'Ente. Le sessioni formative del personale, che sono necessarie, anche con riscontro dell'acquisizione di abilità e competenze, al fine di garantire, nell'attività degli uffici, il massimo di trasparenza possibile e l'assoluto rispetto dei diritti di riservatezza dei dati personali dei cittadini e dipendenti, sono finalizzate alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza di misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi e alla cybersecurity.

3. La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata, a cura del RPCT e del RPD/DPO, con la formazione in materia di prevenzione della corruzione e della illegalità, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, whistleblowing, nei diversi ambiti in cui opera il Titolare. La partecipazione dei dipendenti agli interventi formativi viene

[19] Art. 14, GDPR.
[20] Art. 29, GDPR.

considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

CAPO III - TRATTAMENTO DEI DATI PERSONALI

Art. 7 – Registro dei trattamenti

1. Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, soltanto da parte dei:

- dirigenti dei vari Settori, in qualità di soggetti che esercitano i poteri delegati dal Titolare;
- dipendenti, in qualità di soggetti Autorizzati al trattamento dal Titolare o dai soggetti Delegati.

Il Titolare tratta i dati personali, nei limiti imposti dal Codice, dal GDPR e dalle Linee Guida e dai provvedimenti del Garante, per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari (quale, a titolo esemplificativo, la gestione del personale e dei soggetti che intrattengono rapporti giuridici con il titolare, diversi dal rapporto di lavoro dipendente, e che operano a qualsiasi titolo all'interno della struttura organizzativa del Titolare, ivi compresi gli stagisti, tirocinanti e i volontari), pertanto, istituisce e tiene aggiornato, in forma scritta ed in formato elettronico, con l'ausilio del RPD/DPO, un registro delle attività di trattamento svolte sotto la propria responsabilità[21].

2. All'uopo, va contattato il RPD/DPO ogni qual volta l'Ente attivi un nuovo procedimento amministrativo che comporti un trattamento di dati personali, affinché si vagli la liceità del nuovo trattamento e si provveda all'aggiornamento del registro delle attività di trattamento. Tale operazione, in mancanza di nuovi procedimenti, deve essere comunque espletata almeno ogni due anni, con un'integrale ricognizione e aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del Titolare, funzionali alla formazione dell'indice dei trattamenti e all'analisi del rischio dei trattamenti e alla valutazione di impatto sulla privacy degli interessati (DPIA).

3. Il registro, che deve essere sempre a disposizione delle autorità di controllo, contiene, almeno, le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento e del Responsabile per la protezione dei dati nominato;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie dei dati personali;
- le categorie dei trattamenti effettuati;
- le categorie di destinatari, a cui i dati personali sono o saranno comunicati;
- eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con documentazione delle garanzie in materia di privacy;
- una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;
- l'indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

4. Ove l'Ente dovesse operare in qualità di Responsabile di trattamento, ciò dovrà risultare nel Registro dei trattamenti.

Art. 8- Trattamento dei dati personali dei dipendenti dell'Ente

1. Il Titolare tratta i dati dei propri dipendenti al fine di instaurare e gestire i rapporti di lavoro, ad esempio, per accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi o la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, per adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché agli obblighi retributivi, fiscali e contabili.

2. I dati sullo stato di salute dei dipendenti devono essere conservati separatamente rispetto alle altre informazioni personali. Il fascicolo, che raccoglie tutti gli atti relativi al percorso professionale e ai fatti più significativi, può mantenere la sua unitarietà adottando accorgimenti che impediscano un accesso indiscriminato, quale, ad esempio, l'utilizzo di sezioni o fascicoli dedicati alla custodia dei dati più sensibili, da conservare chiusi o comunque con modalità che riducano la possibilità di una indistinta consultazione nel corso delle ordinarie attività amministrative.

3. Il trattamento di dati del dipendente idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a

[21] Art. 30, GDPR.

identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, deve avvenire secondo i principi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo dei dati personali, e quando non si possa prescindere dall'utilizzo di tali dati, di trattare soltanto le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.

4. Il Titolare si conforma alle Linee Guida del Garante in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico.

Art. 9 – Trattamento dei dati personali nei procedimenti di affidamento di lavori, beni, servizi e forniture, concessioni, ecc.

1. Il trattamento di dati personali, nell'ambito dei procedimenti di affidamento di lavori o forniture di beni o servizi, ecc., risulta necessario per le seguenti finalità:

a) gestione di bandi, concorsi, procedure di appalto per l'assegnazione di lavori, servizi e forniture, concessioni, ecc. a cui l'interessato ritiene di partecipare spontaneamente, nonché la relativa instaurazione e gestione del rapporto contrattuale;
b) accertamento dei requisiti di idoneità morale, onorabilità e/o degli ulteriori requisiti soggettivi e presupposti interdittivi previsti dalla vigente normativa in materia di appalti pubblici;
c) adempiere agli obblighi di legge di natura amministrativa, contabile, civilistica, fiscale, regolamenti, normative;
d) permettere l'assolvimento degli obblighi in materia di trasparenza dei dati e delle informazioni, in conformità a quanto disposto dalle normative vigenti e dalle Linee Guida emanate dalle autorità competenti.

2. La base giuridica di liceità di tali trattamenti è rinvenibile nell'art. 6, par.1, lettere b) e c), GDPR, poiché il trattamento è necessario all'esecuzione di misure precontrattuali, di un contratto di cui l'interessato è parte nonché per adempiere ad un obbligo legale al quale è soggetto il Titolare del trattamento.

3. Nell'ambito delle predette finalità e delle susseguenti operazioni di trattamento, riferite al presente punto, al Titolare è demandato il compito di trattare dati personali di tipo "comune", categorie "particolari" di dati personali, nonché dati relativi a condanne penali e reati, quali, in via meramente esemplificativa, autocertificazioni casellario giudiziario, carichi pendenti e dichiarazioni antimafia, riguardanti, altresì, dipendenti e/o collaboratori e /o soggetti che ricoprono, a diverso titolo, cariche societarie delle imprese partecipanti.

4. Viene in evidenza che, in tali procedimenti, in forza dei poteri attribuiti al Titolare, quest'ultimo potrebbe verificare la veridicità delle informazioni rese dall'impresa/professionista partecipante, anche mediante acquisizione di dati presso altre pubbliche amministrazioni (in via meramente esemplificativa e non esaustiva, Procura della Repubblica, Tribunali, Prefettura, Ordini Professionali, Enti di istruzione formazione, Anagrafe antimafia, Agenzia delle Entrate, INPS, INAIL, Cassa Edile competente territorialmente, ecc.).

Art. 10 – Comunicazione e diffusione dei dati personali

1. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle categorie di cui agli articoli 9 e 10, GDPR, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1 dell'art. 2-ter del Codice privacy o se necessaria ai sensi del comma 1-bis dello stesso articolo[22].

2. Si intende per:
a) "comunicazione" il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2 quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
b) "diffusione" il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione[23].

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 dell'art. 2-ter del Codice privacy o se necessarie ai

[22] Art. 2-ter, comma 2, Codice privacy.
[23] Art. 2-ter, comma 4, Codice Privacy.

sensi del comma 1-bis dello stesso articolo. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione[24].

Art. 11 - Pubblicazione online dei documenti amministrativi per obblighi di trasparenza e pubblicità

1. Poiché documenti e informazioni in pubblicazione sull'Albo pretorio online e nella Sezione "Amministrazione trasparente" possono contenere dati personali, in tal caso, si concretizza un'operazione di "diffusione" dei dati personali.

