COMUNE DI SAN VERO MILIS

Provincia di Oristano

Via Eleonora D'Arborea n. 5 – C.a.p. 09070 – P.I.: 00068380955

www.comune.sanveromilis.or.it

REGOLAMENTO SULLA PROTEZIONE DEI DATI PERSONALI ADOTTATO IN ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679 "GDPR"

(General Data Protection Regulation)

Approvato con deliberazione C.C. n. 17 in data 19/06/2023

SOMMARIO

INTRODUZIONE

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati o "GDPR"), con contestuale abrogazione della cd. "Direttiva Madre" 95/46/CE.
Il nuovo regolamento UE, che si applica negli Stati membri a decorrere dal 25 maggio 2018, si fonda sulla affermazione che la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, sia un diritto fondamentale, come risulta anche dalla circostanza che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea (TFUE) stabiliscano che ogni persona abbia diritto alla protezione dei dati di carattere personale che la riguardano.
Per rafforzare la protezione il GDPR introduce numerose e rilevanti novità, partendo da un approccio fondato sul principio di cautela basato sul rischio del trattamento e su misure di "accountability" di titolari e responsabili, come la valutazione di impatto, il registro dei trattamenti, le misure di sicurezza, la nomina di un RDP-DPO.
Come ha evidenziato il Garante nella guida all'applicazione del Regolamento[1], la nuova disciplina europea pone con forza l'accento sulla "responsabilizzazione" (cd. "accountability") di titolari e responsabili, ossia sull'adozione di comportamenti proattivi che dimostrino la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.
Tra i criteri che i titolari e i responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono:
- il criterio del "data protection by design and by default", ai sensi dell'art. 25 GDPR[2], ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo e dei rischi per i diritti e le libertà degli interessati;
- il criterio del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà ed i diritti degli interessati: impatti che devono essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.
Ne consegue che l'intervento delle autorità di controllo, nel nuovo impianto gestionale, è destinato a svolgersi principalmente "ex post", ossia si colloca successivamente alle determinazioni assunte autonomamente dal Titolare; ciò spiega l'abolizione, a partire dal 25 maggio 2018, di alcuni istituti previsti dalla direttiva del 1995 e dal Codice privacy di cui al D.Lgs. 196/2003 nella sua versione ante D.Lgs. 101/2018, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto "prior checking" (o verifica preliminare), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del Titolare/Responsabile e, appunto, dalla effettuazione di analisi dei rischi e valutazioni di impatto in piena autonomia.
Dall'esame della materia emerge come sia oramai imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non come un oneroso e farraginoso adempimento burocratico, ma piuttosto come una garanzia ed un presidio per il cittadino che si rivolge alla Pubblica Amministrazione.
Il diritto alla privacy è un diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità della persona. Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori delle pubbliche amministrazioni, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa

[1] https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali.
[2] Vedi anche Linee Guida EDPB n. 4/2019: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

potranno essere svolti correttamente tutti gli adempimenti di legge, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.
Pertanto, il Comune di San Vero Milis intende adeguare e conformare la propria normativa regolamentare alle novità introdotte dal succitato GDPR e dalla nuova versione del "Codice privacy" (D.lgs. 196/2003, come novellato dl D.Lgs. 101/2018 e, da ultimo, dalle novità introdotte dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205 e dal decreto-legge 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178) – d'ora in poi "Normativa Privacy" - fermo restando che il presente aggiornamento è destinato ad essere ulteriormente revisionato in presenza di sopravvenienza di linee guida del Garante per la Protezione dei Dati personali o dell'EDPB, o novità normative e giurisprudenziali.

OBIETTIVI DEL DOCUMENTO

Il presente Regolamento definisce la portata e l'attuazione della Normativa Privacy all'interno del Comune di San Vero Milis: esso, in particolare, delinea un sistema organico e strutturato di gestione di tutti gli aspetti concernenti i profili "privacy" attraverso un modello di gestione uniforme, fornendo ai soggetti che di tale sistema fanno parte indicazioni chiare, sia sul piano tecnico/operativo che sul piano organizzativo, sulle modalità di applicazione della Normativa Privacy.
Il presente documento, pertanto:
- definisce i requisiti per il trattamento dei dati personali, affinché esso avvenga, all'interno del quadro delineato dalla Normativa Privacy, nel rispetto delle prescrizioni previste dalla normativa stessa e individua, disciplinandone le modalità, gli adempimenti da porre in essere per garantire la conformità alla normativa in parola;
- fornisce indicazioni sulle modalità di trattamento dei dati personali;
- individua le misure tecniche ed organizzative che l'Ente adotta per garantire ed essere in grado di dimostrare la conformità alla Normativa Privacy delle attività di trattamento dei dati delle persone fisiche;
- disciplina i ruoli e le responsabilità in modo da evitare la possibile irrogazione delle sanzioni amministrative pecuniarie.
Le presenti Linee Guida sono rivolte a tutto il personale del Comune (dipendente e non dipendente).
Il presente documento è da considerarsi ad uso interno e sarà pubblicato sulla rete intranet del Comune, in modo tale da risultare accessibile esclusivamente ai dipendenti.
Obiettivo ulteriore del presente documento è quello, di concerto con le attività formative che verranno poste in essere, di innalzare la cultura di una corretta e sicura gestione dei dati personali e consentire il rispetto e l'effettiva operatività del Sistema di gestione privacy qui delineato.
Viene dunque proposto un regolamento che descrive i ruoli e le responsabilità dei soggetti coinvolti nel trattamento dei dati personali.

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Definizioni

1. Ai fini del presente Regolamento si intende per:

a) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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

c) "dati particolari": dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché la trattazione di 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 (art. 9 GDPR).

d) "dati giudiziari": dati personali relativi alle condanne penali e ai reati e alle connesse misure di sicurezza (art. 10 GDPR);

e) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

f) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi dell'art. 28 GDPR (n.b.: soggetto esterno rispetto all'Ente);

g) "designati di I livello" (ex "responsabili interni del trattamento"): P.O. autorizzate a compiere operazioni di trattamento di dati personali dal titolare ai sensi degli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003;

h) "autorizzati di II livello" (ex "incaricati"): il dipendente della struttura organizzativa del Comune, appositamente nominato ed istruito, ai sensi degli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003, al fine di eseguire specifiche attività di trattamento per conto del titolare del trattamento;

i) "interessato": la persona fisica, cui si riferiscono i dati personali (es: cittadino, paziente ecc.);

l) "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

m) "terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

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

o) "dato anonimo": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
p) “archivio”: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
q) “violazione dei dati personali”: la 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;
r) "Garante": l’Autorità di controllo che, nel caso dell’Italia, è l’Autorità Garante per la Protezione dei Dati Personali, con sede a Roma[3];
s) “profilazione”: qualsiasi forma di trattamento automatizzato di dati personali consistente nell’utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l’affidabilità, il comportamento, l’ubicazione o gli spostamenti di detta persona fisica;
t) “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (es: numero di protocollo).

Art. 2 – Quadro normativo di riferimento
Il presente Regolamento tiene conto dei seguenti documenti:
- Regolamento europeo n. 2016/679 GDPR 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, che abroga la direttiva 95/46/CE[4];
- Codice in materia di dati personali (D.Lgs. n. 196/2003, come novellato dal D.Lgs. 101/2018 e, da ultimo, dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205 e dal decreto-legge 30 settembre 2021, n. 132, convertito, con modificazioni, dalla legge 23 novembre 2021, n. 178)[5];
- D.Lgs. n. 101 del 10 agosto 2018 di adeguamento della normativa interna al GDPR[6];
- Norme internazionali e unionali;
- Linee guida, Provvedimenti e Raccomandazioni del Garante;
- Linee Guida del “Gruppo Articolo 29” (ex WP29);
- Linee-guida dell’EDPB (European Data Protection Board)[7];
- Regolamenti interni.

Art. 3 – Oggetto
Il presente Regolamento ha per oggetto la protezione dei diritti e delle libertà delle persone fisiche in ordine al trattamento dei dati personali effettuato dal titolare del trattamento, Comune di San Vero Milis, con sede in San Vero Milis, Via Eleonora d’Arborea n. 5, PEC: protocollo@pec.comune.sanveromilis.or.it nel rispetto di quanto previsto dalla Normativa Privacy.

Art. 4 – Finalità
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

[3] https://www.garanteprivacy.it.
[4] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597.
[5] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678.
[6] https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.
[7] https://edpb.europa.eu/edpb_en.

riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
Il titolare, nell'ambito delle sue funzioni, gestisce gli archivi e le banche dati rispettando i diritti, le libertà fondamentali e la dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale.
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, vanno gestiti conformemente alle disposizioni del GDPR, del Codice privacy e del presente Regolamento.

