COMUNE DI SAVOGNA D'ISONZO

Regolamento
sulla protezione
dei dati personali
adottato in attuazione del Regolamento (UE) 2016/679

Approvato con deliberazione C.C. n. 4 in data 27/02/2020

Avv. Nadia Corà
Avv. Guido Paratico

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, con abrogazione della direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

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, è un diritto fondamentale come risulta anche dalla circostanza che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Per rafforzare la protezione, il Regolamento UE, 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, la nuova disciplina europea pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili ossia, sull'adozione di comportamenti proattivi e tali da dimostrare 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 default and by design",* 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 ove il trattamento si colloca 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 e 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 a collocarsi 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 italiano, 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, di effettuazione di valutazioni di impatto in piena autonomia.

Dall'esame della materia emerge come sia, quindi, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

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. 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 potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.
Il Titolare intende adeguare e conformare la propria normativa, regolamentare alle novità introdotte dal citato regolamento UE, fermo restando che il presente aggiornamento è destinato ad essere ulteriormente revisionato in presenza di sopravvenienza di linee guida del Garante per protezione dei dati personali, o di novità normative e giurisprudenziali.
L'ulteriore fonte normativa con cui disciplinare il trattamento dei dati personali, è rappresentato dal D.Lgs. 30 giugno 2003, n. 196 così come modificato dal D.Lgs 10 agosto 2018 n. 101.

CAPO I - DISPOSIZIONI GENERALI

Art. 1 Definizioni

Il presente regolamento di avvale delle seguenti definizioni:

- "**Codice**": D.Lgs. n. 196/2003, come modificato dal D.Lgs 101/2018;
- **"GDPR"**: il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR generale sulla protezione dei dati);
- **"Regolamento sui dati sensibili"**: il Regolamento interno, approvato dal Titolare in conformità allo schema tipo approvato dal Garante, che identifica e rende pubblici, per i trattamenti dei dati sensibili e giudiziari, i tipi di dati e le operazioni eseguibili;
- **"Regolamento":** il presente Regolamento;
- **"titolare":** il Comune o l'Amministrazione che adotta il presente regolamento, Comune di Savogna d'Isonzo – Občina Sovodnje ob Soči, con sede in Savogna d'Isonzo, via Primo Maggio, n. 140, 34070 Savogna d'Isonzo (GO)
- "**dirigenti/P.O.**": i soggetti che esercitano i poteri delegati dal titolare o che sono nominati dal titolare per esercitare tali poteri.

Il presente regolamento recepisce le definizioni del D.Lgs. n. 196/2003 e del GDPR, fermo restando che, in caso di discordanza, prevalgono le definizioni contenute nei rispettivi testi normativi:

definizioni ai fini del GDPR:

- **"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;
- **"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;
- **"limitazione di trattamento":** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **"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;
- **"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;

- **"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;
- **"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;
- **"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;
- **"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;
- **"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;
- **"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;
- **"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;
- **"dati genetici":** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **"dati biometrici":** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **"dati relativi alla salute":** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **"stabilimento principale":**

a) per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua Amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un Responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua Amministrazione centrale nell'Unione o, se il Responsabile del trattamento non ha un' Amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale Responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

- **"rappresentante":** la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- **"impresa":** la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- **"gruppo imprenditoriale":** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- **"norme vincolanti d'impresa":** le politiche in materia di protezione dei dati personali applicate da un Titolare del trattamento o Responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un Titolare del trattamento o Responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- **"autorità di controllo":** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;
- **"autorità di controllo interessata":** un'autorità di controllo interessata dal trattamento di dati personali in quanto:
  - il Titolare del trattamento o il Responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
  - gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento;
    oppure
  - un reclamo è stato proposto a tale autorità di controllo;
- **"trattamento transfrontaliero":**
  - trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un Titolare del trattamento o Responsabile del trattamento nell'Unione ove il Titolare del trattamento o il Responsabile del trattamento siano stabiliti in più di uno Stato membro;

oppure

- trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

- **"obiezione pertinente e motivata":** un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del GDPR, oppure che l'azione prevista in relazione al Titolare del trattamento o Responsabile del trattamento sia conforme al GDPR, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- **"servizio della società dell'informazione":** il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- **"organizzazione internazionale":** un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 2 Quadro normativo di riferimento

Il presente Regolamento tiene conto dei seguenti documenti:

- Codice in materia di dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016 (D.Lgs. n.196/2003, come modificato dal D.Lgs 101/2018);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico Titolare o Responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento"possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni

amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;

- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalita' - 13/EN WP 203;
- Allegato 1 al provvedimento n. 467 del 11 ottobre 2018 "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto";
- Norme internazionali;
- Regolamenti interni, approvati dai titolari e/o dai responsabili.

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, nel rispetto di quanto previsto dal GDPR.
Il presente Regolamento sostituisce integralmente il Regolamento sui dati sensibili, approvato con deliberazione C.C. n. 2 in data 16.01.2006, e aggiornato con deliberazione C.C. n. 4 in data 27.02.2020, ferme restando le schede/tabelle allegate al Regolamento medesimo, che identificano i tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento, nonché le operazioni eseguibili in riferimento alle specifiche finalità di rilevante interesse pubblico perseguite nei singoli casi ed espressamente elencate dalla legge, le quali continuano ad applicarsi e vengono allegate al presente Regolamento per farne parte integrante e sostanziale.

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 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 Codice, del GDPR, e del presente Regolamento.

CAPO II – PRINCIPI

Art. 5 Principi e responsabilizzazione

Vengono integralmente recepiti, nell'ordinamento interno del titolare, i principi del GDPR, per effetto dei quali 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 che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati base 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 base del 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 in base ai principi di "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 permettono di identificare l'interessato solo un caso di necessità *("principio di necessità*").

Il titolare è competente per il rispetto dei principi sopra declinati, ed è in grado di comprovarlo in base al principio di "responsabilizzazione".

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:

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

l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dal titolare nell'esecuzione dei propri compiti e funzioni.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 GDPR, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il Titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9 del GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del medesimo GDPR;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art. 7 Condizioni per il consenso

Femi restando i casi, disciplinati dall'art. 6 del GDPR e dagli artt. 2-ter e 2-sexies del Codice, nei quali può essere legittimamente effettuato il trattamento senza consenso, nei casi in cui il trattamento dei dati personali, per una o più specifiche finalità, è subordinato al consenso dell'interessato, si applica la disciplina del GDPR la quale prevede che:

- qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali;
- se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante;
- l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento.
  La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato;
- nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.
- per i dati sensibili il consenso deve essere esplicito e in forma scritta; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;

- il consenso dei minori è valido a partire dai 16 anni, fermo restando il diverso limite di età, comunque non inferiore a 13 anni, previsto dalla normativa nazionale; prima di del limite età previsto dalla normativa nazionale occorre raccogliere il consenso dei genitori o di chi ne fa le veci;
- deve essere, in tutti i casi, libero e autonomo, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo);
- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

Se il consenso dell'interessato al trattamento dei propri dati personali è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione, che costituisca una violazione del GDPR e del presente Regolamento, è vincolante.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato, emergenza sanitaria o di igiene pubblica, rischio grave e imminente per la salute dell'interessato, il consenso può intervenire senza ritardo, anche successivamente alla prestazione, da parte di chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente.

Qualora il trattamento sia basato sul consenso, il consenso deve essere reso, da parte dell'interessato, attraverso la compilazione di apposita modulistica, predisposta dal titolare, previa consegna e presa d'atto dell'informativa.

Non è ammesso il consenso tacito o presunto ovvero l'utilizzo di caselle prespuntate su un modulo.