2. Il Titolare, nell'espletare i propri obblighi di trasparenza e pubblicità previsti dalla normativa vigente, nel rispetto delle Linee guida del Garante privacy *ratione materiae*[25], cui si rinvia, assicura il rispetto dei principi di sicurezza, esattezza e completezza, accessibilità, limitazione delle finalità perseguite con la pubblicazione e, in particolare, il rispetto dell'art. 5 par. 1, lettera c), GDPR, secondo cui, i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati (minimizzazione dei dati). Ai sensi del Codice della trasparenza, «nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione»[26].

3. Il dipendente incaricato della pubblicazione è tenuto, dunque, prima di procedere alla pubblicazione a:
1) verificare:
- l'esistenza di un atto amministrativo generale o di una norma di legge o di regolamento, che preveda la pubblicazione del documento[27];
- che l'amministrazione pubblica agisca per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri, alla stessa attribuiti;

2) qualora la verifica dia esito negativo, pubblicare il documento solo previa anonimizzazione dei dati personali contenuti nel documento (oscuramento, apposizione di "Omissis", ecc.);

3) qualora tale verifica dia, invece, esito positivo è necessario indagare la natura dei dati personali contenuti nel documento[28].

4. Ai sensi del Decreto Legislativo del 14 marzo 2003 n. 33, «è esclusa la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di cui al presente articolo, qualora da tali dati sia possibile ricavare informazioni relative»: «allo stato di salute» o «alla situazione di disagio economico-sociale degli interessati»[29]. In tal caso il legislatore ha effettuato a monte una valutazione circa la prevalenza del diritto alla riservatezza rispetto all'interesse, pur ugualmente importante, alla trasparenza. Spetta quindi all'amministrazione valutare se la tipologia di erogazioni da pubblicare si caratterizzi o meno per essere un aiuto finanziario di sostegno a quelle categorie di soggetti che si trovano nelle condizioni per le quali il comma 4 dell'art. 26 impone particolare tutela della riservatezza. Spesso, la P.A. è tenuta a pubblicare l'elenco dei beneficiari, sostituendo, nella versione "pubblicabile" del documento, i dati personali delle persone fisiche (cognome e nome, residenza o altri dati personali) con un codice che non consenta l'identificazione dell'interessato ("anonimizzazione").

5. I sistemi informativi ed i programmi informatici dovrebbero essere configurati per ridurre al minimo l'utilizzazione di dati personali e devono prevedere la possibilità di estrazione degli atti, con l'esclusione dei dati personali in essi contenuti. Con riferimento alla durata della pubblicazione *on-line*, si rinvia alla normativa di settore di volta in volta emergente.

6. Grande cautela deve essere usata nella pubblicazione on-line delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici,

---

[24] Art. 2-ter, comma 3, Codice privacy.

[25] Autorità Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, 15 maggio 2014, doc. web n. 3134436.

[26] Art. 7-bis, comma 4, Codice della trasparenza.

[27] Art. 2-ter, Codice Privacy, come modificato, da ultimo, dal Decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.

[28] Cfr. art. 2-septies, comma 8, Codice Privacy e art. 9, parr. 1, 2 e 4, GDPR.

[29] Art. 26, comma 4, Codice Privacy, "Obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati".

agevolazioni, elargizioni al personale. In tali casi, la pubblicazione dovrebbe avvenire mediante token, diciture generiche o codici numerici, salvo pubblicazioni obbligatorie previste dalla normativa vigente.

Art. 12 - Diritto di accesso e protezione dei dati personali

1. Con riferimento al diritto di accesso cd. documentale, il Codice Privacy stabilisce che «i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia»[30].Ciò, «fatto salvo quanto previsto dall'articolo 60» del Codice privacy, laddove stabilisce che «quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale»[31].

2. Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, può chiedere documenti in possesso del Titolare e può estrarne copia, anche se contengono dati personali di un terzo interessato[32]. Il rilascio è subordinato alla verifica, da parte dell'Ente, che il diritto difeso sia di rango almeno pari a quello dell'interessato e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile. L'Ente si conforma, in tema di indagini difensive, alla giurisprudenza maggioritaria[33] e alle decisioni del Garante[34], che ha confermato la legittimità dell'accesso a qualsiasi tipologia di dato personale necessario «per far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo»[35], pur ricordando che l'accesso a documenti contenenti dati idonei a rivelare lo stato di salute o la vita sessuale dell'interessato (quali, ad esempio, le "cartelle cliniche") comporta una concreta valutazione dei diritti coinvolti (non il diritto di azione e di difesa, quanto il diritto sostanziale che si vuole difendere), nonché l'applicazione del principio di necessità, pertinenza e non eccedenza.

3. Con riferimento, invece, al diritto di accesso civico generalizzato ai dati e documenti detenuti dalle pubbliche amministrazioni (ulteriori rispetto a quelli oggetto di pubblicazione) disciplinato dal Codice della Trasparenza[36] esso deve essere esercitato nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti[37]. Il Codice Privacy stabilisce che «i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33»[38].Il Responsabile per la Prevenzione della Corruzione e per la Trasparenza ("RPCT") controlla e assicura il regolare esercizio dell'accesso civico e dell'accesso civico generalizzato sulla base di quanto stabilito dal d.lgs. n. 33/2013 e dalle Linee guida ANAC, sentito, ove necessario, il parere del Garante per la protezione dei dati personali.

4. L'accesso civico generalizzato può essere escluso o limitato dall'Ente, con opportuna motivazione, se la richiesta rientra nelle ipotesi di cui all'art. 5-bis commi 1, 2, 3, D.lgs. 33/2013, tali da rappresentare delle eccezioni assolute o relative. Tra le eccezioni relative vi è il pregiudizio concreto alla protezione dei dati personali, in conformità con la disciplina legislativa in materia. Con riferimento a tale limite, qualora i dati personali contenuti nei documenti non siano pertinenti o siano eccedenti rispetto all'interesse manifestato dal richiedente nell'istanza di ostensione, al fine di salvaguardare la riservatezza di terzi, l'accesso agli atti può essere limitato, su valutazione del Responsabile del procedimento, mediante l'adozione di misure di sicurezza adeguate, compresa la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali e l'occultamento o oscuramento, l'apposizione di "Omissis". Il RPCT e i dipendenti dell'Ente possono in ogni momento chiedere al Responsabile Protezione Dati (RPD/DPO) un parere sull'opportunità di accordare l'accesso, affinché la stessa ostensione non vada a ledere il diritto alla riservatezza di eventuali controinteressati.

5. In particolare, «Fatti salvi i casi di pubblicazione obbligatoria, l'amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, ai sensi dell'articolo 5-bis, comma 2, è tenuta

---

[30] Art. 59, comma 1, Codice Privacy.
[31] Art. 60, comma 1, Codice Privacy.
[32] Cfr. L. 7 dicembre 2000, n. 397 e art. 391-quater del codice di procedura penale.
[33] Consiglio di Stato, Sez. IV, sentenza 22 novembre 2022, n. 10277.
[34] Cfr., amplius, Provvedimento Generale del 9 luglio 2003 sui "diritti di pari rango".
[35] Garante privacy, "Dati sanitari. Provvedimento generale sui diritti di 'pari rango'" - 9 luglio 2003, docweb n. 29832.
[36] Art. 5, comma 2, D.lgs. n. 33/2013, ss.mm.ii.
[37] Art. 5-bis, D.lgs. n. 33/2013, ss.mm.ii.
[38] Art. 59, comma 1-bis, Codice Privacy.

a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione»[39]. Rispetto a una domanda di accesso civico generalizzato, sono qualificabili come controinteressati tutti i soggetti che possono subire un pregiudizio concreto agli interessi privati indicati dall'art. 5-bis, comma 2, D.lgs. n. 33/2013. Per quanto riguarda, infine, le modalità di comunicazione della richiesta di accesso civico generalizzato ai controinteressati, il richiamato art. 5, comma 5, ne identifica due: l'invio di copia della richiesta con raccomandata con avviso di ricevimento o l'invio per via telematica per coloro che abbiano consentito tale forma di comunicazione. La finalità di questa disposizione è consentire ai controinteressati di esercitare il diritto di difesa nell'ambito del procedimento amministrativo di accesso.