CAPO II – PRINCIPI

Art. 5 – Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del GDPR e, in particolare, quelli elencati nell'art. 5 GDPR, per effetto dei quali i dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non 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");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, nel rispetto del principio di "minimizzazione dei dati";
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di "esattezza");
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato, in base al principio di "limitazione della conservazione";
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza");
g) 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 permettano di identificare l'interessato solo in caso di necessità ("principio di necessità").
Il titolare è competente per il rispetto dei sopraindicati principi, ed è in grado di comprovarlo in base al principio di "responsabilizzazione" (cd. "accountability") di cui agli artt. art. 5 par. 2 e 24 del GDPR[8].

Art. 6 – Liceità del trattamento

Vengono integralmente recepiti, nell'ordinamento interno del titolare, le disposizioni del GDPR in odine alla liceità del trattamento e, per l'effetto, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

[8] https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili.

a) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c, GDPR);
b) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento (art. 6, par. 1, lett. e, GDPR).
Infatti, come ha avuto modo di ribadire l'Autorità Garante per la Protezione dei Dati personali "*i soggetti pubblici possono trattare dati personali solo se "il trattamento è necessario" per "adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (art. 6, par. 1, lett. c), del Regolamento) o per "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, par. 1, lett. e), del Regolamento). Tali trattamenti devono, comunque, trovare fondamento nel diritto dell'Unione o dello Stato membro, che, deve perseguire un obiettivo di interesse pubblico ed essere proporzionato al perseguimento dello stesso. La finalità del trattamento deve essere necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (cfr. art. 6, par. 3, del Regolamento e 2-ter del Codice). Giova, inoltre, ricordare che il consenso non è una condizione di liceità ammissibile nei trattamenti posti in essere dai soggetti pubblici (con. 43 del Regolamento).*"
Per i dati particolari (dati "sensibili e sensibilissimi" secondo la vecchia nomenclatura), il trattamento è lecito se "il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che 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" (art. 9, par. 2, lett. g, GDPR).
Ulteriori basi di liceità sono previste per il trattamento dei dati dei dipendenti da parte del datore di lavoro (es: legittimo interesse). In casi residuali, infine, possono trovare applicazioni altre basi di liceità.

Art. 7 – Consenso
Poiché il considerando 43 del GDPR prevede che "*Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica*", il Titolare del trattamento, anche al fine di evitare contestazioni e reclami/segnalazioni da parte degli interessati, si adopera affinché dalla modulistica dell'Ente venga rimossa tale base di liceità in relazione ai trattamenti di dati personali connessi ai procedimenti amministrativi dell'Ente.
Inoltre, come ribadito in più occasioni dall'Autorità Garante, il consenso non può costituire base di liceità per il trattamento dei dati dei lavoratori.

Art. 8 – Informativa
Il titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale designato/autorizzato, apposita informativa sul trattamento dei dati personali secondo le modalità previste dagli artt. 13 e 14 del 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.
L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online (es: andrà pubblicato un pdf separato denominato "informativa privacy" o "informativa sul trattamento dei dati personali").
L'informativa è fornita, mediante idonei strumenti:
• attraverso appositi moduli da consegnare agli interessati (es: in calce al modulo/istanza). Nel modulo sono indicati i soggetti a cui l'interessato può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, in particolare il titolare del trattamento ed il DPO nominato;

• 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 ovvero diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet istituzionale 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 di bandi, avvisi, lettere d'invito, con l'indicazione dell'autorizzato al trattamento dei dati relativi alle procedure.

L'informativa privacy ai sensi dell'art. 13 GDPR non può essere fornita dopo che si è proceduto alla raccolta/acquisizione dei dati personali presso l'interessato, in quanto quest'ultimo deve essere messo in grado di conoscere "prima" di conferire i dati all'Ente in che modo gli stessi verranno trattati dal titolare del trattamento.

L'informativa da fornire agli interessati può essere fornita anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico[9].

L'informativa contiene il seguente contenuto minimo:

• l'identità e i dati di contatto del titolare e, ove presente, del suo rappresentante;
• i dati di contatto del RPD/DPO;
• le finalità del trattamento;
• i destinatari dei dati;
• la base di liceità/giuridica del trattamento;
• se il titolare trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
• il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
• i diritti degli interessati di cui agli artt. 12-22 GDPR;
• il diritto di presentare un reclamo all'autorità di controllo;
• l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze di tale trattamento per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 GDPR):

a) il titolare deve informare l'interessato in merito a:

- le categorie di dati personali trattati;
- fonte da cui hanno origine i dati personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;

b) l'informativa ai sensi dell'art.14 GDPR deve essere fornita entro un termine ragionevole che non può superare un mese (1 mese) dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del titolare è predisposta apposita informativa per il personale dipendente.

Apposite informative devono essere inserite nei seguenti documenti:

- nei bandi e nella documentazione di affidamento dei contratti pubblici, nei contratti, accordi o convenzioni, nei bandi di concorso pubblico, nelle segnalazioni di disservizio e, più in generale, in ogni altro documento contenente dati personali.

Nel fornire l'informativa, il titolare fa espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati particolari e giudiziari.

Per evitare contestazioni con gli interessati, il titolare del trattamento si assicurerà che, nel caso in cui l'informativa venga fornita tramite modulo separato (quindi non in calce ad un modulo/istanza),

[9] https://www.garanteprivacy.it/temi/informativechiare.

la stessa venga firmata, con luogo e data, “per presa visione”, dall’interessato (n.b.: non consenso o “autorizzo al trattamento dei dati personali”).

Art. 9 – Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa alla protezione dei dati personali, il titolare sostiene e promuove all’interno della propria struttura organizzativa, con la cooperazione del DPO nominato, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati.

A tale riguardo, il presente regolamento riconosce che uno degli strumenti essenziali di sensibilizzazione è l’attività formativa del personale del titolare e l’attività informativa diretta a tutti coloro che abbiano rapporti con il titolare.

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 tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale.

Il dipendente si impegna ad acquisire copia del Regolamento, prenderne visione ed attenersi alle sue prescrizioni.

Il titolare organizza, nell’ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento, con cadenza almeno annuale, in materia di protezione dei dati personali, finalizzati 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 delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata, a cura del RPCT, con la formazione in materia di prevenzione della corruzione e della illegalità nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera il titolare.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale e verrà appositamente mappata mediante appositi verbali con l’elenco dei dipendenti/collaboratori che vi abbiano preso parte. Sarà cura del Titolare verificare e monitorare la partecipazione alle giornate formative previste, tenendo conto del fatto che non vi può essere personale in servizio che non abbia ricevuto adeguata formazione in materia.

CAPO III – IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 – Trattamento dei dati personali, ricognizione dei trattamenti ed elenco dei trattamenti

Il titolare tratta i dati personali per lo svolgimento delle proprie finalità istituzionali, come identificate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal GDPR, dal Codice privacy e dalle Linee Guida e dai provvedimenti del Garante e dell’EDPB.

Il titolare effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo:

• la gestione del personale dipendente, ivi comprese le procedure di assunzione;

• la gestione 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, i tirocinanti ed i volontari;

• la gestione dei rapporti con i consulenti, i liberi professionisti, i fornitori per l’approvvigionamento di beni e di servizi, nonché con le imprese per l’esecuzione di lavori, opere ed interventi di manutenzione;

• la gestione dei rapporti con i soggetti accreditati o convenzionati per i servizi socio-assistenziali;
• la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi ed ai regolamenti.
Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, solo da parte dei seguenti soggetti:
• Sindaco;
• Segretario Generale/Comunale;
• Assessori/Consiglieri comunali, nei limiti previsti dalla normativa;
• Responsabili di P.O., in qualità di soggetti che esercitano i poteri delegati dal titolare in qualità di soggetti designati al trattamento;
• Dipendenti, in qualità di autorizzati al trattamento;
• tirocinanti/stagisti/collaboratori, espressamente autorizzati al trattamento.
Non è consentito il trattamento da parte di persone non autorizzate.
Ai fini del trattamento, il titolare provvede, in collaborazione con le P.O., alla integrale ricognizione e all'aggiornamento di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti del titolare medesimo, funzionali alla formazione dell'elenco dei trattamenti.
Fermo restando l'obbligo di aggiornamento "dinamico" del Registro dei trattamenti ex art. 30, par. 1, GDPR (ossia continuo, come nel caso di introduzione di un nuovo trattamento, quale ad es.: la rilevazione della temperatura a seguito dell'emergenza Covid-19, l'implementazione di un sistema di videosorveglianza ecc., o la modifica dell'organigramma dell'Ente, del DPO nominato ecc.), è compito delle P.O. provvedere e collaborare con il referente privacy nominato dall'Ente e con il DPO all'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo elenco.
Il titolare, le P.O. e gli autorizzati si attengono alle modalità di trattamento indicate nel GDPR, nel Codice, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali.