Il titolare adotta misure organizzative adeguate a facilitare l'espressione del consenso da parte dell'interessato.

La manifestazione del consenso, ad opera dell'interessato, va resa al momento del primo accesso alle prestazioni, ed è valido ed efficace fino alla revoca della stessa o, per i minorenni, fino al compimento del diciottesimo anno di età.

Il consenso viene registrato nel registro delle attività di trattamento.

Art. 8 Informativa

Il titolare, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, anche avvalendosi del personale incaricato, apposita informativa secondo le modalità previste dal 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, anche se sono ammessi altri mezzi, potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

L'informativa è fornita, mediante idonei strumenti:

- attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
- avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture del titolare, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;

- apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con il titolare.;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, con l'indicazione dell'incaricato del trattamento dei dati relativi alle procedure.

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.

L'informativa contiene il seguente contenuto minimo:

- l'identità e dati di contatto del titolare e, ove presente, del suo rappresentante;
- i dati di contatto del RPD/DPO ove esistente;
- le finalità del trattamento;
- i destinatari dei dati;
- la base giuridica del trattamento;
- l' interesse legittimo del titolare se quest'ultimo costituisce la base 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;
- il diritto dell'interessato di chiedere al titolare l'accesso, la rettifica, la cancellazione dei dati, la limitazione del trattamento che lo riguarda, il diritto di opporsi al trattamento e il diritto alla portabilità dei dati;
- il diritto di presentare un reclamo all'autorità di controllo;
- 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:
a) il titolare deve informare l'interessato in merito a:

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

b) l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure dal momento della comunicazione (e non della registrazione) dei dati a terzi o all'interessato.
Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente del titolare è predisposta apposita informativa per 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 e' effettuato il trattamento dei dati sensibili e giudiziari.

Art. 9 Sensibilizzazione e formazione

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, il titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio.

A tale riguardo, che 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 hanno 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, con i riferimenti per l'acquisizione del presente Regolamento, pubblicato sul sito del Titolare.

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, anche integrati con gli interventi di formazione anticorruzione, 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 RPC, 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

CAPO III - IL TRATTAMENTO DEI DATI PERSONALI

Art. 10 Trattamento dei dati personali, ricognizione dei trattamenti e indice 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 Codice, dal GDPR e dalle Linee guida e dai provvedimenti del Garante.

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, tirocinanti e i volontari;
- la gestione dei rapporti con i consulenti, i libero-professionisti, i fornitori per l'approvvigionamento di beni e di servizi nonché con le imprese per l'esecuzione lavori, opere e di 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 e regolamenti.

Il trattamento dei dati personali è esercitabile, all'interno della struttura organizzativa del titolare, solo da parte dei soggetti appositamente autorizzati:

- titolare
- dirigenti/P.O., in qualità di soggetti che esercitano i poteri delegati dal titolare o in qualità di soggetti nominati dal titolare per l'esercizio di tali poteri
- dipendenti, in qualità di incaricati del trattamento.

Non è consentito il trattamento da parte di persone non autorizzate.
Ai fini del trattamento, il titolare provvede, in collaborazione con i dirigenti/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'indice dei trattamenti.
E' compito dei dirigenti/P.O. dei dati effettuare e documentare l'aggiornamento periodico, almeno annuale, della ricognizione dei trattamenti e del relativo indice, e la valutazione periodica, infrannuale, del rispetto dei principi di cui all'art. 5 del presente Regolamento con riferimento a tutti trattamenti inclusi nell'indice.
Il titolare, i dirigenti/P.O. e gli incaricati si attengono alle modalità di trattamento indicate nel Codice, nel GDPR, nonché nelle disposizioni attuative e nelle Linee guida del Garante per la protezione dei dati personali, in particolare con riferimento all'Allegato 1 al provvedimento n. 467 del 11 ottobre 2018 "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto"

Art.11 Tipologie di dati trattati

Nell'ambito dei trattamenti inclusi nell'indice 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 identificativi
- dati sensibili
- dati giudiziari

Art. 12 Trattamento dei dati sensibili e giudiziari

Il titolare conforma il trattamento dei dati sensibili 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 degli articoli 9 paragrafo 1 del GDPR e l'art. 2-sexies del Codice e si conforma alle Linee Guida del Garante in materia.

Il titolare sensibilizza, forma e aggiorna i dipendenti in ordine al trattamento dei dati sensibili e giudiziari.

Art.13 Trattamento dei dati sensibili relativi alla salute

Il Titolare si conforma all'art. 2-septies del Codice nonché alle Linee Guida del Garante in materia di trattamento dei dati personali sensibili relativi allo stato di salute.

I dati idonei a rivelare lo stato di salute e la vita sessuale sono trattati da soggetti adeguatamente formati e sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.

Art. 14 Trattamento dei dati del personale

Il titolare tratta i dati, anche di natura sensibile o giudiziaria, dei propri dipendenti per le finalità, considerate di rilevante interesse pubblico, di instaurazione e di gestione di rapporti di lavoro di qualunque tipo.

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 sensibili 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 sensibili, 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 sensibile.

Il titolare, nel trattamento dei dati sensibili 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.

Art. 15 Rilevanza delle schede/tabelle identificative delle tipologie di tipi di dati sensibili e giudiziari per cui è consentito il relativo trattamento

Fermo restando che la base giuridica per il trattamento dei dati sensibili e giudiziari è fondata su quanto disposto dall'articoli 9 paragrafo 1 del GDPR e, soprattutto, dall'elenco di cui all'art. 2-sexies del Codice, le schede identificative delle tipologie di dati sensibili e giudiziari, che continuano ad applicarsi venendo allegate al presente Regolamento:

a) vanno consegnate, personalmente, agli incaricati a cui, in materia o competenza, si riferiscono;
b) costituiscono oggetto di formazione;
c) costituiscono oggetto di interventi di monitoraggio e di verifica con riguardo alla loro applicazione.

Art. 16 Registro delle attività di trattamento e delle categorie di trattamento

Il titolare del trattamento istituisce un registro, in forma scritta, delle attività di trattamento e delle categorie di trattamenti svolte sotto la propria responsabilità.

Il registro deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo.

Tale registro contiene le seguenti informazioni:

- il nome e i dati di contatto del Titolare del trattamento, del Responsabile per la protezione dei dati, dei responsabili e degli incaricati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie dei dati personali;
- le categorie dei trattamenti effettuati;
- la categorie di destinatari, a cui i dati personali sono o saranno comunicati;
- l'indicazione delle cautele specifiche, a cui ciascun Responsabile deve attendere in modo che siano appropriate rispetto ai trattamenti verso cui dovrà rispondere;
- un'eventuale possibilità di trasferimenti di dati all'estero;
- una descrizione generale delle misure di sicurezza, generiche e specifiche, così come disciplinate dalla normativa vigente in tema di sicurezza dei dati personali;
- indicazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati trattati.

Il responsabile di trattamento tiene registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la docu- mentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzati-ve di cui

all'articolo 32, paragrafo 1 GDPR

I registri sono tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento, mettono il registro a disposizione del Garante.

CAPO IV – DIRITTI DEGLI INTERESSATI

Art. 17 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 trasparenza, contengano dati personali, questi ultimi devono essere oscurati, tranne deroghe previste da specifiche disposizioni.

Salva diversa disposizione di legge, il titolare garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on line o sulla rete civica, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. A tal fine, il titolare adotta e implementa adeguate misure organizzative, di gestione documentale e di formazione.

In ogni caso, i documenti, soggetti a pubblicazione, riportanti informazioni di carattere sensibile o giudiziario dell'interessato, devono essere anonimizzati con adeguate tecniche di anonimizzazione.

I dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

Il titolare si conforma alle Linee guida del Garante in materia di pubblicazione e diffusione di dati personali contenuti in atti e provvedimenti amministrativi.