6. Non sono ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro dei dipendenti dell'Ente, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'Amministrazione, idonee a rivelare taluna delle informazioni di cui agli articoli 9 e 10 del GDPR.

Art. 13 – Trattamento di dati personali da parte di soggetti esterni all'ARSAC

I dati personali trattati da ARSAC in qualità di Titolare possono essere trattati da soggetti esterni all'ARSAC (ad es. consulenti, società affidatarie, ecc.) soltanto previo apposito accordo di contitolarità ai sensi dell'art. 26, GDPR, o clausole contrattuali ai sensi dell'art. 28, GDPR, fatti salvi i casi di titolarità autonoma.

CAPO IV – ORGANIGRAMMA PRIVACY

Art. 14 - Titolarità del trattamento dei dati personali

1. Il Titolare del trattamento dei dati personali è l'ARSAC, che come tale, dunque, ha la piena responsabilità delle decisioni circa le finalità e i mezzi del trattamento. Essa è rappresentata, ai fini del GDPR, dal rappresentante legale pro-tempore e, di volta in volta, dai soggetti Delegati al trattamento per specifici compiti e funzioni.

2. Il Titolare provvede:
- a definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento, provvedendo all'inserimento di tali obiettivi strategici negli altri documenti di programmazione e pianificazione;
- a garantire il rispetto dei principi elencati nel presente Regolamento nonché le disposizioni del GDPR e del Codice privacy;
- a far sì che le misure siano definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio;
- a delegare ovvero a nominare, con proprio atto, i Dirigenti, per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali, impartendo ad essi le necessarie istruzioni in relazione agli obblighi previsti dal GDPR;
- a designare, con proprio atto, il Responsabile per la protezione dei dati personali (RPD/DPO);
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- a svolgere un'analisi del rischio dei trattamenti di dati personali per i diritti e le libertà degli interessati e a svolgere, ove richiesto dalla normativa, una valutazione di impatto (DPIA) sulla privacy degli interessati, ai sensi dell'art. 35, GDPR;
- ad assolvere agli obblighi nei confronti del Garante, nei casi previsti dalla vigente normativa.

3. Il Titolare si trova in rapporto di contitolarità con altri Titolari quando, insieme, determinano congiuntamente le finalità e i mezzi del trattamento. Ad esempio, ciò avviene nei casi di esercizio associato di funzioni e servizi, nonché quando all'Ente sono affidati compiti da altri enti ed organismi statali o regionali. I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i Titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale

[39] Art. 5, comma 5, Codice della Trasparenza.

dell'accordo è messo a disposizione dell'interessato. Indipendentemente dalle disposizioni dell'accordo interno, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun Titolare del trattamento[40].

Art. 15- Soggetti Delegati dal Titolare (Dirigenti, Responsabili di Settore, ecc.)

1. Il Titolare, ai sensi del Codice Privacy[41], può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Ciò avviene mediante apposito provvedimento di delega di funzioni ai Dirigenti, in cui il Titolare informa ciascun soggetto Delegato delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento.

2. Negli obblighi e poteri dei soggetti Delegati rientra, oltre alla vigilanza sul personale che presta attività nel Settore o Ufficio di competenza, la funzione di garantire il rispetto, nell'Ente, delle disposizioni della normativa vigente, del presente Regolamento e delle specifiche istruzioni impartite dal Titolare, in merito, ad esempio, a:

- modalità del trattamento;
- designazione dei Responsabili esterni del trattamento e stipula degli accordi di contitolarità;
- elaborazione delle informative da fornire agli interessati;
- comunicazione tempestiva dell'inizio di un nuovo trattamento, della cessazione o modifica dei trattamenti in atto, nonché di ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva);
- vigilanza sulle misure di sicurezza del trattamento;
- collaborazione e assistenza al Responsabile della protezione dei dati (RPD/DPO) nell'esercizio delle proprie funzioni, in particolare nelle fasi di aggiornamento del registro dei trattamenti e di analisi del rischio e valutazione di impatto sulla protezione dei dati nonché in caso di richieste per l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22, GDPR;
- richiesta di pareri al medesimo Responsabile della protezione dei dati (RPD/DPO) ogniqualvolta ciò si renda necessario.

3. Ciascun soggetto Delegato risponde al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e dal presente Regolamento.

4. Ciascun soggetto Delegato è tenuto a partecipare agli interventi di formazione e aggiornamento in materia di protezione dati personali organizzati dal Titolare e dal Responsabile della protezione dei dati (RPD/DPO).

5. L'incarico di soggetto Delegato è gratuito e strettamente collegato e funzionale alle mansioni svolte e necessario per lo svolgimento delle stesse, pertanto, non costituisce conferimento di nuova mansione o ruolo. La nomina può essere revocata in qualsiasi momento, anche senza preavviso, e si intende automaticamente revocata al venir meno del rapporto di lavoro con l'Ente così come al venir meno della funzione dirigenziale.

Art. 16 - Soggetti Autorizzati al trattamento dei dati personali

1. Il Titolare del trattamento fa sì che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso[42]. Il titolare individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta[43]. A tali fini, l'Ente, in persona del rappresentante legale pro tempore o dei rispettivi soggetti "Delegati", formalizza la responsabilizzazione del personale coinvolto nelle attività di trattamento dei dati personali nei procedimenti amministrativi dell'Ente[44] mediante una nomina ai soggetti "Autorizzati".

---

[40] Art. 26, GDPR.

[41] Art. 2-quaterdecies, comma 1, Codice privacy.

[42] Art. 32, par. 4, GDPR.

[43] Art. 2-quaterdecies, comma 2, Codice privacy.

[44] Art. 29, GDPR.

2. La nomina informa i soggetti Autorizzati delle istruzioni e obblighi da seguire in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento in materia di protezione dei dati personali trattati nell'esercizio dei propri compiti e mansioni, e, in particolare, contiene istruzioni riguardanti almeno i seguenti ambiti: postazione di lavoro e personal computer, password, internet, posta elettronica, altri device, minacce e rischi del trattamento online, misure a tutela del trattamento, anche per i documenti su supporto cartaceo. La nomina deve altresì informare il soggetto Autorizzato che deve rendersi disponibile a collaborare con il RPD/DPO e il Referente Privacy/Gruppo di lavoro privacy, al fine di:

- prevenire, individuare e porre rimedio ai casi di violazione di dati personali (Data Breach);
- provvedere alla mappatura dei trattamenti e di analisi del rischio e valutazione di impatto sulla protezione dei dati;
- gestire le richieste per l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22, GDPR.

3. I soggetti Autorizzati sono destinatari degli interventi di formazione di aggiornamento organizzate dall'Ente sul tema della protezione dei dati.

4. Ciascun soggetto Autorizzato risponde al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e dal presente Regolamento.

5. L'incarico di soggetto Autorizzato è gratuito e strettamente collegato e funzionale alle mansioni svolte e necessario per lo svolgimento delle stesse, pertanto, non costituisce conferimento di nuova mansione o ruolo. La nomina può essere revocata in qualsiasi momento, anche senza preavviso, e si intende automaticamente revocata al venir meno del rapporto di lavoro con l'Ente.