Art. 11 – Tipologie di dati trattati
Nell'ambito dei trattamenti inclusi nell'elenco dei trattamenti, il titolare, nell'esercizio delle sue funzioni istituzionali, tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:
• dati comuni (es: dati anagrafici e di contatto ecc.)
• dati particolari di cui all'art. 9 GDPR (ex dati sensibili e sensibilissimi, come quelli di salute ecc.)
• dati giudiziari di cui all'art. 10 GDPR (es: casellario giudiziale, carichi pendenti ecc.)

Art. 12 – Trattamento dei dati particolari e giudiziari
Il titolare conforma il trattamento dei dati particolari e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. A tale fine, il titolare applica i principi e le pertinenti disposizioni del GDPR e del Codice privacy e si conforma alle Linee Guida del Garante e dell'EDPB in materia.
Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati particolari e giudiziari[10].

Art. 13 – Trattamento dei dati del personale
Il titolare tratta i dati, anche di natura particolare e giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.

[10] Vedi questo documento: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9124510.

Tra tali trattamenti sono compresi quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, di adempiere agli obblighi connessi alla definizione dello stato giuridico od economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili, relativamente al personale in servizio o in quiescenza.
Secondo la normativa vigente, il titolare adotta le massime cautele nel trattamento di informazioni personali del proprio personale dipendente che siano idonee a rivelare lo stato di salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose filosofiche o d'altro genere e l'origine razziale ed etnica.
Il trattamento dei dati particolari del dipendente, da parte del datore di lavoro, 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 dei dati giudiziari e particolari, di trattare solo le informazioni che si rivelino indispensabili per la gestione del rapporto di lavoro.
La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando diciture generiche o codici numerici. Non sono infatti 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, 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 natura particolare.
Il titolare, nel trattamento dei dati particolari relativi alla salute dei propri dipendenti, deve rispettare i principi di necessità e indispensabilità.
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 – 14 giugno 2017 (G.U. 13 luglio 2007, n. 161)[11].

Art. 14 – Registro delle attività di trattamento

Il titolare del trattamento, ai sensi dell'art. 30 par. 1 GDPR, ha istituito un registro delle attività di trattamento svolte sotto la propria responsabilità[12].
Il registro è continuamente aggiornato, almeno con cadenza annuale, affinché possa essere messo a disposizione dell'Autorità di controllo o della Guardia di Finanza – Nucleo Speciale Privacy e Frodi tecnologiche nel caso di una ispezione/controllo/richiesta di esibizione.
Infatti, come precisato dall'Autorità Garante "*Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile. In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.*
Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:
"- scheda creata in data XY"
"- ultimo aggiornamento avvenuto in data XY"

[11] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1417809.
[12] Accessibile tramite il software privacy in cloud DPM al seguente url: https://sanveromilis.privacymanager.eu

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (art. 30, par. 1 del GDPR) e in quello del responsabile (art. 30, par. 2 del GDPR).
Con riferimento ai contenuti si rappresenta quanto segue:
(a) per ciò che concerne le "finalità del trattamento" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. art. 6 del GDPR; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare (v. provvedimento del Garante del 22 febbraio 2018 – [doc web n. 8080493]). Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'art. 9, par. 2 del GDPR; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del GDPR;
(b) per ciò che concerne la "descrizione delle categorie di interessati e delle categorie di dati personali" andranno specificate sia le tipologie di interessati (es. cittadini, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati relativi a condanne penali o reati, ecc.);
(c) per ciò che concerne le "categorie di destinatari a cui i dati sono stati o saranno comunicati" andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento – siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento). Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;
(d) per ciò che concerne i "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del GDPR (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.);
(e) per ciò che concerne i "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso");
(f) per ciò che concerne la "descrizione generale delle misure di sicurezza" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del GDPR tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha di per sé un carattere dinamico (e non più statico, come è stato per l'Allegato B del D.Lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di

fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).
In ordine, invece, al "Registro del responsabile" (esterno del trattamento di cui all'art. 28 GDPR), disciplinato dall'art. 30, par. 2 del GDPR, si rappresenta quanto segue in merito alle modalità di compilazione dello stesso:
a) nel caso in cui uno stesso soggetto agisca in qualità di responsabile del trattamento per conto di più clienti quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all'art. 30, par. 2 del GDPR dovranno essere riportate nel registro con riferimento a ciascuno dei suddetti titolari. In questi casi il responsabile dovrà suddividere il registro in tante sezioni quanti sono i titolari per conto dei quali agisce; ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del GDPR;
b) con riferimento alla "descrizione delle categorie di trattamenti effettuati" (art. 30, par. 2, lett. b) del GDPR) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28 del RGPD, deve individuare, in particolare, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo;
c) in caso di sub-responsabile, parimenti, il registro delle attività di trattamento svolte da quest'ultimo potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'art. 28, paragrafi 2 e 4 del GDPR.

CAPO IV – COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI, PUBBLICITA' E TRASPARENZA

Art. 15 - Comunicazione e diffusione dei dati personali

Per ciò che concerne la comunicazione[13] e la diffusione[14] dei dati personali, L'Ente si conforma alle indicazioni di cui all'art. 2-ter del Codice privacy (D.Lgs. 196/2003), recentemente modificato, secondo cui:
"*1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali.*
1-bis. Fermo restando ogni altro obbligo previsto dal Regolamento […] il trattamento dei dati personali da parte di un'amministrazione pubblica è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento.

[13] Si intende per "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.

[14] Si intende per "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, 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 o se necessaria ai sensi del comma 1-bis.
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 o se necessarie ai sensi del comma 1-bis. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.".

Art. 16 – Pubblicità e diffusione di dati personali contenuti in atti e provvedimenti amministrativi

Il Titolare, in sede di pubblicazione e diffusione, tramite l'albo pretorio informatico e la rete civica, di dati personali contenuti in atti e provvedimenti amministrativi, assicura, mediante l'implementazione delle necessarie misure tecniche ed organizzative, il rispetto dei seguenti principi:
a) sicurezza;
b) completezza;
c) esattezza;
d) accessibilità;
e) legittimità e conformità ai principi di pertinenza, non eccedenza, temporaneità ed indispensabilità rispetto alle finalità perseguite.

Laddove documenti, dati e informazioni oggetto di pubblicazione obbligatoria per finalità di pubblicità o trasparenza contengano dati personali, il Titolare dovrà conformarsi alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi del 2014, ancora vigenti, sebbene in corso di aggiornamento[15].

In applicazione di tali regole, l'operatore addetto alle pubblicazioni, prima di pubblicare un documento, dovrà eseguire le seguenti operazioni preliminari:
1) Verificare la presenza di dati personali nel documento da pubblicare, nonché la tipologia dei dati coinvolti (comuni, particolari ai sensi dell'art. 9 GDPR, giudiziari ai sensi dell'art. 10 GDPR);
2) In presenza di dati personali, verificare la sussistenza dell'obbligo, previsto da una norma di legge o di regolamento, di pubblicazione del documento nel proprio sito web istituzionale (albo pretorio online o amministrazione trasparente) ed identificare la finalità per cui viene prescritta, dalla legge o dal regolamento, la pubblicazione.

A tal fine, è necessario tenere conto che gli obblighi di pubblicazione si distinguono in:
a) obblighi di pubblicazione per finalità di trasparenza ai sensi del D.Lgs. n. 33/2013. Ai fini di trasparenza e del D.Lgs. n. 33/2013, si applicano le disposizioni relative all'accesso civico, all'indicizzazione nei motori di ricerca, al riutilizzo, alla durata dell'obbligo di permanenza sul web di 5 anni e alla trasposizione in archivio. Gli obblighi di pubblicazione, cristallizzati dal decreto, costituiscono la base giuridica per dar corso alla diffusione online dei dati e dei documenti. Fermo restando che il conseguimento di un livello di trasparenza più elevato rispetto al livello minimo prescritto dal D.Lgs. n. 33/2013 costituisce irrinunciabile obiettivo strategico, tuttavia non possono essere pubblicati dai personali ulteriori rispetto a quelli per i quali è prevista la pubblicazione obbligatoria, a meno che tali dati non vengano resi effettivamente anonimi e non vi sia più la possibilità di identificare gli interessati, nemmeno indirettamente ed in un momento successivo;
b) obblighi di pubblicazione per altre finalità, diverse dalla trasparenza, contenuti in puntuali disposizioni di settore, come quelli che prevedono la pubblicazione legale di determinati atti amministrativi (ad esempio, le pubblicazioni ufficiali dello Stato; le pubblicazioni di deliberazioni,