Art. 18 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, 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 sensibili e giudiziari, e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.

Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Il titolare si conforma alle Linee guida del Garante in tema di rapporti tra accesso alla documentazione, diritto di accesso civico e protezione dei dati personali.

Art. 19 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.

Art. 20 Diritto di accesso

Il presente Regolamento tiene conto della disciplina del GDPR in tema di diritto di accesso 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. 21 Diritto alla rettifica e cancellazione

Il presente Regolamento tiene conto della disciplina del 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", 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:

- 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; o
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Art. 22 Diritto alla limitazione

Il presente Regolamento tiene conto della disciplina del 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) benchè 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. 23 Diritto alla portabilità

Il presente Regolamento tiene conto della circostanza che, in forza della disciplina del 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.

Art. 24 Diritto di opposizione e processo decisionale automatizzato relativo alle persone

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del GDPR, compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli 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 riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Art. 25 Modalità di esercizio dei diritti dell'interessato

Per l'esercizio dei diritti dell'interessato, in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni del GDPR, del Codice e del presente Regolamento.

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, come ad esempio, la conoscenza personale;
- 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, 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 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.

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.

All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa.

I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.

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.

Il titolare si conforma alle Linee guida del Garante in tema di esercizio dei diritti dell'interessato.

Art. 26 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.

Il titolare si conforma alle Linee guida del Garante in tema di indagini difensive.

CAPO V - SOGGETTI

Art. 27 Titolare e contitolari

Il titolare del trattamento è il Comune di XXX, rappresentato dal Sindaco pro tempore, in qualità di legale rappresentante del titolare, con sede in via xxx n. xxx, xxx.

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 Codice, al GDPR e al presente Regolamento;

- a delegare ovvero a nominare, con proprio atto, i dirigenti/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 dei dirigenti/P.O., delegati o nominati, e a pubblicarlo sul sito web istituzionale del titolare;
- a designare, con proprio atto, il Responsabile per la protezione dei dati personali;
- a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
- a favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
- a favorire l'adesione a 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 quando determinano congiuntamente le finalità e i mezzi del trattamento.

I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e dal presente Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che 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 può designare un punto di contatto per gli interessati. L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale 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.

Art. 28 Dirigenti e Responsabili di Posizione organizzativa-P.O.

Il titolare conferisce i sotto indicati compiti e funzioni, e i correlati poteri, mediante apposito provvedimento di delega o di nomina, da adottarsi secondo il proprio ordinamento ai:

- dirigenti/ P.O.

Nel suddetto provvedimento, il titolare deve informare ciascun dirigente/ P.O., delle responsabilità che gli sono affidate in relazione a quanto disposto dal Codice, dal GDPR e dal presente Regolamento.

Compiti, funzioni e poteri:

- trattare i dati personali solo su istruzione del titolare del trattamento;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare il tempestivo ed integrale rispetto dei doveri del titolare previsti dal Codice, compreso

il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;

- osservare le disposizioni del presente Regolamento nonché delle specifiche istruzioni impartite dal titolare;
- adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute nel presente Regolamento, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;
- collaborare con il titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti del titolare, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
- curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'organizzazione del titolare per l'applicazione del Codice, del GDPR, e del presente Regolamento;
- assistere il titolare del trattamento con misure tecniche ed 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 per quanto previsto nella normativa vigente;
- assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel Codice, GDPR e nel presente Regolamento;
- contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente regolamento, comprese le ispezioni, realizzate dal titolare o da un altro soggetto da questi incaricato;
- curare la costituzione e l'aggiornamento dei seguenti archivi/banche dati, per quanto di competenza:
  - elenco dei contitolari, dei responsabili dei trattamenti, e degli incaricati, con i relativi punti di contatto;
  - elenco degli archivi/ banche;
- garantire l'aggiornamento, almeno annuale, della ricognizione dei trattamenti;
- fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

Ciascun dirigente/P.O., nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, collabora con il titolare al fine di:

- comunicare tempestivamente, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative

adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato; la redazione della valutazione d'impatto sulla protezione dei dati; la consultazione preventiva;

- predisporre le informative previste e verificarne il rispetto e fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;
- designare gli incaricati del trattamento, e fornire loro specifiche istruzioni;
- rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
- garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del titolare ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;
- informare il titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

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.
I dirigenti/P.O. sono destinatari degli interventi di formazione di aggiornamento.

Art. 29 Responsabili del trattamento e sub responsabili

Il Responsabile è il soggetto che agisce per conto del titolare.
Il Responsabile è designato dal titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Il Responsabile del trattamento non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del titolare.
Il titolare, in considerazione della complessità e della molteplicità delle funzioni istituzionali, può designare quali Responsabili del trattamento dei dati personali, unicamente i soggetti 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 (GDPR, art. 28).
I Responsabili del trattamento hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia;
- rispettare le misure di sicurezza previste dal Codice sulla privacy e adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di

distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

- nominare al loro interno i soggetti incaricati del trattamento;
- garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;
- trattare i dati personali, anche di natura sensibile e sanitaria esclusivamente per le finalità previste dal contratto o dalla convenzione;
- attenersi alle disposizioni impartite dal Titolare del trattamento;
- specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
- comunicare le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

Nel caso di mancato rispetto delle predette disposizioni, e in caso di mancata comunicazione al titolare dell'atto di nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso il titolare, il Responsabile del trattamento.
La designazione del Responsabile viene effettuata mediante atto da parte del titolare del trattamento da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente al titolare.
L'accettazione della nomina e l'impegno a rispettare le disposizioni del Codice, del GDPR e del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 30 Incaricati del trattamento dipendenti del titolare

Gli incaricati del trattamento sono le persone fisiche, dipendenti del titolare, designati da ciascun dirigente/P.O., 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.
La designazione dell'incaricato al trattamento dei dati personali è di competenza del dirigente/P.O.; la nomina è effettuata per iscritto e individua specificatamente i compiti spettanti all'incaricato e le modalità cui deve attenersi per l'espletamento degli stessi e 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, "incaricato" ai sensi dell'art. 2-quaterdecies del Codice nonché ai sensi degli artt. 4 comma 10 e art. 29 del GDPR.
Gli incaricati devono 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 incaricati 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 incaricati devono assicurare che, nel corso del trattamento, i dati siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- 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;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità pel quali i dati sono trattati;
- trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

Gli incaricati sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propri 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 incaricati dipendenti del titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 31 Incaricati del 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 e i soggetti che operano temporaneamente all'interno della struttura organizzativa del titolare o incaricati nominati dal Responsabile esterno, devono essere incaricati del trattamento tramite atto scritto di nomina.
Questi ultimi sono soggetti agli stessi obblighi cui sono sottoposti tutti gli incaricati dipendenti del titolare, in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
Gli incaricati non dipendenti dal titolare sono destinatari degli interventi di formazione di aggiornamento.

Art. 32 Amministratore di sistema

L'amministratore di sistema, individuato nel Responsabile del Centro Elaborazione Dati, 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 deve avvenire 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.

Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, 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.

Il titolare di sistema applica le disposizioni impartite dal Garante in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

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

Art. 33 Responsabile della protezione dei dati personali (RPD) - Data Protection Officer (DPO)

Il Titolare designa il Responsabile della protezione dei dati (RPD/DPO).

Il RPD/PDO deve essere in possesso di:

- un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
- deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

Il RPD/PDO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.

Il RPD/PDO svolge i seguenti compiti:

- informa e fornisce consulenze 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, pareri 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.