6. Tutti i soggetti che svolgono un'attività di trattamento dei dati personali, e che non sono dipendenti dell'Ente (quali a titolo meramente esemplificativo i tirocinanti, i volontari, i soggetti che operano temporaneamente all'interno dell'Ente, ecc.): a) devono essere autorizzati mediante atto scritto di nomina; b) sono soggetti agli stessi obblighi cui sono sottoposti i dipendenti dell'Ente; c) sono destinatari degli interventi di formazione di aggiornamento organizzate dall'Ente sul tema della protezione dei dati.

Art. 17- Referente Privacy/Gruppo di lavoro privacy

1. Uno dei soggetti Delegati dal Titolare per specifici compiti e funzioni può rivestire anche la figura di "Referente privacy"per una migliore gestione dei rapporti dell'Ente con il RPD/DPO, dando un primo punto di riferimento al personale interno in materia di privacy. In alternativa, l'Ente può nominare un "Gruppo di lavoro privacy" per le medesime funzioni. In particolare, tali soggetti curano l'archiviazione della documentazione relativa ai rapporti con il DPO e al Sistema di Gestione privacy interno, così come l'adozione di modelli, procedure e policies.

2. L'incarico, da formalizzare mediante nomina, è gratuito e strettamente collegato e funzionale alle mansioni svolte e necessario per lo svolgimento delle stesse, pertanto, non costituisce conferimento di nuova mansione o ruolo. La nomina può essere revocata in qualsiasi momento, anche senza preavviso, e si intende automaticamente revocata al venir meno del rapporto di lavoro con l'Ente.

Art. 18 - Amministratore di sistema

1. L'Ente, ove necessario, si conforma al Provvedimento del Garante in merito all'Amministratore di Sistema[45]. Le nomine di Amministratore di sistema, da formalizzarsi mediante atto scritto, individuano generalmente tali figure nel Responsabile del Centro Elaborazione Dati o dell'Area ICT dell'Ente. Le nomine sono individuali e devono recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

2. L'operato dell'amministratore di sistema deve essere verificato, con cadenza periodica, da parte del Titolare, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto alle attività di trattamento dei dati personali.

3. L'amministratore di sistema è tenuto a coadiuvare, se richiesto, il Titolare, nella predisposizione e nell'aggiornamento o nell'integrazione della documentazione del rispetto del GDPR ed è destinatario degli interventi di formazione e aggiornamento organizzati dal Titolare.

---

[45]Provvedimento del Garante "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" del 27/11/2008, pubblicato in G.U. n. 300 del 24 dicembre 2008 e successive modifiche e integrazioni.

4. Poiché il punto 3-bis del richiamato Provvedimento del Garante dispone che «l'eventuale attribuzione al Responsabile del compito di dare attuazione alle prescrizioni impartite avvenga nell'ambito della designazione del Responsabile da parte del Titolare o anche tramite opportune clausole contrattuali», l'Ente, nelle nomine ai Responsabili del trattamento ex art. 28, GDPR, si assicura che tali soggetti, lì dove ne ricorrano i presupposti stabiliti dalla normativa vigente, provvedano a procedere alla designazione individuale degli Amministratori di Sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, dandone comunicazione al Titolare e alla persona designata, conservando un elenco con gli estremi identificativi e i dati di contatto degli Amministratori di Sistema, e verificandone, con cadenza periodica, l'operato.

Art. 19- Autorità garante per la protezione dei dati personali

1. Il GDPR stabilisce che ciascuno Stato membro dell'Unione europea dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del GDPR al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»)[46], con poteri di indagine, correttivi, autorizzativi e consultivi elencati nell'art. 58 del GDPR.

2. Tale autorità, in Italia, è individuata nel Garante per la protezione dei dati personali[47].

Art. 20 - Responsabile della protezione dei dati personali/Data Protection Officer (RPD/DPO)

1. L'Ente, quale organismo pubblico, ai sensi del GDPR è tenuto a nominare un proprio Responsabile della protezione dei dati personali/Data Protection Officer (RPD/DPO)[48]. Egli svolge i compiti assegnati dall'art. 39, par. 1, GDPR, agisce in posizione di autonomia e non può ricevere istruzioni in merito ai propri compiti né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati[49]. La nomina del RPD/DPO è comunicata dal Titolare al Garante privacy mediante apposita piattaforma online, nonché a tutto il personale in modo che la sua presenza e le sue funzioni siano note a tutti i dipendenti. Il nominativo e i dati di contatto del RPD/DPO devono essere pubblicati nel sito web istituzionale dell'Ente (generalmente nella sezione "Privacy" e/o nella sezione "Amministrazione trasparente").

2. Il Titolare si assicura che il RPD/DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali[50]. L'Ente mette a disposizione del RPD/DPO le risorse necessarie per adempiere ai suoi compiti e lascia accedere il RPD/DPO ai dati personali e ai trattamenti, sostenendo il medesimo nell'esecuzione dei propri compiti e per mantenere la propria conoscenza specialistica[51].

3. Il Titolare si assicura che il RPD/DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti. Il RPD/DPO non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti; egli riferisce direttamente al Presidente o a un suo delegato[52].Il RPD/DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri[53].

4. Gli interessati possono contattare il RPD/DPO per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR[54].

5. Il RPD/DPO esprime pareri (non vincolanti) sulle questioni sollevate dal personale dell'Ente; l'eventuale adozione di condotta difforme da quella suggerita dal RPD/DPO deve essere motivata.

Art. 21 - Responsabili del trattamento e Sub-Responsabili

1. Il Responsabile del trattamento ("data processor") è un soggetto esterno all'Organizzazione Titolare, definito, nell'art. 4 del GDPR, come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

2. Il Titolare può avvalersi di soggetti pubblici o privati che, in qualità di Responsabili del trattamento, per esperienza, capacità ed affidabilità, forniscano sufficienti garanzie del pieno rispetto delle vigenti

[46] Art. 51, par. 1, GDPR.
[47] Art. 2-bis, Codice privacy.
[48] Art. 37, par. 1, GDPR.
[49] Art. 38, par. 3, GDPR.
[50] Art. 38, par. 1, GDPR.
[51] Art. 38, par. 2, GDPR.
[52] Art. 38, par. 3, GDPR.
[53] Art. 38, par. 5, GDPR.
[54] Art. 38, par. 4, GDPR.

disposizioni, ivi compreso il profilo relativo alla sicurezza, e garantisca la tutela dei diritti dell'interessato[55].

3. La nomina del Responsabile del trattamento da parte del Titolare viene effettuata mediante atto giuridico, da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di servizi che comportano trattamenti di dati personali.

4. La nomina deve contenere tutti gli elementi previsti dalla Decisione di esecuzione (UE) 2021/915 della Commissione UE del 4 giugno 2021, relativa alle Clausole Contrattuali Tipo ("CCT") tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del GDPR.

5. Il Responsabile del trattamento non ricorre a un altro Responsabile (Sub-Responsabile) senza previa autorizzazione scritta, specifica o generale, del Titolare[56]. Al Sub-Responsabile sono imposti dal Responsabile, mediante atto giuridico, gli stessi obblighi presenti nella nomina del Titolare e al Responsabile, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR[57]. Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile.

CAPO V - SICUREZZA DEI DATI PERSONALI

Art. 22 - Misure di sicurezza

1. In ossequio ai principi enunciati nell'articolo 3 del presente Regolamento, il Titolare è tenuto a valutare l'adeguatezza delle misure di sicurezza in base al rischio del trattamento dei dati personali per i diritti e le libertà degli interessati. Stante l'abrogazione dell'Allegato B del Codice privacy, non esistono più "misure minime" da implementare per tutti i trattamenti. Dunque, 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 mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) 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 presentati dal trattamento 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.
Il Titolare (o un suo Delegato) fa sì che chiunque agisca sotto la propria autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso[58].