[15] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3134436.

ordinanze e determinazioni sull'albo pretorio online; le pubblicazioni matrimoniali; la pubblicazione degli atti concernenti il cambiamento del nome; la pubblicazione della comunicazione di avviso di deposito delle cartelle esattoriali a persone irreperibili etc.).
Trattandosi di pubblicazioni per finalità diverse dalla trasparenza (es: albo pretorio online), non si applicano le specifiche previsioni del D.Lgs. n. 33/2013 relative all'accesso civico, all'indicizzazione nei motori di ricerca, al riutilizzo, alla durata dell'obbligo di permanenza sul web di 5 anni e la trasposizione in archivio. Gli obblighi di pubblicazione, cristallizzati nelle varie disposizioni di settore, costituiscono la base giuridica per dar corso alla diffusione online dei dati e documenti. In particolare, si ricorda che la diffusione di dati personali nell'albo pretorio online è lecita soltanto se prescritta da una specifica norma di legge o di regolamento e deve essere contenuta nei tempi obbligatori di pubblicazione (15 gg. o diversa durata indicata dalla specifica disposizione che prevede la pubblicazione).
3) Minimizzare i dati personali (vedi art. 5, par. 1, lett. c, GDPR), limitandosi ad includere negli atti da pubblicare solo i dati personali realmente necessari, proporzionati e pertinenti alla finalità perseguita nel caso concreto. In forza dell'obbligatoria attività di minimizzazione, l'operatore deve:
• verificare, caso per caso, se i dati personali contenuti nel documento da pubblicare risultino pertinenti rispetto al contenuto ed alla tipologia di documento da pubblicare;
• verificare, caso per caso, se i dati personali contenuti nel documento da pubblicare risultino eccedenti rispetto alla finalità da conseguire mediante la pubblicazione e, conseguentemente, verificare se ricorrano i presupposti per l'oscuramento delle informazioni non necessarie (es: non andranno mai pubblicati codici fiscali, recapiti personali, documenti di identità);
• sottrarre alla reperibilità, sulla rete e da parte dei motori di ricerca (indicizzazione), i dati particolari ex art. 9 GDPR (ossia gli ex dati sensibili e sensibilissimi), i dati giudiziari ex art. 10 GDPR consultando, se del caso, l'Amministratore di sistema, ai fini del reperimento di idonee istruzioni tecniche per effettuare tale operazione.
4) Accertare, per i dati particolari ex art. 9 GDPR diversi da quelli inerenti la salute, l'assoluta "indispensabilità" della pubblicazione per le finalità da conseguire, qualora le stesse non possano essere soddisfatte mediante il ricorso a dati anonimi. Oscurare/anonimizzare i dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.
Con riferimento a tale operazione, si ricorda preliminarmente che per le categorie particolari di dati personali ex art. 9 GDPR o relativi ai procedimenti giudiziari i dati possono essere trattati solo se indispensabili.
Ciò premesso, resta fermo il divieto assoluto di diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici (ad esempio, vanno oscurati dai siti web i dati personali contenuti nelle ordinanze con le quali il sindaco dispone il trattamento sanitario obbligatorio).
Per oscurare/anonimizzare il documento non basta sostituire il nome e cognome con le iniziali dell'interessato, ma è necessario oscurare del tutto il nominativo (comprese le iniziali, sostituendo, ad esempio con "XXX" il Cognome ed il Nome) e oscurare, altresì, le informazioni riferite all'interessato che ne possono consentire l'identificazione, anche a posteriori.
La necessità di minimizzare e oscurare, secondo quanto in precedenza indicato, i dati personali presenti nel documento da pubblicare, impone di adottare soluzioni organizzative e procedurali in grado di consentire, ai fini della diffusione in rete, quali:
- la disponibilità di un documento originale conforme, di default, alle esigenze di minimizzazione ed oscuramento ("privacy by design and by default", ossia "protezione dei dati fin dalla progettazione e per impostazione predefinita" ex art. 25 GDPR), ad esempio mediante l'utilizzo della tecnica

dell'inserimento dei dati personali in un allegato al documento (c.d. allegato privacy) da sottrarre alla diffusione in rete e da rendere accessibile mediante l'accesso documentale;
- in alternativa, la formazione, a partire dal documento originale, del documento minimizzato e oscurato da pubblicare in rete, quale copia dell'originale formata a fini di pubblicazione (c.d. documento web).
5) Oscurare i dati personali che sono stati resi pubblici una volta raggiunti gli scopi per i quali sono stati pubblicati, anche prima del termine di 5 anni, e dopo la decorrenza di pubblicazione obbligatoria (generalmente 15 giorni o diverso termine previsto dalla legge) per le pubblicazioni sull'albo pretorio.
Infine, per attuare "fin dalla progettazione" in modo efficace i principi di protezione dei dati, provvedendo a integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del GDPR e tutelare i diritti degli interessati, si precisa che l'Ente si impegna a configurare il sistema gestionale per l'adozione degli atti che consenta la visione circoscritta alla sola "unità organizzativa" emittente l'atto medesimo, il cui personale è istruito allo specifico trattamento, limitando in tal modo la visibilità degli allegati di cui si omette la pubblicazione ai soli soggetti autorizzati (artt. 25, par. 1, GDPR; 2-quaterdecies, del Codice).
Maggiori approfondimenti e chiarimenti sul tema sono rinvenibili nelle "FAQ – Trasparenza online della P.A. e privacy"[16].

Art. 17 – Diritto di accesso alla documentazione, diritto di accesso civico e protezione dei dati personali

I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato (cd. accesso "FOIA"), contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla normativa in materia di accesso agli atti e di accesso civico, anche per ciò che concerne i tipi di dati particolari e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.
Per ciò che riguarda l'accesso agli atti e i suoi rapporti con la privacy, l'Ente si conforma alle indicazioni di cui agli artt. 59 e 60 del Codice privacy (D.Lgs. 196/2003), ai limiti (per l'accesso documentale) dell'art. 24 della L. 241/90 (in particolare, il comma 6, lett. d) e dell'art. 5-bis del D.Lgs. 33/2013 (per l'accesso civico), alla giurisprudenza in materia (in particolare, le argomentazioni della Corte Costituzionale[17]) e, per ciò che riguarda l'accesso FOIA, alle "Linee guida ANAC di cui alla determinazione n. 1309 del 28/12/2016" (in particolare, il paragrafo 8.1 delle stesse, che individua limiti all'accesso civico generalizzato derivanti dalla necessità di proteggere i dati personali[18]).

CAPO V – DIRITTI DEGLI INTERESSATI

Art. 18 – Diritti dell'interessato

Il titolare attua e implementa le misure organizzative, gestionali, procedurali e documentali necessarie a facilitare l'esercizio dei diritti dell'interessato, di seguito elencati, in conformità alla disciplina contenuta nel GDPR e nel Codice.
L'Ente si impegna ad adottare (e aggiornare/revisionare periodicamente) una procedura (cd. "policy") per la gestione dei diritti degli interessati.

[16] https://www.garanteprivacy.it/faq/trasparenza-online.
[17] https://www.cortecostituzionale.it/documenti/relazioni_internazionali/RelazioneZANON_Lisbona10-12ottobre2019.pdf.
[18] https://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666.

Per maggiori approfondimenti sul tema, si rinvia alla pagina dell'Autorità Garante per la Protezione dei Dati personali[19].

Art. 19 – Diritto di accesso

Il presente Regolamento tiene conto della disciplina dell'art. 15 GDPR in tema di diritto di accesso e delle indicazioni delle Linee guida dell'EDPB n. 1/2022[20], secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.

Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Art. 20 – Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina degli artt. 16 e 17 GDPR in tema di diritto di rettifica e cancellazione ("diritto all'oblio"), di seguito indicata.

Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Il titolare comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Quanto al diritto "all'oblio"[21], consistente nel diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, lo stesso non si applica nella misura in cui il trattamento sia necessario:

---

[19] https://www.garanteprivacy.it/Regolamentoue/diritti-degli-interessati.

[20] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

[21] Vedi anche le Linee Guida dell'EDPB n. 5/2019: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_it.

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 GDPR;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1 GDPR, nella misura in cui il diritto all'oblio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 21 – Diritto alla limitazione

Il presente Regolamento tiene conto della disciplina dell'art. 18 GDPR in tema di diritto alla limitazione, e di seguito indicata. L'interessato ha il diritto di ottenere dal titolare la limitazione del trattamento quando ricorre una delle seguenti condizioni:
a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18 GDPR, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare prima che detta limitazione sia revocata.
Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Art. 22 – Diritto alla portabilità

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina dell'art. 20 par. 3 GDPR, il diritto alla portabilità dei dati non si applica al trattamento 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. Pertanto, tale diritto non potrà essere esercitato nei confronti dell'Ente e non dovrà essere inserito tra i diritti esercitabili nelle informative privacy fornite agli interessati.