CAPO VI - SICUREZZA DEI DATI PERSONALI

Art. 34 Misure di sicurezza

Il titolare, nel trattamento dei dati personali, garantisce l'applicazione di adeguate misure di sicurezza

che consentono di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
In particolare il titolare del trattamento mette in atto misure e tecniche, organizzative, di gestione, procedurali e documentali adeguate per garantire un livello di sicurezza adeguato al rischio. Tali misure che comprendono almeno:

- la pseudonimizzazione e la cifratura dei dati personali trattati;
- procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

ART. 35 Valutazione d'impatto sulla protezione dei dati- DPIA

La valutazione d'impatto sulla protezione dei dati (di seguito solo "DPIA") è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
La DPIA è uno strumento importanti per la responsabilizzazione in quanto sostiene il titolari non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del medesimo GDPR.
La DPIA sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, intendendosi per "rischio" uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, e per "gestione dei rischi" l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
Prioritariamente alla DPIA deve:
- essere effettuata o aggiornata la ricognizione dei trattamenti.
- essere effettuata la determinazione in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati.

La decisione in ordine alla possibilità che il trattamento possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA, fermo restando l'elenco dei trattamenti per i quali la DPIA è obbligatoria e di cui all'Allegato 1 al provvedimento del Garante n. 467 del 11 ottobre 2018, viene adottata applicando i casi indicati l'art. 35, paragrafo 3 del GDPR e i criteri esplicativi contenuti nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida").
Nell'applicare i suddetti criteri si deve tenere conto di quanto segue:

- la DPIA è sempre obbligatoria, indipendentemente dalla presenza di uno o più criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dall'Autorità di controllo ai sensi dell'art. 35, paragrafo 4 GDPR e rappresentata dall'Allegato 1 al

provvedimento del Garante n. 467 del 11 ottobre 2018;

- la DPIA è sempre obbligatoria per i trattamenti inclusi nell'indice dei trattamenti dei dati sensibili e giudiziari ai sensi del Regolamento sul trattamento dei dati sensibili e giudiziari approvato dall'Ente conformemente allo schema tipo del Garante;
- fermo restando che, secondo le Linee guida, un trattamento che soddisfa 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati, tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio costituisce elemento sufficiente per originare l'obbligo di svolgimento della DPIA;
- maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;
- se, pur applicando i criteri sopra indicati, la necessità di una DPIA non emerge con chiarezza, va comunque ritenuto sussistente l'obbligo - secondo quanto raccomandato dal WP29 - di farvi ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento.

La DPIA non è richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche";
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) GPDR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR).

La DPIA deve contenere almeno:

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

Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.
Per conseguire l'obiettivo della riduzione del rischio la DPIA, tenuto conto dei principi contenuti nelle pertinenti norme UNI ISO (31000 e 27001) nonché degli orientamenti contenuti nelle Linee guida e, in

particolare, nell'Allegato n. 2, si svolge attraverso le fasi, di seguito indicate, previste dall'art. 35, paragrafo 7 del GDPR:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1, art. 35 del GDPR;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il Responsabile della protezione dei dati.
Laddove la DPIA riveli la presenza di rischi residui elevati, il titolare è tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento ai sensi dell' art. 36, paragrafo 1 GDPR.

Art. 36 Pubblicazione sintesi della valutazione d'impatto – DPIA

Il titolare effettua la pubblicazione della DPIA o di una sintesi della stessa al fine di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare, nonché 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. 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. 37 Consultazione preventiva

Il titolare, prima di procedere al trattamento dei dati, consulta, per il tramite del RPD/PDO, il Garante qualora la valutazione d'impatto sulla protezione dei dati abbia evidenziato che il trattamento potrebbe presentare un rischio elevato in assenza di misure adottate.

ART. 38 Modulistica e procedure

Il titolare, al fine di agevolare e semplificare la corretta e puntuale applicazione delle disposizioni del Codice, del GDPR, del presente Regolamento, e di tutte le linee guida e provvedimenti del Garante
a) adottata e costantemente aggiorna:

- modelli uniformi di informativa;
- 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. 39 Responsabilità in caso di violazione delle disposizioni in materia di protezione dei dati personali

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è sanzionato con le sanzioni previste dall'art. 166 del Codice e 83 del Regolamento da parte del Garante, nonché con sanzioni di natura disciplinare.

Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.

Il Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi previsti nel Codice, nel GDPR e nel presente regolamento, e a lui specificamente diretti o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal titolare del trattamento.

Il Titolare e il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non è in alcun modo loro imputabile.

Art. 40 Notificazione di una violazione dei dati personali

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante 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 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.

La notifica deve almeno:

a) 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;

b) 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;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) 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.

Art. 41 Comunicazione di una violazione dei dati personali

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 del presente articolo 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.

Art. 42 Disposizioni finali

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

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

Avv. Nadia Corà
Avv. Guido Paratico

OBČINA SOVODNJE OB SOČI

Pravilnik
o varstvu
osebnih podatkov
sprejet na podlagi Uredbe (EU) 2016/679

Sprejet s sklepom občinskega sveta št. 4 dne 27. 2. 2020

Avv. Nadia Corà
Avv. Guido Paratico

KAZALO

Avv. Nadia Corà
Avv. Guido Paratico

Avv. Nadia Corà
Avv. Guido Paratico

UVOD

27. aprila 2016 je bila sprejeta Uredba (EU) 2016/679 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
Nova uredba EU, ki za države članice velja od 25. maja 2018, temelji na predpostavki, da varstvo fizičnih oseb v zvezi z obdelavo osebnih podatkov predstavlja temeljno pravico, kar potrjuje tudi dejstvo, da člen 8, odstavek 1 Listine Evropske unije o temeljnih pravicah (»listina«) in člen 16, odstavek 1 Pogodbe o delovanju Evropske unije (»PDEU«), določata, da ima vsak človek pravico do varstva osebnih podatkov, ki se nanašajo nanj.
Uredba EU za okrepitev varstva vnaša številne pomembne novosti, začenši pri pristopu, ki temelji na načelu previdnosti, v zvezi s tveganji, ki obstajajo pri obdelavi, in ukrepi za prevzemanje odgovornosti s strani upravljavcev in obdelovalcev (kot na primer ocena vpliva, evidenca obdelave, varnostni ukrepi, imenovanje DPO).
Kot je že izpostavil varuh osebnih podatkov v vodniku za izvajanje Uredbe, nova evropska ureditev odločno poudarja pomen »prevzemanja odgovornosti« (accountability) za upravljavce in obdelovalce oziroma pomen proaktivnega ravnanja, s katerim se dokazuje konkretno sprejemanje ukrepov, namenjenih zagotavljanju izvajanja Uredbe. Med merili, ki so jih upravljavci in obdelovalci dolžni uporabljati pri izpolnjevanju obveznosti, so:

- merilo *»data protection by default and by design«* (vgrajeno in privzeto varstvo podatkov) oziroma potreba po tem, da se obdelava zastavi na tak način, da so že od začetka zagotovljena nujna jamstva »z namenom, da se izpolnjujejo zahteve« iz uredbe in zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki, pri čemer se upoštevajo skupni kontekst, v katerega se umešča obdelava, in tveganja za pravice ter svoboščine posameznikov,
- merilo tveganja, povezanega z obdelavo, mišljeno kot tveganje za negativne posledice na svoboščinah in pravicah posameznikov, pri čemer morajo biti takšne posledice preučene skozi ustrezen proces ocenjevanja ob upoštevanju znanih in dokazljivih tveganj ter tehničnih in organizacijskih ukrepov (tudi varnostnih), za katere upravljavec meni, da jih je ustrezno sprejeti, da se takšno tveganje ublaži.