2. Il Titolare definisce e attua procedure operative in materia di individuazione dei ruoli privacy, gestione delle violazioni dei dati personali (data breach), gestione delle richieste degli interessati, analisi del rischio e valutazione di impatto sulla protezione dati, misure di sicurezza, audit, monitoraggio dei tempi di conservazione dei dati personali (data retention).

3. In caso di avvalimento di soggetti esterni (responsabili del trattamento), per l'adozione di misure di sicurezza, l'Ente provvede a richiedere a tali soggetti, per iscritto, la descrizione delle misure di sicurezza attuate in materia di protezione dei dati personali.

4. Restano fermi tutti gli obblighi, cui sono tenute le P.A., derivanti da altre disposizioni, quali, ad esempio, le «Misure minime di sicurezza ICT per le pubbliche amministrazioni»[59] e successive modifiche e integrazioni.

Art. 23- Sicurezza dei dati raccolti mediante il proprio sito web istituzionale

1. Con riferimento ai dati raccolti mediante il proprio sito web istituzionale, l'Ente incarica fornitori affidabili in grado di adottare soluzioni che garantiscano la riservatezza, la disponibilità e l'integrità dei dati, nonché di

---

[55] Art. 28, par. 1, GDPR.
[56] Art. 28, par. 2, GDPR.
[57] Art. 28, par. 4, GDPR.
[58] Art. 32, GDPR.
[59] Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata in Gazzetta Ufficiale, Serie Generale n. 103 del 5 maggio 2017.

effettuare controlli periodici della sicurezza; gli interessati sono informati ai sensi dell'art. 13, GDPR.

2. Il sito deve essere crittografato con un certificato "Secure Socket Layer" (SSL) e deve utilizzare il linguaggio di markup HTTPS, che permettono trasferimenti di dati in sicurezza; deve, altresì utilizzare le ultime versioni dei browser e dei software e prevedere backup completi e periodici.

3. Con riferimento ai cookie, l'Ente si conforma alle Linee Guida del Garante del 10 giugno 2021[60] e, nello specifico, prevedere gli accorgimenti necessari a: anonimizzare i dati personali ove necessario; ridurre all'indispensabile l'utilizzo di identificatori utente univoci; informare gli utenti sulle categorie di cookie installati nella navigazione del sito.

Art. 24- Audit

1. Al fine di dimostrare la conformità alla normativa vigente, tramite verifiche periodiche (audit), l'Ente, con l'ausilio del RPD/DPO, vigila sull'osservanza dell'applicazione del GDPR, del Codice privacy e del presente Regolamento.

2. All'uopo, l'Ente adotta una procedura di audit (basata sulle norme ISO 19011 e ISO27001), che può svolgersi all'interno dell'Organizzazione del Titolare oppure presso i Responsabili del trattamento, i quali, ai sensi del GDPR, sono tenuti a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da un altro soggetto da questi incaricato[61].

3. Poiché il GDPR stabilisce che tra i compiti del RPD/DPO vi è quello di svolgere attività di sorveglianza e monitoraggio sull'applicazione della normativa[62], anche mediante verifiche programmate, gli audit possono essere condotti sia dal RPD/DPO sia da un Dirigente sia da terze parti.

Art. 25 - Violazione dei dati personali

1. Ai sensi del GDPR, il data breach è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati[63]. Esso consegue a condotte, colpose o dolose, in cui vi è una compromissione della sicurezza dei dati personali pertanto il GDPR, per tali casi, prescrive specifici adempimenti. Possono avvenire tre tipi di violazione (RID), anche in combinazione tra loro: a) violazione di riservatezza (R), quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale; b) violazione di integrità (I), quando si verifica un'alterazione di dati personali non autorizzata o accidentale; c) violazione di disponibilità (D), quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

2. La rilevazione di un evento di data breach può avvenire da diverse fonti (ad es. da un alert automatico, internamente o esternamente all'Ente, ecc.). Allo scopo di disegnare un flusso per la gestione delle violazioni dei dati personali, l'Ente adotta una procedura ad hoc rivolta a tutti i soggetti che, a qualsiasi titolo e livello, trattano dati personali di competenza del Titolare del trattamento, compresi i Responsabili del trattamento, i quali, se vengono a conoscenza di una violazione dei dati personali sono tenuti a informare, senza ingiustificato ritardo, il Titolare, relazionando ad esso e indicando la categoria di dati violati.

3. Al Titolare del trattamento compete la valutazione sulla gravità (severity) della violazione, pertanto, la procedura prevede una prima fase "investigativa" di raccolta delle informazioni sull'evento, nonché una seconda fase in cui l'unità di crisi analizza la natura della violazione dei dati personali e, ove possibile, le categorie dei dati e il loro volume, il numero (anche solo approssimativo) e le categorie degli interessati coinvolti (come prescrive il Gruppo di lavoro dei Garanti europei[64]). Ciò al fine di individuare i possibili rischi per i diritti e le libertà delle persone fisiche, derivanti dal data breach, alla luce dei parametri di gravità degli impatti (G) e probabilità che essi si verifichino (P), anche al fine di adottare nell'immediato le misure necessarie in risposta all'emergenza, con il primario scopo di contenere gli effetti negativi.

---

[60] GARANTE PRIVACY, Provvedimento 10 giugno 2021, n. 231, "Linee guida cookie e altri strumenti di tracciamento" (doc. web n. 9677876, pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021), che aggiorna il precedente Provvedimento dell'8 maggio 2014, n. 229, avente ad oggetto "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie"

[61] Art. 28, par. 3, lettera h), GDPR.

[62] Art. 39, par. 1, lettera b), GDPR.

[63] Art. 4, par. 1, n. 12, GDPR.

[64] WP29, Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679.

4. Raccolte le richiamate evidenze e acquisito il parere del RPD/DPO dell'Ente, questi sono i possibili scenari:

1. Nel caso in cui si ritenga che, anche in forza dell'adozione delle misure di sicurezza correttive adottate, la probabilità che la violazione conduca ad un rischio per i diritti e le libertà degli Interessati classificato come Basso, si provvede unicamente all'aggiornamento del Registro dei Data breach.
2. Ove si evidenzi il caso che la violazione possa condurre ad un rischio per i diritti e le libertà degli interessati, l'Ente si mobilita per circostanziare ed attribuire le responsabilità, dettare i tempi tempistiche per l'adozione delle misure correttive individuate (anche, eventualmente, nei confronti dei Responsabili del trattamento coinvolti), nonché per provvedere all'acquisizione di tutte le informazioni necessarie per la notifica dell'evento al Garante entro 72 ore dall'avvenuta conoscenza, in particolare indicando esplicitamente se le azioni correttive previste sono già concluse o in corso[65]. Successivamente, l'Ente provvede all'aggiornamento del Registro dei Data breach.
3. Nel caso si desuma che la violazione possa comportare un rischio elevato per i diritti e le libertà degli interessati, l'Ente, verificata l'urgenza di comunicare il data breach anche agli interessati, provvede in tal senso senza giustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze derivanti dalla violazione[66]. Successivamente, provvede all'aggiornamento del Registro dei Data breach.

5. Il Titolare documenta ogni violazione dei dati personali, compresi i falsi positivi, mediante verbali delle riunioni previste allo scopo e mediante annotazione degli eventi nel Registro dei Data breach, che resta a disposizione di eventuali ispezioni e verifiche da parte del Garante privacy.

Art. 26 - Analisi del rischio dei trattamenti e valutazione d'impatto sulla protezione dei dati (DPIA)

1. L'Ente adotta apposita procedura per l'analisi del rischio dei vari trattamenti di dati personali (o insiemi di trattamenti similari) per i diritti e le libertà degli interessati nonché per la conseguente, ove il rischio sia elevato, valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment, di seguito solo "DPIA"), atteso che il GDPR stabilisce che, quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali[67].