Art. 23 – Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il 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.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Il diritto di cui ai paragrafi 1 e 2 dell'art. 21 GDPR è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1 del GDPR, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Art. 24 – Modalità di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, si applicano le disposizioni del GDPR, del Codice e del presente Regolamento, nonché dell'apposita procedura/policy adottata dall'Ente.
La richiesta per l'esercizio dei diritti può essere fatta pervenire:
- direttamente dall'interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia o anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'interessato stesso;
- tramite altra persona fisica o associazione, a cui abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
- tramite chi esercita la potestà o la tutela/amministrazione di sostegno, per i minori e gli incapaci;
- in caso di persone decedute, da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione;
- dalla persona fisica legittimata in base ai relativi statuti od ordinamenti, se l'interessato è una persona giuridica, un ente o un'associazione.

L'interessato può presentare o inviare la richiesta di esercizio dei diritti:
- al titolare o al responsabile del trattamento, che conserva e gestisce i dati personali dell'interessato;
- all'ufficio protocollo generale del titolare o all'ufficio per le relazioni con il pubblico;
- al Responsabile della protezione dei dati (RPD/DPO) ai recapiti indicati.

La richiesta per l'esercizio dei diritti di accesso ai dati personali può essere esercitata dall'interessato solo in riferimento:
- alle informazioni che lo riguardano e non ai dati personali relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

Fermo restando l'accesso ai dati personali, il dirigente/P.O. autorizza l'esibizione degli atti all'interessato, ricorrendo le condizioni per l'accesso.
I soggetti competenti alla valutazione dell'istanza sono:
- il dirigente/P.O. competente, il quale decide sull'ammissibilità della richiesta d'accesso e sulle modalità di accesso ai dati, dopo aver coinvolto il DPO dell'Ente.

All'istanza deve essere dato riscontro, ai sensi dell'art. 12 par. 3 GDPR, senza ingiustificato ritardo e comunque al più tardi entro un mese (1 mese) dal ricevimento della richiesta stessa.
Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

Se non ottempera alla richiesta dell'interessato, il titolare del trattamento deve, in ogni caso, informare l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale (cons. 59 e art. 12, par. 4, del Regolamento).
Si rappresenta che il mancato o inidoneo riscontro alle richieste di esercizio dei diritti dell'interessato, entro i termini sopra indicati, può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del GDPR.
I diritti degli interessati incontrano i limiti previsti nell'art. 2-undecies del D.Lgs. 196/2003.
Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.
L'accesso dell'interessato ai propri dati personali può essere differito limitatamente al periodo strettamente necessario durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza del titolare. L'accesso è tuttavia consentito agli altri dati personali dell'interessato che non incidono sulle ragioni di tutela a base del differimento.

Art. 25 – Indagini difensive
Ai fini delle indagini svolte nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-quater del Codice di procedura penale, può chiedere documenti in possesso del titolare, e può estrarne copia, anche se contengono dati personali di un terzo interessato.
Il rilascio è subordinato alla verifica 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 rinviando, per ogni altro e ulteriore aspetto, alla relativa disciplina al Regolamento del titolare sul diritto di accesso.

CAPO VI – SOGGETTI

Art. 26 – Titolare e contitolari
Il titolare del trattamento, ai sensi degli artt. art. 4 n. 7) e 24 GDPR, è il Comune di San Vero Milis nella persona del Sindaco in qualità di legale rappresentante *pro tempore*, con sede in San Vero Milis, nella via Eleonora d'Arborea n. 5, PEC: protocollo@pec.comune.sanveromilis.or.it.
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 nel DUP e negli altri documenti di programmazione e pianificazione del titolare;
- a mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al GDPR, al Codice privacy e al presente Regolamento, nonché alle policy adottate;
- a delegare ovvero a nominare, con proprio atto, le P.O. per i compiti, le funzioni e i poteri in ordine ai processi, procedimenti e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, impartendo ad essi le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
- a formare e aggiornare l'elenco delle P.O. delegate o nominate;
- 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, potendo configurarsi una “culpa in vigilando” in caso di omesso controllo;
- a favorire l’adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
- a favorire l’adesione a meccanismi di certificazione;
- ad assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

Il titolare si trova in rapporto di contitolarità con altri titolari, ai sensi dell’art. 26 GDPR, quando determinano congiuntamente le finalità e i mezzi del trattamento (es: PLUS, videosorveglianza urbana integrata).

I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno (cd. “accordo di contitolarità”), 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 e 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 di contitolarità può designare un punto di contatto unico per gli interessati. L’accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale 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.

Per la definizione dei rispettivi ruoli e un approfondimento su compiti, obblighi e rapporti reciproci, nonché sul contenuto dell’accordo di contitolarità, l’Ente si conforma alle Linee Guida dell’EDPB n. 7/2020 sui concetti di titolare del trattamento e responsabile del trattamento ai sensi del GDPR, adottate il 7 luglio 2021[22].

Art. 27 – Responsabili di Posizione Organizzativa – Designati di I livello.

Il titolare conferisce i sottoindicati compiti e funzioni, ed i correlati poteri, mediante apposito provvedimento di delega o di nomina, da adottarsi secondo il proprio ordinamento, alle P.O facenti parte della propria struttura organizzativa.

Con specifico atto di nomina, redatto in conformità agli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003, titolare informa ciascun dirigente/ P.O., delle responsabilità che gli sono affidate in relazione a quanto disposto dal GDPR, dal Codice privacy e dal presente Regolamento.

Tra i compiti, funzioni e poteri, i soggetti designati (di I livello) debbono:

• nominare, mediante individuazione per iscritto, gli autorizzati al trattamento, stabilendone i compiti e fornendo loro idonee istruzioni, oltre che vigilarne;

• richiedere, ove l’attività da svolgere non sia espressamente disciplinata dal presente documento di nomina, l’intervento del DPO mediante richiesta di parere sulla corretta modalità di trattamento dei dati personali;

• vigilare sulla corretta custodia delle credenziali e delle password fornite agli autorizzati al trattamento, nonché sull’uso degli strumenti informatici;

• cooperare alla redazione e all’aggiornamento del “Registro delle attività di trattamento” ex art. 30 par. 1 GDPR;

• adottare, nell’organizzazione dei servizi di propria competenza, misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al GDPR, e sia idoneo a garantire il rispetto dei diritti e delle libertà fondamentali e procedere se necessario, al loro riesame;

[22] https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf.

• sottoscrivere, ove rientri nella sua competenza, gli atti di nomina a responsabile (esterno) del trattamento ai sensi dell'art. 28 GDPR, autorizzare (ove necessario) le attività dei sub-responsabili, e vigilare sul loro operato;
• verificare che siano attuate tutte le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato, ai fini di ridurre i rischi di distruzione o perdita dei dati, accessi non autorizzati, trattamenti non consentiti o non conformi alle finalità della raccolta, segnalando eventuali mancanze o criticità;
• comunicare tempestivamente al Titolare e al DPO l'inizio di ogni nuovo trattamento di dati personali, la modifica o la cessazione dei trattamenti in atto;
• vigilare sulla corretta conservazione dei documenti e degli archivi, sia in formato cartaceo che digitale, contenenti dati personali di cui l'Ente sia Titolare o Responsabile del trattamento;
• vigilare e verificare che gli autorizzati al trattamento seguano quanto disposto in materia di utilizzazione di dispositivi di memorizzazione e sul divieto d'uso di dispositivi personali, se non espressamente autorizzati;
• vigilare e verificare che gli autorizzati al trattamento rispettino quanto stabilito relativamente alla duplicazione dei documenti dell'Ente;
• informare senza ritardo l'Ente nella eventualità che si siano rilevati dei rischi incombenti sul corretto trattamento dei dati personali;
• quando un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, collaborare con il Titolare del trattamento e con il DPO nell'effettuazione, prima di procedere al trattamento, alla valutazione di impatto dei trattamenti previsti sulla protezione dei dati personali ai sensi dell'art. 35 del GDPR (cd. "DPIA");
• assicurare che il trattamento dei dati personali sia preceduto da idonee informazioni sul trattamento dei dati personali, in relazione alle modalità particolari per informare l'interessato per il trattamento dei dati personali in ambito pubblico;
• segnalare eventuali esigenze relative ad interventi di formazione e sensibilizzazione delle persone autorizzate al trattamento rispetto all'applicazione delle norme in materia di protezione dei dati personali e, ove necessario, fornire la necessaria collaborazione nella relativa programmazione e pianificazione;
• prestare la massima collaborazione nei confronti dell'Ente per le ipotesi di esercizio dei diritti ai sensi degli artt. 15-22 del GDPR da parte degli interessati (accesso, rettifica, cancellazione, limitazione, blocco, etc.), comunicando senza ritardo al Titolare (e al DPO) ogni richiesta di esercizio dei diritti;
• assicurare che, con riferimento ai dati personali concernenti persone decedute, i diritti di cui agli articoli da 15 a 22 siano esercitati da chi abbia un interesse proprio o agisca a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione;
• rispondere tempestivamente alle richieste, eventualmente concordando con il DPO modalità e tempi della richiesta, ed eventuali reclami degli interessati, nonché offrire la massima collaborazione ed interagire con soggetti che, per legge, compiano verifiche, controlli o ispezioni sugli adempimenti riguardanti la tutela dei dati personali;
• adottare le misure necessarie e rispettare i principi sanciti dal GDPR al fine di consentire, qualora si renda necessario, un corretto trasferimento dei dati personali verso Paesi terzi ovvero Organizzazioni internazionali;
• verificare che i trattamenti di dati genetici, biometrici e relativi alla salute siano conformi anche alle misure di garanzia disposte dal garante ai sensi dell'art. 2-septies del D.Lgs. 196/2003;
• rispettare in maniera rigorosa quanto prescritto dal Regolamento privacy dell'Ente, dalle diverse policy adottate (es: sulla gestione dei diritti degli interessati, sulla gestione dei data breach, sull'uso degli strumenti informatici etc.), nonché da tutti gli altri documenti rilevanti in materia di protezione dei dati personali;