Zato se ukrepanje nadzornega organa v novem načinu ureditve v glavnem izvaja »ex post« oziroma se umešča v čas po tistem, ko je upravljavec odločitve samostojno sprejel. Zaradi tega so bili s 25. majem 2018 razveljavljeni nekateri inštituti, predvideni po direktivi iz leta 1995 in po italijanskem zakoniku, kot na primer vnaprejšnje obvestilo o obdelavi podatkov, posredovano nadzornemu organu, in tako imenovano predhodno preverjanje (prior checking), ki ju je nadomestilo obvezno vodenje evidence o dejavnostih obdelave s strani upravljavca/obdelovalca in povsem samostojno ocenjevanje vpliva.
Iz obravnave omenjenega področja tako izhaja, da je nujno spremeniti način razmišljanja, saj je z njim treba zagotoviti polno varstvo osebnih podatkov, s čimer ni mišljeno zgolj upoštevanje administrativnih obveznosti, ki terja veliko truda, temveč zlasti jamstvo za državljana, ki se obrne na organe javne uprave, da ti zagotavljajo popolno zaupnost z dejanskega in vsebinskega stališča.
Pravica do varstva osebnih podatkov je nekršljiva osebna pravica, ki ni omejena na varstvo zaupnosti in zaščito podatkov, temveč vključuje celovito spoštovanje pravic in temeljnih svoboščin ter dostojanstva. Zato mora kultura varstva osebnih podatkov rasti in se krepiti zlasti med delavci v javni upravi, saj lahko ti, ob vsaj minimalnem poznavanju temeljnih načel, na katerih temeljijo

predpisi, ustrezno izvajajo vse zakonske obveznosti, povezane z obdelavo podatkov v pristojnosti posameznega organa ob hkratnem zavedanju, da ne gre za nekoristno breme, temveč se na tak način konkretno prispeva k izboljševanju kakovosti odnosov s strankami.
Upravljavec želi svoje predpise urediti in uskladiti, urediti novosti, ki ji uvaja navedena uredba EU, ob zagotovilu, da se bo ta posodobitev v prihodnje še nadgrajevala skladno s kasnejšimi smernicami varuha osebnih podatkov, namenjenih varstvu osebnih podatkov oziroma novostim s področja predpisov in sodne prakse.
Varstvo osebnih podatkov je urejeno še z drugim predpisom oziroma z Zakonsko uredbo št. 196 z dne 30. junija 2003, kot je spremenjena z Zakonsko uredbo št. 101 z dne 10. avgusta 2018.

Avv. Nadia Corà
Avv. Guido Paratico

RAZDELEK I – SPLOŠNA DOLOČILA

Člen 1 Pojmi

Ta Pravilnik vsebuje naslednje pojme:

- **»Zakonik«**: Zakonska uredba 196/2003, kot je spremenjena z Zakonsko uredbo 101/2018;
- **»GDPR«:** Uredba (UE) 2016/679 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov),
- **»Pravilnik o občutljivih podatkih«:** interni pravilnik, ki ga sprejme upravljavec skladno s tipskim obrazcem, ki ga odobri varuh osebnih podatkov, s katerim se za obdelavo občutljivih in sodnih podatkov opredelijo tipi podatkov ter postopki, ki se lahko izvajajo,
- **»Pravilnik«:** ta pravilnik,
- **»upravljavec«:** občina oziroma upravni organ, ki sprejme ta pravilnik, Občina Sovodnje ob Soči - Comune di Savogna d'Isonzo, s sedežem v Sovodnjah ob Soči, Ulica prvega maja 140, 34070 Sovodnje ob Soči (GO),
- **»vodstveni delavci/nosilci organizacijskega položaja (OP)«**: osebe, ki izvajajo pooblastila, katera dodeli upravljavec oziroma jih upravljavec imenuje za izvajanje takšnih pooblastil.

Ta pravilnik vsebuje pojme iz Zakonske uredbe št. 196/2003 in iz GDPR, pri čemer se v primeru razhajanj kot prevladujoči štejejo pojmi, vsebovani v obeh predpisih:

pojmi za namene po GDPR:

- **»osebni podatek«:** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (»posameznikom, na katerega se nanašajo osebni podatki«); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
- **»obdelava«:** pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;
- **»omejitev obdelave«:** pomeni označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;
- **»oblikovanje profilov«:** pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;
- **»psevdonimizacija«:** pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;

- **»zbirka«:** pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
- **»upravljavec«:** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;
- **»obdelovalec«:** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- **»uporabnik«:** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
- **»tretja oseba«:** pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
- **»privolitev posameznika, na katerega se nanašajo osebni podatki«:** pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj;
- **»kršitev varstva osebnih podatkov«:** pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
- **»genetski podatki«:** pomeni osebne podatke v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;
- **»biometrični podatki«:** pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;
- **»podatki o zdravstvenem stanju«:** pomeni osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;
- **»glavni sedež«:**
    a) v zvezi z upravljavcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, kadar se odločitve o namenih in sredstvih obdelave osebnih podatkov sprejemajo na drugem sedežu upravljavca v Uniji in ima ta sedež pooblastila za izvajanje takih odločitev, sedež, ki sprejema take odločitve;
    b) v zvezi z obdelovalcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, če obdelovalec nima osrednje uprave v Uniji, sedež obdelovalca v

Uniji, kjer se izvajajo glavne dejavnosti obdelave v okviru dejavnosti sedeža obdelovalca, kolikor za obdelovalca veljajo posebne obveznosti iz te uredbe;

- **»predstavnik«:** pomeni fizično ali pravno osebo s sedežem v Uniji, ki jo pisno imenuje upravljavec ali obdelovalec v skladu s členom 27 GDPR in ki predstavlja upravljavca ali obdelovalca v zvezi z njegovimi obveznostmi iz te uredbe;
- **»podjetje«:** pomeni fizično ali pravno osebo, ki opravlja gospodarsko dejavnost, ne glede na njeno pravno obliko, vključno s partnerstvi ali združenji, ki redno opravljajo gospodarsko dejavnost;
- **»povezana družba«:** pomeni obvladujočo družbo in njene odvisne družbe;
- **»zavezujoča poslovna pravila«:** pomeni politike na področju varstva osebnih podatkov, ki jih upravljavec ali obdelovalec s sedežem na ozemlju države članice spoštuje pri prenosih ali nizih prenosov osebnih podatkov upravljavcu ali obdelovalcu povezane družbe ali skupine podjetij, ki opravljajo skupno gospodarsko dejavnost, v eni ali več tretjih državah;
- **»nadzorni organ«:** pomeni neodvisen javni organ, ki ga v skladu s členom 51 GDPR ustanovi država članica;
- **»zadevni nadzorni organ«:** pomeni nadzorni organ, ki ga obdelava osebnih podatkov zadeva, ker:
  - ima upravljavec ali obdelovalec sedež na ozemlju države članice tega nadzornega organa,
  - obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, s prebivališčem v državi članici tega nadzornega organa,
    ali
  - je bila vložena pritožba pri tem nadzornem organu;
- **»čezmejna obdelava osebnih podatkov«: pomeni**
  - obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti sedežev upravljavca ali obdelovalca v več kot eni državi članici, kadar ima upravljavec ali obdelovalec sedež v več kot eni državi članici,
    ali
  - obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edinega sedeža upravljavca ali obdelovalca, vendar obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici;
- **»ustrezen in utemeljen ugovor«:** pomeni ugovor osnutku odločitve glede tega, ali je bila uredba kršena, oziroma glede tega, ali je predvideno ukrepanje v zvezi z upravljavcem ali obdelovalcem v skladu s to uredbo, kar jasno navede pomen tveganja, ki ga predstavlja osnutek odločitve, kar zadeva temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in – kjer je to ustrezno – prosti pretok osebnih podatkov v Uniji,
- **»storitev informacijske družbe«:** pomeni storitev, kakor je opredeljena v točki (b) člena 1(1) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta,
- **»mednarodna organizacija«:** pomeni organizacijo in njena podrejena telesa, ki jih ureja mednarodno javno pravo ali kateri koli drugo telo, ustanovljeno s sporazumom med dvema ali več državami ali na podlagi takega sporazuma.