2. Il trattamento è di per sé a rischio "elevato" (e dunque sussiste la necessità di svolgere la DPIA, per il Titolare) in presenza di casi quali:
– valutazione sistematica di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione e sulla quali si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
– trattamento su larga scala, di categorie particolari di dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, relativi alla salute, alla vita sessuale o condanne penali, a reati e misure di sicurezza;
– sorveglianza sistematica su larga scala di una zona accessibile al pubblico[68].

3. La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli e mitigarli. Si fa riferimento, in tal senso, alle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017, e le raccomandazioni ratione materiae delle autorità di controllo[69].

---

[65] Art. 33, GDPR. La notifica viene effettuata mediante piattaforma presente sul sito web dell'Autorità.
[66] Art. 34, GDPR.
[67] Art. 35, par. 1, GDPR.
[68] Art. 35, par. 3, GDPR.
[69] Art. 35, parr. 4, 5 e 6, GDPR.

4. Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto, ove applicabili, dei principi contenuti nelle pertinenti norme UNI ISO (31000 e 27001) nonché degli orientamenti contenuti nelle Linee guida europee, la DPIA deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione[70].

5. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti[71].

6. Il Titolare, allorquando svolge una DPIA, si consulta con il RPD/DPO. Tale parere, se richiesto, è obbligatorio, ma non vincolante[72]. Il Gruppo di lavoro WP29 ha raccomandato che il Titolare del trattamento si consulti con il RPD/DPO, fra l'altro, sui seguenti temi: se condurre o meno una DPIA (ciò, all'esito dell'analisi del rischio-base, prima di iniziare la DPIA, che potrebbe non essere necessaria); quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne, ovvero esternalizzandola[73].

7. Nella fase di validazione della DPIA, il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio entro limiti di accettabilità) ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento[74].

8. Il Titolare effettua la pubblicazione di una sintesi della DPIA, al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal Titolare, nonché di dimostrare la responsabilizzazione e la trasparenza.

9. Periodicamente, o quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare procede a un aggiornamento della DPIA[75].

CAPO VI - DIRITTI DEGLI INTERESSATI

Art. 27 - Diritti degli interessati

1. Prima che inizi qualunque trattamento di dati personali, il Titolare fornisce all'interessato le informazioni necessarie per consentirgli l'esercizio dei propri diritti[76]. In qualunque momento, gli interessati possono far valere i diritti loro attribuiti dagli articoli da 12 a 22 del GDPR, dei quali il presente regolamento tiene conto. Il Titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti degli interessati, in conformità alla disciplina del GDPR[77] e nel Codice Privacy, anche rendendo disponibili modelli per le diverse richieste. Le modalità di esercizio dei diritti degli interessati, nonché le responsabilità sull'evasione delle richieste, sono esplicate nella procedura per la gestione delle richieste dei medesimi interessati. Il Responsabile del trattamento e i Sub-Responsabili sono tenuti a collaborare con il Titolare per la verifica della sussistenza dei diritti degli interessati.

2. Il Titolare è tenuto a fornire risposta entro 30 giorni dal ricevimento della richiesta, termine che può essere prorogato di due mesi in casi di particolari complessità o ricorra un giustificato motivo, avvisando l'interessato del differimento entro un mese dall'istanza[78].

---

[70] Art. 35, par. 7, GDPR.
[71] Art. 35, par. 9, GDPR.
[72] Art. 35, par. 2, GDPR
[73] Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017.
[74] Art. 36, par. 1, GDPR.
[75] Art. 35, par. 11, GDPR.
[76] Con riferimento agli obblighi informativi, si rinvia all'art. 5 del presente Regolamento.
[77] Art. 12, par. 2, GDPR.
[78] Art. 12, par. 3, GDPR.

3. Qualora l'Ente agisca come un Responsabile del Trattamento è tenuto a inoltrare le richieste di esercizio dei diritti degli interessati al Titolare del Trattamento competente.

4. I diritti riconosciuti agli interessati, per il cui esercizio si rinvia agli articoli da 15 a 22 del GDPR, nonché alla procedura appositamente adottata dal Titolare, sono:

- diritto di accesso ai dati personali[79];
- diritto alla rettifica e alla cancellazione[80];
- diritto di limitazione e obblighi di notifica[81];
- diritto alla portabilità dei dati personali[82];
- diritto di opposizione al trattamento[83];
- diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona[84];
- diritto di proporre reclami[85] e segnalazioni[86] all'autorità di controllo.

5. Le limitazioni ai diritti di cui agli articoli da 12 a 22 del GDPR sono disciplinate nell'art. 23 del Regolamento.

Capo VII – TRATTAMENTI DI DATI PERSONALI PER MEZZO DI SISTEMI DI VIDEOSORVEGLIANZA

Art. 28 - Trattamento di dati personali per mezzo di sistemi di videosorveglianza

1. Il trattamento dei dati personali effettuato dall'Ente mediante l'uso di sistemi di videosorveglianza si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, di conseguenza, l'Ente si conforma al GDPR, al Codice privacy, alla Direttiva UE 2016/680, al Provvedimento in materia di videosorveglianza 08/04/2010 emesso dell'Autorità Garante per la protezione dei dati personali, alle Linee guida dell'European Data Protection Board n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Le immagini catturate dai sistemi di videosorveglianza non sono oggetto di elaborazione tecnica specifica per identificare in modo univoco una persona fisica ("riconoscimento facciale"). Nessuna decisione che possa produrre effetti giuridici nei confronti dell'interessato è basata sul trattamento automatizzato dei dati che lo riguardano, né sono effettuate attività di profilazione.

2. La finalità dell'installazione di sistemi di videosorveglianza è la tutela del patrimonio dell'Ente (veicoli, locali, ecc.) sia mediante la prevenzione di fatti illeciti, attraverso l'azione di deterrenza, che la presenza del sistema di videosorveglianza esercita a prescindere, sia per consentire la ricostruzione, in tempo reale, della dinamica dei fatti, permettendo un pronto intervento, ove possibile.

3. Il Sistema di videosorveglianza si compone di un numero variabile di telecamere dislocate nei pressi e all'interno degli immobili dell'ARSAC, nonché degli schermi ubicati nei luoghi di pertinenza dell'ARSAC.

4. Le immagini, eventualmente acquisite, inerenti all'attività lavorativa del personale non potranno essere utilizzate ai fini disciplinari, così come le apparecchiature mobili non potranno servire per il controllo a distanza del rispetto degli obblighi di diligenza dei lavoratori medesimi. L'utilizzo di detti impianti di videosorveglianza dovrà in ogni caso essere conforme ai dettami dello Statuto dei Lavoratori[87].

---

[79] Art. 15, GDPR.
[80] Artt. 16 e 17, GDPR.
[81] Artt. 18 e 19, GDPR.
[82] Art. 20, GDPR.
[83] Art. 21, GDPR.
[84] Art. 22, GDPR.
[85] Art. 77, GDPR e artt. 140-bis e 142, Codice privacy.
[86] Art. 144, Codice Privacy.
[87] Art. 4, St. lav.: «1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.»

5. I sistemi di videosorveglianza, nel pieno rispetto dei principi di liceità, finalità, necessità e proporzionalità sanciti dalla normativa a tutela dei dati personali, comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area videosorvegliata. L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando quando, non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa sono quindi stabilite in modo conseguente.

Art. 29 - Base giuridica del trattamento per mezzo di sistemi di videosorveglianza

La base giuridica del trattamento mediante videosorveglianza è costituita dall'art. 6, par. 1, lett. e), GDPR "Compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", ossia la protezione del patrimonio dell'ARSAC.