• dare, nel caso in cui constati o sospetti un incidente di sicurezza e di violazione dei dati personali (cd. data breach), immediata comunicazione (e comunque entro le 24 ore) al Titolare e al DPO, includendo, ove possibile, una breve descrizione dell'evento;
• mettere a disposizione del Titolare e del DPO tutte le informazioni necessarie per dimostrare il rispetto degli obblighi specificati nel presente atto di nomina.
Ciascun dirigente/P.O. risponde al titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di sicurezza.
Le P.O. sono destinatari degli interventi di formazione di aggiornamento.

Art. 28 – Autorizzati al trattamento dipendenti del titolare
Gli autorizzati al trattamento sono le persone fisiche, dipendenti del titolare, nominati da ciascun dirigente/P.O. (ossia dai designati di I livello di cui al precedente articolo), incaricati di svolgere le operazioni di trattamento dei dati personali di competenza con l'indicazione specifica dei compiti, dell'ambito di trattamento consentito, e delle modalità di trattamento.
La nomina dell'autorizzato al trattamento dei dati personali è di competenza del dirigente/P.O.; la nomina è effettuata per iscritto, con specifico atto di nomina redatto in conformità agli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003, e individua specificatamente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi, nonché l'ambito del trattamento consentito.
A prescindere dalla nomina, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare soggetto "autorizzato al trattamento" ai sensi degli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003.
Gli autorizzati debbono comunque ricevere idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.
Gli autorizzati collaborano con il titolare ed il dirigente/P.O. segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.
In particolare, gli autorizzati devono:
• attenersi alle istruzioni impartite dal Titolare (anche per il tramite del Designato), il quale, anche mediante periodiche verifiche e audit interni ed esterni, vigila sulla corretta osservanza delle stesse;
• richiedere, ove l'attività da svolgere non sia espressamente disciplinata dal presente documento di nomina, l'intervento del DPO mediante richiesta di parere sulla corretta modalità di trattamento dei dati personali;
• consultare e fornire collaborazione all'attività del Data Protection Officer, sia per le funzioni di consulenza, che di controllo, che di cooperazione e punto di contatto con l'Autorità di controllo;
• cooperare alla redazione e all'aggiornamento del "Registro delle attività di trattamento" ex art. 30 par. 1 GDPR;
• informare senza ritardo il Designato nella eventualità che si siano rilevati dei rischi incombenti sul corretto trattamento dei dati personali, o che vi sia una variazione del rischio;
• garantire che il trattamento dei dati si svolga nel rispetto delle misure di sicurezza, e delle connesse misure adottate dall'Ente, per quanto di propria competenza;
• adottare ogni misura idonea a ridurre il rischio di distruzione dati, perdita o accesso non autorizzato;
• rispettare gli obblighi di segretezza e non divulgazione dei dati di cui siano venuti a conoscenza;
• nel caso in cui abbiano ricevuto credenziali di autenticazione per il trattamento dei dati personali, le stesse devono essere conservate con la massima segretezza così come le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo;

• non lasciare in nessun caso incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
• non indicare e annotare le parole chiave e le credenziali di accesso ad aree riservate in spazi comuni o agevolmente accessibili, ad esempio mediante l'uso di agende, post-it o altre modalità che siano in grado, anche solo potenzialmente, di mettere a rischio l'integrità e la disponibilità degli strumenti informatici o telematici dell'Ente;
• controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali. I documenti cartacei contenenti dati personali devono essere conservati in archivi provvisti di serratura, e i documenti cartacei contenenti categorie particolari di dati (es: dati sensibili, sensibilissimi) devono essere, per quanto possibile, conservati in separato archivio, sempre provvisto di serratura;
• quando gli atti e i documenti contenenti dati personali e particolari categorie di dati di cui agli articoli 9 e 10 GDPR (ivi compresi i dati relativi allo stato di salute), sono affidati al/agli Autorizzato/i al trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dall'Autorizzato fino alla restituzione;
• garantire che, all'interno dei locali adibiti al trattamento delle informazioni, non accedano persone prive di autorizzazione o siano oggetto di danneggiamenti intenzionali o accidentali. Devono altresì identificare e registrare i soggetti ammessi dopo l'orario di chiusura degli uffici stessi;
• impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali che gli sono stati affidati in custodia;
• trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare. Non è consentito l'accesso ai sistemi informatici per finalità non attinenti all'attività lavorativa o, comunque, per finalità differenti da quelle per le quali sia stata concessa l'abilitazione all'uso degli strumenti o l'accesso alle informazioni attraverso essi o in essi memorizzate;
• con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
• effettuare le copie di dati personali, oggetto di trattamento, esclusivamente se necessario e soltanto previa autorizzazione, generale o specifica, del Designato;
• omettere di trattare, duplicare, portare all'esterno dell'ambito dell'Ente o dall'ufficio qualsiasi dispositivo di memorizzazione (di qualsiasi natura) contenente dati nella disponibilità dell'Ente o relativi alle attività da quest'ultima poste in essere in assenza di preventiva ed espressa autorizzazione;
• non utilizzare dispositivi personali non espressamente autorizzati anche al fine di memorizzare o di esportare all'esterno immagini, registrazioni audio/video o altre informazioni relativi a luoghi, macchinari, documenti contenenti dati personali appartenenti al Titolare del trattamento;
• assicurarsi che il trattamento dei dati personali sia preceduto da idonee informazioni sul trattamento dei dati personali, in relazione alle modalità particolari per informare l'interessato e per il trattamento dei dati personali in ambito pubblico;
• prestare la massima collaborazione nei confronti dell'Ente, per le ipotesi di esercizio dei diritti ai sensi degli artt. 15-22 del GDPR da parte degli interessati, comunicando senza ritardo al Designato e, se del caso, al Titolare (e al DPO) ogni richiesta di esercizio dei diritti;
• cooperare con il Designato e il Titolare al fine di rispondere tempestivamente alle richieste, eventualmente concordando con il DPO modalità e tempi della richiesta, ed eventuali reclami degli interessati, nonché offrire la massima collaborazione ed interagire con i soggetti che, per legge, compiano verifiche, controlli o ispezioni sugli adempimenti riguardanti la tutela dei dati personali;
• quando un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, collaborare con il Titolare del trattamento, con il Designato e con il DPO nell'effettuazione, prima di procedere al trattamento, alla valutazione di impatto dei trattamenti previsti sulla protezione dei dati personali ai sensi dell'art. 35 del GDPR (cd. "DPIA");
• rispettare in maniera rigorosa quanto prescritto dal Regolamento privacy dell'Ente, dalle diverse policy adottate (es: sulla gestione dei diritti degli interessati, sulla gestione dei data breach, sull'uso