Člen 2 Referenčni predpisi

Ta pravilnik upošteva naslednje dokumente:

- Zakonik s področja osebnih podatkov, ki vsebuje določila za prilagoditev pravnega reda določilom Uredbe (EU) št. 679/2016 (Uredba z zakonsko močjo 196/2003, kot je spremenjena z Uredbo z zakonsko močjo 101/2018);
- Smernice in priporočila varuha osebnih podatkov,
- GDPR EU 679/2016 Evropskega parlamenta in sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES,
- Zakon št. 163 z dne 25. oktobra 2017 (člen 13), ki vsebuje pooblastilo za uskladitev nacionalne zakonodaje z določili GDPR EU 2016/679 Evropskega parlamenta in sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES,
- Zakonska uredba 101/2018 o uskladitvi internih predpisov GDPR,
- izjava delovne skupine po 29. členu o varstvu osebnih podatkov (WP29) - 14/EN,
- Smernice o pooblaščenih osebah za varstvo podatkov (DPO) - WP243, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 13. decembra 2016,
- Smernice o pravici do »prenosljivosti podatkov« - WP242, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 13. decembra 2016,
- Smernice za opredelitev vodilnega nadzornega organa upravljavca ali obdelovalca - WP244, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 13. decembra 2016,
- Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je »verjetno, da bi obdelava povzročila veliko tveganje« za namene Uredbe 2016/679 - WP248, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 4. aprila 2017,
- Smernice, ki jih je izdelala delovna skupina iz člena 29 na področju smernic o uporabi in določanju upravnih glob - WP253, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 3. oktobra 2017,
- Smernice, ki jih je izdelala delovna skupina iz člena 29 o profiliranju in avtomatiziranem odločanju po GDPR - WP251, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 6. februarja 2018,
- Smernice, ki jih je izdelala delovna skupina iz člena 29 o obveščanju o kršitvi varnostnih osebnih podatkov (data breach notification) - WP250, ki jih je sprejela delovna skupina za varstvo podatkov iz člena 29 dne 6. februarja 2018,
- Mnenje WP29 o omejitvi namena - 13/EN WP 203,
- priloga 1 k Odločbi št. 467 z dne 11. oktobra 2018 »Seznam tipov obdelave, za katere se upošteva mehanizem skladnosti, ki se predloži v oceno posledic«,
- mednarodni predpisi,
- interni pravilniki, ki jih sprejmejo upravljavci in/oziroma obdelovalci.

Člen 3 Namen pravilnika

Pravilnik je namenjen varstvu pravic in svoboščin fizičnih oseb v zvezi z obdelavo osebnih podatkov s

strani upravljavca ob upoštevanju določil GDPR.
Ta pravilnik v celoti nadomesti Pravilnik o občutljivih podatkih, sprejet s sklepom občinskega sveta št. 2 z dne 16. 1. 2006, posodobljen s sklepom občinskega sveta št. 4 z dne 27. 2. 2020, pri čemer ostanejo v veljavi preglednice/tabele, priložene Pravilniku, s katerimi so določeni tipi občutljivih in sodnih podatkov, za katere je dovoljena zadevna obdelava ter postopki, ki se izvajajo glede na posamezne cilje v pomembnejšem javnem interesu, ki se izvajajo v posameznih primerih in jih izrecno navaja zakon, kateri se še naprej izvajajo in se priložijo temu Pravilniku ter postanejo njegov sestavni in bistven del.

Člen 4 Cilji

Upravljavec zagotavlja, da bo za namene varnosti fizičnih oseb obdelava potekala ob spoštovanju pravic in temeljnih svoboščin ter dostojanstva posameznika, na katerega se nanašajo osebni podatki, zlasti glede zaupnosti, osebne identitete in pravice do varstva osebnih podatkov, ne glede na njihovo državljanstvo oziroma stalno prebivališče.
Upravljavec v okviru svojih funkcij upravlja z zbirkami in bazami podatkov ter spoštuje pravice, temeljne svoboščine in dostojanstvo oseb, zlasti glede zaupnosti in osebne identitete.
Za zaščito pravic in svoboščin fizičnih oseb pri obdelavi osebnih podatkov se vsi procesi, vključno z administrativnimi postopki v pristojnosti upravljavca, vodijo skladno z določili Zakonika, GDPR in tega Pravilnika.

RAZDELEK II - NAČELA

Člen 5 – Načela in prevzemanje odgovornosti

V notranjo ureditev upravljavca se v celoti sprejmejo načela GDPR, na podlagi katerih:

a) se osebni podatki obdelujejo zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo osebni podatki (»zakonitost, pravičnost in preglednost«);
b) se osebni podatki zbirajo v določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni; nadaljnja obdelava v namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene ne velja za nezdružljivo s prvotnimi nameni (»omejitev namena«);
c) so osebni podatki ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (»najmanjši obseg podatkov«);
d) so osebni podatki točni in, kadar je to potrebno, posodobljeni; sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo na podlagi načela »točnosti«;
e) so osebni podatki hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo; osebni podatki se lahko shranjujejo za daljše obdobje, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene v skladu s členom 89(1), pri čemer je treba izvajati ustrezne tehnične in organizacijske ukrepe iz te uredbe, da se zaščitijo pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki na podlagi načela »omejitve shranjevanja«;
f) osebni podatki se obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov,

vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi na podlagi načel »celovitosti in zaupnosti«;

g) osebni podatki so zasnovani z minimalno uporabo osebnih identifikacijskih podatkov, s čimer se izključi obravnava, če se cilji lahko izvajajo z anonimnimi podatki oziroma na ustrezne načine, ki omogočajo identifikacijo posameznika samo, če je to potrebno *(»načelo potrebe«)*.

Upravljavec je dolžan spoštovati zgoraj navedena načela in lahko to dokaže po načelu »prevzemanja odgovornosti«.

Člen 6 Zakonitost obdelave

Upravljavec je v notranjo ureditev v celoti sprejel določila GDPR glede zakonitosti obdelave in posledično je obdelava upravičena samo če je podan najmanj eden izmed naslednjih pogojev in v tolikšni meri, kolikor je najmanj takšen pogoj podan:

a) posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
b) obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
c) obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;
d) obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
e) obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu;
f) obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

Točka (f) prvega pododstavka se ne uporablja za obdelavo s strani javnih organov pri opravljanju njihovih nalog.

Kadar obdelava podatkov za drug namen kot za tistega, za katerega so bili osebni podatki zbrani, ne temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki, ali na pravu Unije ali pravu države članice, kar predstavlja potreben in sorazmeren ukrep za uresničevanje ciljev iz člena 23(1), upravljavec, da bi ocenil, ali je obdelava za drug namen združljiva z namenom, za katerega so bili osebni podatki prvotno zbrani, med drugim upošteva:

a) kakršno koli povezavo med nameni, za katere so bili osebni podatki zbrani, in nameni načrtovane nadaljnje obdelave;
b) okoliščine, v katerih so bili osebni podatki zbrani, zlasti kar zadeva razmerje med posamezniki, na katere se nanašajo osebni podatki, in upravljavcem;
c) naravo osebnih podatkov, zlasti ali se obdelujejo posebne vrste osebnih podatkov v skladu s členom 9 GDPR ali pa se obdelujejo osebni podatki v zvezi s kazenskimi obsodbami in prekrški v skladu s členom 10 GDPR;
d) morebitne posledice načrtovane nadaljnje obdelave za posameznike, na katere se nanašajo osebni podatki;
e) obstoj ustreznih zaščitnih ukrepov, ki lahko vključujejo šifriranje ali psevdonimizacijo.