Art. 30 - Ruoli e responsabilità nel trattamento dei dati raccolti per mezzo di sistemi di videosorveglianza

1. Titolare del trattamento dei dati è l'ARSAC, che, come tale, ha la piena responsabilità delle decisioni circa le finalità e i mezzi del trattamento[88]. Tuttavia, ai fini del GDPR, tale responsabilità può essere attribuita a un Dirigente (soggetto Delegato al trattamento per specifici compiti e funzioni) che ha potere amministrativo decisionale sul funzionamento e sulla gestione del sistema.

2. Il Soggetto Delegato è responsabile del coordinamento delle attività, della tenuta della documentazione tecnica del sistema, dello svolgimento della DPIA e della tenuta del registro dei trattamenti con il supporto del RPD/DPO, della nomina dei soggetti autorizzati alla visione delle immagini, delle attività conseguenti ad eventuali istanze da parte degli interessati (ad es. istanza di blocco delle immagini, istanza di accesso ai dati, ecc). Nei vari Centri ARSAC, la gestione delle telecamere di videosorveglianza può essere affidata dal Soggetto Delegato ad altri dipendenti, opportunamente nominati quali "soggetti autorizzati". Tali soggetti si occupano della tenuta del registro degli accessi alle immagini (in cui sono riportati l'identificazione del terzo autorizzato, gli estremi e la motivazione dell'autorizzazione all'accesso, la data e l'ora dell'accesso) e della custodia dei locali e delle immagini, comprese le parole chiave per l'utilizzo dei mezzi e dei materiali nell'ambito delle competenze loro affidate. L'accesso alle immagini, in ogni caso, deve essere motivato. Eventuali accessi di persone diverse devono essere autorizzati, per iscritto, dal soggetto Delegato dal Titolare.

3. Ove la società fornitrice del servizio di installazione e manutenzione del sistema abbia accesso alle immagini, essa assume il ruolo di Responsabile del trattamento[89], pertanto, si applica l'articolo 21 del presente Regolamento.

Art. 31 - Informazioni rese al momento della raccolta

Poiché i soggetti interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata (anche in occasione di eventi pubblici o aperti al pubblico), l'Ente, prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti, affigge adeguata segnaletica (informativa "di primo livello") su cui sono riportate informazioni sintetiche sulle finalità del trattamento e i tempi di conservazione, nonché i dati di contatto del Titolare e del RPD/DPO. Il cartello ha un formato e un posizionamento tali da essere chiaramente visibile in ogni condizione di illuminazione ambientale e ingloba altresì il simbolo della telecamera. Tale segnaletica rinvia, anche mediante QR Code, all'informativa di II livello presente sul sito web istituzionale dell'Ente, i cui requisiti devono rispettare quanto previsto nell'art. 5 del presente Regolamento.

Art. 32 - Comunicazione dei dati personali a soggetti terzi e accertamenti di illeciti ed indagini giudiziarie o di polizia

1. Ai sensi del presente articolo, non si considera comunicazione la conoscenza dei dati personali da parte delle persone autorizzate per iscritto a compiere le operazioni del trattamento dal Titolare o dal Responsabile e che operano sotto la loro diretta autorità.

2. In caso di rilevazioni di immagini di fatti concernenti ipotesi di reato o di altri eventi rilevanti ai fini della pubblica sicurezza, della tutela ambientale o del patrimonio pubblico, il soggetto Delegato competente

[88] Cfr. art. 14 del presente Regolamento.
[89] Cfr. art. 21 del presente Regolamento.

provvederà a darne comunicazione senza ritardo all'Autorità competente, provvedendo, nel contempo, al blocco delle immagini su appositi supporti, per evitare la sovrascrittura delle stesse.

3. La comunicazione dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento, da parte dell'Ente a favore di altri soggetti pubblici, esclusi gli enti pubblici economici, è ammessa, altresì, quando è prevista da una norma di legge o regolamento specifica, e, in mancanza, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali connesse alle finalità per le quali è stato installato l'impianto.

4. È in ogni caso fatta salva la comunicazione dei dati richiesti, in conformità alla legge, a Forze di Polizia, all'Autorità Giudiziaria, a organismi di informazione e sicurezza o altri soggetti pubblici ai sensi di quanto disposto dal D.lgs. n. 51/2018 (Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016), per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati e ai sensi dell'art. 58, comma 2, del decreto legislativo n. 196 del 30 giugno 2003 e s.m.i. Qualora gli organi di Polizia, nello svolgimento dei loro compiti istituzionali, necessitino di una copia delle riprese effettuate, devono presentare un'istanza scritta, dettagliata e motivata indirizzata all'Ente, che rilascerà, ove ammesso, copia delle immagini.

5. Alle immagini, tuttavia, possono accedere soltanto gli appartenenti all'Amministrazione Giudiziaria, le persone da essi espressamente autorizzate e gli organi di Polizia.

6. Dal momento in cui le immagini vengono comunicate ad altri soggetti, essi assumono il ruolo di autonomi titolari del trattamento dei dati personali. In ogni caso, l'acquisizione dei dati da parte delle forze di Polizia deve avvenire in conformità alle disposizioni normative[90].

7. La diffusione dei dati personali non è prevista in alcun caso.

Art. 33 - Tempi di conservazione dei dati raccolti per mezzo di sistemi di videosorveglianza

1. Come imposto dall'art. 5, par. 1, lett. c) ed e), GDPR, al fine di garantire un trattamento corretto e trasparente, i dati vengono conservati per un termine massimo di ventiquattro ore (o quarantott'ore in presenza di adeguata motivazione) 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 debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

2. Con riferimento alla comunicazione dei dati raccolti disciplinata nell'art. 32 del presente Regolamento, tali dati non soggiacciono alle regole di conservazione pocanzi richiamate ma al dettato dell'art. 3, comma 1, lettera e), del D.lgs. n. 51/2018 («conservati con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico per verificarne la persistente necessità di conservazione, cancellati o anonimizzati una volta decorso tale termine»).

3. Trascorsi tali termini, i dati vengono automaticamente sovrascritti, salvo che non ne sia necessaria la conservazione per i casi di blocco o per altre e diverse finalità previste per espressa previsione di legge.

Art. 34 - Sicurezza dei dati raccolti per mezzo di sistemi di videosorveglianza

1. Con riferimento ai dati raccolti mediante sistemi di videosorveglianza, l'Ente applica le Linee Guida n. 3/2019 dell'European Data Protection Board[91], vigilando sulla protezione dei medesimi dati con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.

2. L'Ente applica i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa. Non sono attivate funzioni che non siano necessarie, quali, ad esempio, movimento illimitato delle telecamere, capacità di zoom, trasmissione radio, analisi e registrazioni audio.

3. L'Ente si impegna ad adottare, ove possibile, le seguenti specifiche misure tecniche ed organizzative:

---

[90] Cfr. Garante privacy, Parere n. 13588/2019 (Provincia di Brescia).

[91] Linee Guida dell'EDPB n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0, adottata il 29 gennaio 2020.