degli strumenti informatici etc.), nonché da tutti gli altri documenti rilevanti in materia di protezione dei dati personali;
• segnalare al Titolare e al Designato la mancata effettuazione della formazione privacy obbligatoria;
• adottare le misure necessarie e rispettare i principi sanciti dal GDPR al fine di consentire, qualora si renda necessario, un corretto trasferimento dei dati personali verso Paesi terzi ovvero Organizzazioni internazionali;
• dare, nel caso in cui constati o sospetti un incidente di sicurezza e di violazione dei dati personali (cd. data breach), immediata comunicazione al Designato, includendo, ove possibile, una breve descrizione dell'evento.
Gli autorizzati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal titolare e dal dirigente/P.O., nei soli casi previsti dalla legge, nello svolgimento dell'attività istituzionale del titolare. Gli autorizzati dipendenti del titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 29 – Autorizzati al trattamento non dipendenti del titolare
Tutti i soggetti che svolgono un'attività di trattamento dei dati e che non sono dipendenti del titolare, quali, a titolo meramente esemplificativo, i tirocinanti, i volontari ed i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare, devono essere autorizzati al trattamento con specifico atto di nomina redatto in conformità agli artt. 29 e 32.4 GDPR ed art. 2-quaterdecies D.Lgs. 196/2003.
Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli autorizzati dipendenti del titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
Gli autorizzati non dipendenti dal titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 30 – Responsabili (esterni) del trattamento e sub-responsabili
Il Responsabile (esterno) del trattamento, ai sensi del combinato disposto degli artt. 4 par. 8 e 28 GDPR, nonché conformemente alle precisazioni delle Linee Guida dell'EDPB n. 7/2020[23], è la persona, fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare (es: società che fornisce i software gestionali agli uffici, l'amministratore di sistema, il tesoriere dell'Ente, il consulente del lavoro, gli aggiudicatari degli appalti ecc.).
Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato (es: la verifica preliminare può essere effettuata mediante "check-list").
Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.
Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri (ad esempio, un allegato che costituirà parte integrante del contratto di servizi stipulato), che vincoli il responsabile del trattamento al titolare del trattamento.
Il suddetto contratto/atto di nomina prevede, in particolare, che il responsabile del trattamento:

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_it).

- tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure richieste ai sensi dell'articolo 32;
- rispetti le condizioni di cui all'art. 28 paragrafi 2 e 4 GDPR per ricorrere a un altro responsabile del trattamento;
- tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
- assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GDPR (es: DPIA, comunicazione "data breach"), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del titolare del trattamento, cancelli o restituisca al titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;
- informi immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, senza ingiustificato ritardo, e comunque, non oltre il termine di 24 ore dal momento in cui è venuto a conoscenza della violazione. La mancata comunicazione nei termini previsti comporterà le conseguenze indicate nel contratto di nomina.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del GDPR, del Codice privacy e del presente Regolamento è condizione necessaria per l'instaurarsi o il mantenimento del rapporto giuridico fra le parti.

Maggiori dettagli sulle istruzioni impartite ai Responsabili del trattamento ex art. 28 GDPR sono contenute nello specifico atto di nomina a disposizione degli uffici, secondo un modello/schema il cui contenuto è stato elaborato sotto la supervisione del DPO nominato.

Tale modello è sottoposto a revisione/controllo periodico e viene aggiornato secondo le indicazioni provenienti dal Garante privacy, dall'EDPB e dalla migliore dottrina in materia.

Art. 31 – Amministratore di sistema

L'amministratore di sistema sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata l'Amministrazione.

La nomina dell'amministratore di sistema avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza.

La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'amministratore di sistema svolge attività, quali il salvataggio dei dati, l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware e propone al Titolare del trattamento un documento di valutazione del rischio informatico.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, l'amministratore di sistema:

- deve adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni ("access log") devono essere complete, inalterabili, verificabili nella loro integrità e adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi;
- dovrà collaborare con il titolare del trattamento ed il DPO nominato nel caso di (presunte) violazioni di dati personali ("data breach"), fornendo l'assistenza e la consulenza richiesta (es: sopralluoghi, relazioni ecc.).
- supporta l'Ente nell'implementazione delle misure di sicurezza di cui all'art. 32 GDPR, ivi comprese le "misure minime di sicurezza ICT per le P.A." di cui alla circolare AgID n. 2/2017[24], utilizzando il modulo di implementazione messo a disposizione dall'AgID e sottoponendolo al titolare del trattamento, affinché richieda un parere al DPO[25].
- supporta l'Ente alla redazione e all'aggiornamento di un "Regolamento sull'uso degli strumenti informatici".

Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza almeno annuale (ma è preferibile prevedere un intervallo più ridotto), da parte del titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

A tal proposito, l'AdS dovrà fornire al Comune una relazione analitica del proprio operato, individuando le misure di sicurezza adottate e da adottare e gli ambiti di rischio individuati. Tale relazione dovrà poi essere sottoposta al DPO per un suo parere in merito e per avviare una sinergia tra le parti volta a migliorare la sicurezza dell'Ente.

Inoltre, l'Amministratore di sistema, in quanto responsabile (esterno) del trattamento ai sensi dell'art. 28 GDPR, dovrà essere nominato con apposito contratto di nomina, secondo quanto disposto dall'art. 29 del presente Regolamento.

I dati di contatto dell'Amministratore di sistema nominato saranno comunicati a tutti i soggetti designati/autorizzati al trattamento, nonché al DPO dell'Ente, affinché questi possano contattarlo e coinvolgerlo in riferimento a qualsiasi questione in materia di sicurezza informatica.

L'Ente titolare del trattamento applica le disposizioni impartite dal Garante privacy in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema[26].

L'amministratore di sistema è destinatario degli interventi di formazione di aggiornamento.

Art. 32 – Responsabile della protezione dei dati personali (RPD) – Data Protection Officer (DPO)

Il Comune di San Vero Milis ha provveduto a nominare un DPO (o "Responsabile della Protezione dei Dati"), che ha la funzione di affiancare il Titolare del trattamento ed i soggetti designati/autorizzati al trattamento nelle attività di trattamento dei dati personali, seguendo i principi e le indicazioni inserite nella Normativa vigente e nel presente Regolamento.

Il RPD/PDO, conformemente alla disciplina applicabile di cui agli artt. 37-39 GDPR:

- è in possesso di un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- adempie alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;

[24] https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict.

[25] L'adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel CAD (art. 17) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firma e digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017. Secondo la circolare, le misure minime di sicurezza devono essere adottate da parte di tutte le pubbliche Amministrazioni entro il 31 dicembre 2017.

[26] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499.

- opera sulla base di un contratto di servizio;
- è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il RPD/PDO svolge, inoltre, i seguenti compiti:

- informa e fornisce consulenza al titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
- verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
- fornisce, qualora venga richiesto, un proprio parere in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
- funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
- funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

Ai sensi dell'art. 38 par. 3 GDPR, il titolare del trattamento e il responsabile del trattamento si assicurano che:

- vengano messe a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti;
- il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti;
- il DPO non sia rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti;
- il DPO riferisca direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

Il Titolare del trattamento ha provveduto a pubblicare i dati di contatto del RPD/DPO (cfr. art. 37, par. 7, del Regolamento) nel proprio sito internet istituzionale, secondo quanto previsto dall'Autorità Garante, ossia "*per quanto concerne la pubblicazione, questa dovrà essere effettuata sul sito web dell'amministrazione, all'interno di una sezione facilmente riconoscibile dall'utente e accessibile già dalla homepage, oltre che nell'ambito della sezione dedicata all'organigramma dell'ente ed ai relativi contatti" ("Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico)", allegato al provv. 29 aprile 2021, n. 186, doc. web n. 9589104, par. 7; ma v. già le "Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29"", FAQ n. 4)*". Inoltre, i dati di contatto del DPO sono inseriti nelle informative privacy e, più in generale, in tutta la modulistica privacy dell'Ente.

CAPO VII – SICUREZZA DEI DATI PERSONALI

Art. 33 – Misure di sicurezza

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento, conformemente a quanto previsto dall'art. 32 GDPR e col supporto dei rispettivi "amministratori di sistema" nominati, mettono in atto misure tecniche e organizzative adeguate per 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 (es: “penetration test” ecc.).
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.
L'adesione a un codice di condotta approvato di cui all'articolo 40 GDPR o a un meccanismo di certificazione approvato di cui all'articolo 42 GDPR può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 dell’art. 32 GDPR, come sopra indicati.
Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Art. 34 – Valutazione d’impatto sulla protezione dei dati (DPIA)
Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati particolari/sensibili, o anche per una combinazione di questi e altri fattori), il regolamento europeo 2016/679 GDPR obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti, ossia quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.
Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (cd “accountability”) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l’osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.
Le linee guida del WP29[27] offrono alcuni chiarimenti sul punto; in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.
Le linee guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.
Il messaggio finale delle linee-guida è che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l’altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (“data protection by design”) di qualsiasi trattamento.
Maggiori chiarimenti sulla DPIA, che può essere svolta sia mediante il software privacy in dotazione all’Ente, sia tramite il software gratuito del CNIL suggerito dall’Autorità Garante[28], sono rinvenibili nella pagina dedicata del Garante privacy[29] e nelle Linee guida del Gruppo di lavoro Articolo 29[30].