Člen 7 Pogoji za privolitev

Ob nespremenjeni veljavi primerov, urejenih po členu 6 GDPR in členih 2-ter in 2-sexies Zakonika, v katerih se lahko obdelava zakonito izvede brez privolitve, v primeru, da je za obdelavo osebnih podatkov v enega ali več specifičnih namenov zahtevana privolitev posameznika, se upošteva ureditev po GDPR, ki predvideva da:

- kadar obdelava temelji na privolitvi, mora biti upravljavec zmožen dokazati, da je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo svojih osebnih podatkov;
- če je privolitev posameznika, na katerega se nanašajo osebni podatki, dana v pisni izjavi, ki se nanaša tudi na druge zadeve, se zahteva za privolitev predloži na način, ki se jasno razlikuje od drugih zadev, v razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Deli take izjave, ki predstavljajo kršitev te uredbe, niso zavezujoči;
- Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da svojo privolitev kadar koli prekliče.
  Preklic privolitve ne vpliva na zakonitost obdelave, ki temelji na privolitvi, podani pred njenim preklicem. O tem se pred privolitvijo obvesti posameznika, na katerega se nanašajo osebni podatki. Privolitev je enako enostavno preklicati kot dati,
- Pri ugotavljanju, ali je bila privolitev dana prostovoljno, se med drugim zlasti upošteva, ali je izvajanje pogodbe, vključno z zagotavljanjem storitve, pogojeno s privolitvijo v obdelavo osebnih podatkov, ki ni potrebna za izvedbo zadevne pogodbe.
- za občutljive podatke mora biti privolitev izrecna in v pisni obliki; enako velja za privolitev k odločitvam, ki temeljijo na avtomatizirani obdelavi, vključno z oblikovanjem profila;
- privolitev za otroka je veljavna od 16. leta starosti, pri čemer je možno določiti tudi drugačno starostno omejitev, vendar ne manj kot 13 let starosti skladno z nacionalnimi predpisi; pred upoštevanjem zakonske omejitve po nacionalnih predpisih je treba pridobiti privolitev staršev oziroma skrbnikov;
- v vseh ostalih primerih mora biti podana prosto, samostojno, specifično, na obveščen in nedvoumen način. Tiha ali domnevna privolitev ni dovoljena (vnaprej izpolnjena okenca na obrazcu niso veljavna);
- privolitev mora biti dana z »izjavo ali jasnim pritrdilnim dejanjem«.

Če je privolitev posameznika, na katerega se nanašajo osebni podatki, dana v pisni izjavi, ki se nanaša tudi na druge zadeve, se zahteva za privolitev predloži na način, ki se jasno razlikuje od drugih zadev, v razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Deli take izjave, ki predstavljajo kršitev GDPR in tega pravilnika, niso zavezujoči.

V primeru fizične nezmožnosti, poslovne nesposobnosti oziroma opravilne nesposobnosti posameznika, zdravstvenega izrednega dogodka ali javne higiene, hujše grozeče nevarnosti za zdravje posameznika, se privolitev lahko brez zamude pridobi tudi potem, ko jo poda oseba, ki pravno zastopa posameznika oziroma njegov bližnji sorodnik, družinski član ali oseba, ki s posameznikom živi v skupnem gospodinjstvu.

Če prijava temelji na privolitvi, jo posameznik poda tako, da izpolni ustrezen obrazec, ki ga pripravi upravljavec, po predhodni izročitvi in seznanitvi z obvestilom.

Tiho ali domnevno soglasje oziroma uporaba vnaprej označenih okenc za obrazcu niso dovoljeni.

Upravljavec sprejme ustrezne organizacijske ukrepe, da posameznik lažje poda soglasje.
Posameznik soglasje poda ob prvem dostopu do storitev. Soglasje velja in učinkuje do preklica oziroma za mladoletne do dopolnjenega osemnajstega leta starosti.
Soglasje se vpiše v evidenco dejavnosti obravnave.

Člen 8 Obvestilo

Upravljavec je ob zbiranju osebnih podatkov dolžan posamezniku, ki ga lahko zastopa tudi osebni pooblaščenec, podati ustrezne informacije na načine, predvidene po GDPR, v strnjeni, pregledni, razumljivi in lahko dostopni obliki v preprostem in jasnem jeziku, zlasti glede informacij, posebej namenjenih mladoletnim osebam.
Informacije se načeloma podajajo pisno in po možnosti v elektronski obliki, zlasti pri spletnih storitvah, čeprav so dovoljena tudi druga sredstva in se lahko podajo tudi ustno, vendar ob upoštevanju zgoraj navedenih značilnosti.
Obvestilo je lahko podano tudi z ustreznimi sredstvi:

- z ustreznimi obrazci, ki se izročijo posameznikom. Na obrazcu so navedene osebe, na katere se lahko uporabnik lahko obrne za dodatne informacije in za uveljavljanje svojih pravic, tudi z namenom vpogleda v posodobljen seznam odgovornih oseb;
- javnosti dobro vidnimi obvestili, izobešenimi v prostorih, skozi katere se dostopa v objekte upravljavca, v čakalnicah in drugih prostorih, kamor dostopajo uporabniki oziroma se posredujejo z institucionalnimi objavami in z objavo na spletni strani upravljavca;
- ustreznim obvestilom, vnesenim v pogodbe oziroma v dopise o določitvi delovnih nalog zaposlenim, osebam, s katerimi se vzpostavlja sodelovanje oziroma, ki delajo v okviru samostojne intelektualne dejavnosti, pripravnikom, prostovoljcem, udeležencem delovnih usposabljanj oziroma drugim osebam, ki sodelujejo z upravljavcem;
- podano ob objavi razpisov, obvestil, pozivov k sodelovanju, z navedbo zadolženega za obdelavo osebnih podatkov, povezanih s postopki.

Obvestilo se posameznikom lahko posreduje tudi v kombinaciji s standardiziranimi ikonami na tak način, da se na viden, razumljiv in enostavno čitljiv način posreduje celovit opis obravnavane obdelave. Če so posredovane v elektronski obliki, morajo biti ikone takšne, da jih lahko odčita avtomatska naprava.

Obvestilo vsebuje najmanj naslednjo vsebino:

- identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja;
- kontaktne podatke o pooblaščeni osebi za varstvo podatkov/DPO, če obstaja;
- namene, za katere se osebni podatki obdelujejo,
- uporabnike podatkov;
- pravno osnovo obdelave;
- zakonit interes upravljavca, če ta predstavlja pravno osnovo za obdelavo;
- če upravljavec posreduje osebne podatke v tretje države in če je temu tako, preko katerih instrumentov;
- čas hrambe podatkov oziroma meril, upoštevanih za določanje časa hrambe;

- obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;
- pravico do vložitve pritožbe pri nadzornem organu;
- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

V primeru, da osebni podatki niso bili pridobljeni od posameznika:
a) je upravljavec posamezniku, na katerega se nanašajo osebni podatki, dolžan zagotoviti naslednje informacije:

- kategorije osebnih podatkov, ki se obdelujejo;
- od kje izvirajo osebni podatki in po potrebi, ali izvirajo iz javno dostopnih virov;

b) obvestilo mora biti podano v razumnem roku, ki ne sme biti daljši od 1 meseca od zbiranja oziroma od trenutka obvestila (in ne shranjevanja) podatkov tretjim osebam oziroma posamezniku.
Za obdelavo podatkov, povezano z vodenjem delovnega razmerja z zaposlenimi pri upravljavcu, je pripravljeno posebno obvestilo za zaposlene.
Ustrezna obvestila morajo biti vnesena v naslednje dokumente:

- v razpise in v dokumentacijo o izbiri dobaviteljev/izvajalcev za javna naročila, v pogodbe, dogovore oziroma sporazume, v postopkih javnega naročanja, pri prijavi nepravilnega delovanja in na splošno v vse druge dokumente, ki vsebujejo osebne podatke.