- è limitata ai casi necessari la possibilità, per i soggetti abilitati, di visionare, sia in diretta sia in differita, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- nel caso di interventi derivanti da esigenze di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
- qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi sono protetti contro i rischi di accesso abusivo;
- nel rispetto dell'art. 28.5 del presente Regolamento, non sono effettuate riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato;
- l'utilizzo del brandeggio e dello zoom da parte degli operatori autorizzati al trattamento deve essere conforme alle finalità dell'impianto;
- il settore di ripresa delle telecamere deve essere impostato in modo tale da consentire il controllo e la registrazione di quanto accada nei luoghi pubblici o aperti al pubblico, con esclusione delle proprietà private;
- i segnali video delle unità di ripresa possono essere raccolti in Centrali Operative, in cui sono visualizzate su monitor e registrate su supporto magnetico da un sistema appositamente predisposto al fine di ricostruire le varie fasi dell'evento quando la sala di controllo non sia presidiata, oppure nel caso in cui si renda necessario il riesame dei fotogrammi sfuggiti alla percezione oculare dell'addetto alla Centrale per qualsiasi motivo;
- fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui all'art. 33 del presente Regolamento, solo in caso di effettiva necessità per il conseguimento delle finalità istituzionali e a seguito di regolare autorizzazione di volta in volta richiesta al soggetto competente; la mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali;
- il sistema è fornito di vari "log" di accesso, da cui si può evincere l'orario di accesso e uscita dal sistema, che devono essere conservati almeno per un anno;
- i "server" di registrazione sono protetti, mediante misure di sicurezza tecniche, da ogni possibile rischio di distruzione, di perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini;
- i dati personali oggetto di trattamento sono custoditi nei sistemi di registrazione di proprietà delle Centrali Operative o di altri soggetti autorizzati collegati;
- i monitor degli impianti di videosorveglianza presso le Centrali Operative devono essere collocati in modo tale da non permettere la visione delle immagini, neanche occasionalmente, a persone estranee non autorizzate;
- l'accesso alle immagini da parte dei soggetti autorizzati al trattamento dei dati si limita alle attività oggetto della sorveglianza; eventuali altre informazioni di cui costoro dovessero venire a conoscenza mentre osservano il comportamento di un soggetto ripreso non devono essere prese in considerazione;
- nel caso le immagini siano conservate, i relativi supporti vengono custoditi, per l'intera durata della conservazione, in un armadio o simile struttura dotato di serratura, cui possono avere accesso soltanto i soggetti autorizzati;
- la cancellazione automatica delle immagini videoriprese, dopo il periodo stabilito per la loro conservazione, è garantita mediante gli strumenti e le procedure tecnologiche più avanzate; le operazioni di cancellazione devono essere effettuate esclusivamente sul luogo di lavoro;
- nel caso il supporto debba essere sostituito per eccessiva usura, viene distrutto in modo da renderlo inutilizzabile, in modo che non possano essere recuperati i dati in esso presenti;
- nel caso di accesso ai dati da parte dell'interessato questi ha visione solo delle immagini che lo riguardano direttamente e non può accedere a immagini che ritraggono altre persone;
- non possono, di norma, essere rilasciate copie delle immagini registrate concernenti altri soggetti diversi dall'interessato, valutando altresì l'opzione di ricorrere ad un programma oscuratore ("pixellaggio").

Art. 35 – Diritti degli interessati

1. Gli interessati cui i dati raccolti dai sistemi di videosorveglianza si riferiscono hanno i diritti riconosciuti dal GDPR (in tal senso, si rinvia all'art. 27 del presente Regolamento). Le peculiarità dell'esercizio di tali diritti, per i casi di dati raccolti mediante sistemi di videosorveglianza, sono le seguenti:

- con riferimento al diritto di accesso, agli Interessati è riconosciuto il diritto di accesso alle immagini della videosorveglianza in cui compare la loro persona, nei limiti di cui alle Linee Guida dell'EDPB n. 3/2019 (p. 6.1); al fine di garantire tale diritto, è previsto che le richieste di accesso vengano immediatamente trasmesse al soggetto che si occupa della conservazione dei filmati, di modo che questi possa estendere il tempo di conservazione delle immagini oggetto di richiesta, al fine di permettere all'Ente di meglio valutare la richiesta medesima e procedere l'applicazione delle tecniche consentite dal sistema eventualmente necessarie a tutelare altri soggetti interessati che compaiono nei video richiesti;
- con riferimento ai diritti di portabilità, di rettifica e di cancellazione dei dati, tali diritti non sono riconosciuti, non sussistendone i presupposti di cui al GDPR;
- con riferimento ai diritti di limitazione, è previsto che le richieste in tal senso vengano immediatamente trasmesse al soggetto che si occupa della conservazione dei filmati, di modo che questi possa limitare il tempo di conservazione delle immagini oggetto della richiesta.
- con riferimento al diritto di opposizione, in linea generale non è previsto il riconoscimento del diritto di opposizione, sussistendo motivi legittimi cogenti per procedere al trattamento, in considerazione delle finalità di interesse pubblico perseguite e della necessità e proporzionalità del trattamento medesimo, tuttavia, le richieste in tal senso verranno comunque prese in considerazione.

2. L'istanza deve indicare a quale impianto di videosorveglianza si fa riferimento ed il giorno e l'ora in cui l'interessato potrebbe essere stato oggetto di ripresa: nel caso tali indicazioni manchino, o siano insufficienti a permettere il reperimento delle immagini, di ciò deve essere data comunicazione al richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione.

3. Il soggetto Delegato competente è tenuto ad accertare l'effettiva esistenza delle immagini e di ciò da comunicazione al richiedente; nel caso di accertamento positivo fissa altresì il giorno, l'ora ed il luogo in cui il suddetto può visionare le immagini che lo riguardano.

4. La risposta alla richiesta di accesso a dati conservati deve essere inoltrata entro quindici giorni dalla ricezione e deve riguardare i dati attinenti alla persona richiedente e può comprenderne eventualmente altri, riferiti a terzi, soltanto nei limiti previsti dalla normativa vigente.

5. I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute, possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.

CAPO VIII - MEZZI DI TUTELA E RESPONSABILITÀ. DISPOSIZIONI FINALI

Art. 36 – Mezzi di tutela

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il diritto di proporre reclamo a un'Autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione. L'Autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78, GDPR[92].

2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda[93].

3. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, GDPR, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del GDPR siano stati violati a seguito di un trattamento. Le azioni nei confronti del Titolare o del Responsabile sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il Titolare o il Responsabile ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle

[92] Art. 77, GDPR.
[93] Art. 78, GDPR.

autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il Titolare o il Responsabile sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri[94].

Art.37 - Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

1. Il mancato rispetto delle disposizioni in materia di protezione dei dati personali può essere oggetto, a diversi livelli e in diversi ambiti, secondo quanto previsto dal Codice Privacy[95] e dal GDPR[96], delle sanzioni dell'Autorità Giudiziaria, dell'Autorità Garante per la protezione dei dati personali, nonché di sanzioni di natura disciplinare.

2. Chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento. Un Titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il GDPR. Un Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare. Il Titolare e il Responsabile vanno esenti da responsabilità se provano che l'evento dannoso non è loro imputabile[97].

3. Il RPD/DPO non risponde nei confronti dei danneggiati ma solo nei confronti del Titolare ed in relazione alle specifiche competenze attribuite al momento del conferimento dell'incarico e con successivi accordi scritti.

Art. 38- Disposizioni finali

1. Per quanto non previsto nel presente Regolamento si applicano le disposizioni del Codice e del GDPR, nonché le Linee guida e i Provvedimenti del Garante.

2. Il presente Regolamento entra in vigore dalla data di esecutività dell'atto con cui viene approvato e abroga tutte le disposizioni che risultino incompatibili con le norme in esso previste.

3. Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.

4. Il Regolamento è reso pubblico mediante pubblicazione sul sito web istituzionale dell'Ente, all'Albo Pretorio on-line e nella Sezione Amministrazione Trasparente; della sua entrata in vigore viene informato tutto il personale dell'Ente.

---

[94] Art. 79, GDPR.

[95] Cfr. articoli da 160 a 172 del Codice Privacy, come modificato, da ultimo, dal Decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali.

[96] Art. 83, GDPR.

[97] Art. 82, GDPR.