[27] https://ec.europa.eu/newsroom/article29/items/611236.
[28] Link per il download: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.
[29] https://www.garanteprivacy.it/Regolamentoue/DPIA.
[30] https://ec.europa.eu/newsroom/article29/items/611236/en.

Art. 35 – Pubblicazione sintesi della valutazione d'impatto (DPIA)

Il titolare del trattamento può, secondo una propria valutazione discrezionale, effettuare la pubblicazione della sintesi della DPIA al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare, nonché al fine di dimostrare la responsabilizzazione e la trasparenza.

La DPIA pubblicata non deve contenere l'intera valutazione qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare o divulgare segreti commerciali o informazioni commerciali sensibili (es: non va pubblicata la DPIA integrale del sistema di videosorveglianza urbana integrata). In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

Art. 36 – Consultazione preventiva

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 GDPR indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Se ritiene che il trattamento previsto di cui all'art. 36 par. 1 GDPR violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58 GDPR. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

Al momento di consultare l'autorità di controllo, ai sensi dell'art. 36 par. 1 GDPR, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del responsabile della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 GDPR;

f) ogni altra informazione richiesta dall'autorità di controllo.

Art. 37 – Modulistica e procedure (policy)

Il titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del GDPR, del Codice privacy e del presente Regolamento:

a) adotta e costantemente aggiorna:

- modelli uniformi di informativa;
- modelli uniformi di nomine privacy interne e nomine dei responsabili esterni del trattamento;
- modelli e formule uniformi necessarie per gestire il trattamento dei dati e le misure di sicurezza;

b) elabora, approva, e costantemente aggiorna adeguate procedure gestionali, da raccogliere in un apposito Manuale delle procedure.

Art. 38 – Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Il mancato rispetto delle disposizioni in materia di trattamento e protezione dei dati personali potrebbe comportare l'applicazione, nei confronti del titolare del trattamento, di sanzioni amministrative pecuniarie effettive, proporzionate e dissuasive (fino a 10 o 20 milioni di euro) ai sensi dell'art. 83 GDPR (calcolate secondo i criteri delle Linee guida dell'EDPB n. 4/2022[31]).

Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j) GDPR (che riconosce all'Autorità di controllo poteri di indagine, correttivi, autorizzativi e consultivi), o in luogo di tali misure.

La violazione delle norme in materia di trattamento e protezione dei dati personali potrebbe comportare anche la configurazione di fattispecie penali, tra cui quella di cui all'art. 684 c.p. nel caso di violazione dell'art. 50 del D.Lgs. 196/2003, oppure quelle di cui agli artt. 167, 167-bis, 167-ter, 168, 170, 171 del D.Lgs. 196/2003 (così come introdotte o modificate dal D.Lgs. 101/2018).

Restano, in ogni caso, configurabili anche le fattispecie incriminatrici, legate al trattamento di dati personali, previste dal D.Lgs. 101/2018 e quelle contenute nel codice penale (ad es. art. 615-ter c.p., art. 615-quater c.p., etc.).

Resta ferma, inoltre, la possibilità che chiunque subisca un danno materiale o immateriale dalla violazione del GDPR possa ottenere, ai sensi dell'art. 82 GDPR, il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento, salvo che questi dimostrino che l'evento dannoso non gli è in alcun modo imputabile.

Art. 39 – Notificazione di una violazione dei dati personali (cd. "data breach")

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 33 GDPR senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione (entro le 24 ore, secondo lo schema di nomina approvato dall'Ente).

La notifica della violazione (cd. "data breach"), ai sensi dell'art. 33 par. 3 GDPR, deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La notificazione al Garante deve essere eseguita tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità[32] (Vedi: Provvedimento del 27 maggio 2021).

È possibile altresì procedere con la notifica "per fasi" ogniqualvolta non sia possibile corredare la notifica di tutta la documentazione utile (ad es. perché l'indagine sul "data breach" non si è ancora

[31] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_it.

[32] Link procedura telematica: https://servizi.gpdp.it/databreach/s/.

conclusa e non si dispone di tutti gli elementi atti a circostanziarlo). Si procederà allora con una prima notifica sommaria (cd. “notifica preliminare”), seguita poi da quelle più dettagliate (cd. “notifica integrativa”).
La notifica deve essere sottoscritta digitalmente con firma elettronica qualificata/firma digitale.
Si può effettuare una unica complessiva notifica al Garante nelle ipotesi in cui si verifichino nel breve periodo ripetute violazioni, simili tra loro per categorie di dati e tipologia di violazione.
Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (“self assessment”) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza[33].
Inoltre, lo stesso Garante ha messo a disposizione un fac-simile del modello di notificazione, utile per capire quali sono i campi da compilare nella procedura telematica[34].
Il Titolare del trattamento si impegna ad adottare una “policy di gestione dei data breach”, della quale verrà data la massima diffusione all’interno dell’Ente.
Maggiori dettagli sul tema, ivi comprese le Linee guida in materia di notifica delle violazioni di dati personali WP250[35], le Linee guida dell’EDPB n. 1/2021 sugli esempi riguardanti la notifica di violazioni di dati personali[36], le Linee guida dell’EDPB n. 9/2022 sulla notificazione dei data breach di dati personali sotto il GDPR[37], sono rinvenibili nella pagina dedicata dell’Autorità Garante per la Protezione dei Dati personali[38].

Art. 40 – Comunicazione di una violazione dei dati personali all’interessato
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all’interessato senza ingiustificato ritardo.
La comunicazione all’interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all’articolo 33, paragrafo 3, lettere b), c) e d) del GDPR.
Non è richiesta la comunicazione all’interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
Nel caso in cui il titolare del trattamento non abbia ancora comunicato all’interessato la violazione dei dati personali, l’autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

[33] https://servizi.gpdp.it/databreach/s/self-assessment.
[34] https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni.
[35] https://ec.europa.eu/newsroom/article29/items/612052/en.
[36] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en.
[37] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en
[38] https://www.garanteprivacy.it/regolamentoue/databreach.

Il Comune si impegna a disciplinare le modalità di comunicazione all'interessato mediante un'apposita "policy/procedura di gestione dei data breach", della quale verrà data la massima diffusione all'interno dell'Ente.

Art. 41 – Videosorveglianza

Il Comune di San Vero Milis, in qualità di Amministrazione aderente al Progetto della Regione Autonoma della Sardegna "Reti per la Sicurezza del Cittadino e del Territorio - Reti di Sicurezza - Fase 2", con il quale, attraverso un sistema centralizzato, si monitorano, visionano e trasferiscono, in tempo reale, i flussi video provenienti dalle reti locali di videosorveglianza delle Amministrazioni Locali aderenti, ha predisposto il proprio impianto di videosorveglianza affinché lo stesso sia pienamente interoperabile con le specifiche del DVMS Regionale (Digital Video Management System della RAS - Sistema di Gestione Video Digitale della Regione Autonoma della Sardegna) e con le Forze dell'Ordine collegate al sistema DVMS di cui sopra, nel rispetto delle norme sul trattamento dei dati personali e secondo i protocolli di sicurezza e gli standard tecnologici previsti dalla normativa.
Inoltre L'Ente ha approvato un regolamento per la disciplina della videosorveglianza e posto in essere tutti gli adempimenti richiesti dalla normativa applicabile (es: cartellonistica aggiornata, informativa privacy, DPIA, lettere di nomina dei soggetti designati/autorizzati ecc.), ossia il GDPR, il D.Lgs. 51/2018[39], il provvedimento del Garante privacy in materia di videosorveglianza del 08 aprile 2010[40], le Linee guida dell'EDPB n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video[41] e le FAQ del Garante privacy[42].
Maggiori dettagli sul sistema di videosorveglianza e sulla disciplina dello stesso sono rinvenibili nel regolamento videosorveglianza, approvato con delibera consiliare e pubblicato nel sito internet istituzionale dell'Ente.

Art. 42 – Disposizioni finali
Per quanto non previsto nel presente Regolamento si applicano le disposizioni del GDPR, del Codice privacy, le Linee guida ed i provvedimenti del Garante privacy e dell'EDPB.
Il presente Regolamento è aggiornato a seguito di ulteriori modificazioni alla vigente normativa in materia di riservatezza e protezione dei dati personali.

[39] https://www.gazzettaufficiale.it/eli/id/2018/05/24/18G00080/sg.
[40] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1712680.
[41] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it.
[42] https://www.garanteprivacy.it/faq/videosorveglianza.