Pri posredovanju obvestila se je upravljavec dolžan izrecno sklicevati na predpise, ki določajo obveznosti in naloge, na podlagi katerih se obdelujejo občutljivi in sodni podatki.

Člen 9 Ozaveščanje in obveščanje

Za namene pravilnega in doslednega izvajanja ureditve, povezane z načeli in zakonitostjo obdelave, s soglasjem, obveščanjem in bolj na splošno varstvom osebnih podatkov, upravljavec podpira in znotraj svoje organizacijske strukture spodbuja uporabo vseh sredstev za ozaveščanje, ki lahko izboljšajo ozaveščenost o pomenu zaupnosti podatkov in izboljšajo kakovost storitve.
V zvezi z navedenim ta pravilnik priznava kot enega izmed osnovnih instrumentov ozaveščanja izobraževanje zaposlenih pri upravljavcu in neposredno obveščanje vseh, ki z njim sodelujejo.
Za zagotavljanje podrobnega poznavanja določil tega pravilnika se ob nastopu službe vsakemu zaposlenemu posreduje specifično obvestilo z ustreznim določilom, vnesenim v pogodbo o zaposlitvi, ki vsebuje vsa temeljna načela z obravnavanega področja, navedena preprosto, jasno in točno z navodili, kako pridobiti ta pravilnik, objavljen na spletni strani upravljavca.
Zaposleni se obveže, da bo pridobil izvod pravilnika, ga vpogledal in spoštoval njegova določila.
Upravljavec v okviru stalnega obveznega izobraževanja zaposlenih organizira posebne oblike izobraževanja in usposabljanja, tudi v povezavi z izobraževanjem s področja boja proti korupciji, zaščite osebnih podatkov, z namenom seznanjanja s predpisi, preprečevanja zlorab in nezakonitosti pri izvajanju predpisov, sprejemanja ustreznih modelov ravnanja in postopkov obdelave, seznanjanja z varnostnimi ukrepi za obdelavo in hrambo podatkov, ugotovljenimi tveganji in načini, da se

posameznikom prepreči nastanek škode.
Odgovorni za preprečevanje korupcije poskrbi za izobraževanje s področja preprečevanja tveganja za kršitve na področju osebnih podatkov v povezavi in usklajeno z izobraževanjem na področju preprečevanja korupcije in nezakonitosti ter z izobraževanjem s področja preglednosti in dostopanja, zlasti glede odnosov, ki se nanašajo na varstvo osebnih podatkov, preglednost dostopanja do upravnih dokumentov in dostopanja s strani državljanov na preprost in posplošen način na posameznih področjih, na katerih upravljavec posluje.
Sodelovanje zaposlenih pri izobraževanju se šteje kot element za merjenje in ocenjevanje kolektivne in osebne uspešnosti.

RAZDELEK III - OBDELAVA OSEBNIH PODATKOV

Člen 10 Obdelava osebnih podatkov, prepoznavanje obdelave in seznam obdelave

Upravljavec obdeluje osebne podatke za opravljanje svojih institucionalnih funkcij, kot jih določajo zakon, statut, in pravilniki, v mejah, kot jih nalagajo Zakonik, GDPR in smernice ter odločbe varuha osebnih podatkov.

V skladu z določili zakonov in pravilnikov upravljavec obdeluje osebne podatke, ki se primeroma, pri čemer navedba ni izčrpna, nanašajo na:

- vodenje kadrovskih zadev, vključno z zaposlovanjem,
- upravljanje z osebami, ki imajo pravne odnose z upravljavcem, če ne gre za delovno razmerje in ki iz katerega koli naslova delujejo znotraj organizacijske strukture upravljavca, vključno z osebami na delovnem izobraževanju, pripravniki in prostovoljci,
- vodenje odnosov s svetovalci, samostojnimi izvajalci intelektualnih storitev, dobavitelji za oskrbo z blagom in storitvami ter s podjetji, ki izvajajo dela oziroma opravljajo vzdrževanje,
- vodenje odnosov z akreditiranimi osebami, ki opravljajo socialno-varstvene storitve oziroma takšne storitve opravljajo na podlagi pogodb,
- vodenje odnosov z republiškim tožilstvom in drugimi pristojnimi javnimi organi v zvezi z inšpekcijskimi dejavnostmi spremljanja, nadzora in ugotavljanja kršitev zakonov ter pravilnikov.

Obdelavo osebnih podatkov lahko znotraj organizacijske strukture upravljavca opravljajo samo osebe, ki imajo za to ustrezno dovoljenje:

- upravljavec,
- vodstveni delavci/OP, kot osebe, ki izvajajo pooblastila, katera dodeli upravljavec oziroma jih upravljavec imenuje za izvajanje takšnih pooblastil,
- zaposleni kot pooblaščene osebe za obdelavo.

Nepooblaščene osebe osebnih podatkov ne smejo obdelovati.
Za namene obdelave upravljavec v sodelovanju z vodstvenimi delavci/OP zagotovi celotno prepoznavo in posodabljanje vseh obdelav osebnih podatkov, ki potekajo v okviru procesov in postopkov upravljavca in so namenjeni oblikovanju seznama obdelave.
Vodstveni delavci/OP so dolžni izvajati in dokumentirati redno, vsaj letno, posodabljanje pri prepoznavanju obdelave in s tem povezanem kazalniku, rednem medletnem ocenjevanju ob

upoštevanju načel iz člena 5 tega pravilnika za vse vrste obdelave, vključene v seznam.
Upravljavec, vodstveni delavci/OP in pooblaščene osebe upoštevajo načine obdelave, kot so navedeni v Zakoniku, GDPR in v izvedbenih določilih ter smernicah varuha osebnih podatkov, zlasti glede priloge 1 k Odločbi št. 467 z dne 11. oktobra 2018 »Seznam tipov obdelave, za katere se upošteva mehanizem skladnosti, ki se predložijo v oceno posledic«.

Člen 11 Tipi obdelanih podatkov

V okviru obdelav, vključenih v seznam obdelav, upravljavec pri izvajanju svojih institucionalnih nalog tudi na celoten in deloma avtomatiziran način obdeluje naslednje tipe podatkov:

- skupne identifikacijske podatke,
- občutljive podatke,
- sodne podatke.

Člen 12 Obdelava občutljivih in sodnih podatkov

Upravljavec prilagodi obdelavo občutljivih in sodnih podatkov na tak način, da se prepreči kršenje pravic, temeljnih svoboščin in dostojanstva posameznika.
V ta namen upravljavec upošteva načela člena 9, odstavka 1 GDPR in člena 2-sexies Zakonika ter spoštuje smernice varuha osebnih podatkov z navedenega področja.
Upravljavec ozavešča, seznanja, izobražuje in usposablja zaposlene na področju obdelave občutljivih in sodnih podatkov.

Člen 13 Obdelava občutljivih podatkov, povezanih z zdravjem

Upravljavec spoštuje določila 2-septies Zakonika ter Smernice varuha osebnih podatkov s področja obdelave občutljivih osebnih podatkov, povezanih z zdravjem.
Podatke, ki razkrivajo zdravstveno stanje in spolno življenje, obdelujejo ustrezno izobražene osebe in takšni podatki se za namene, ki ne zahtevajo njihove uporabe, hranijo ločeno od ostalih osebnih podatkov.

Člen 14 - Obdelava podatkov o zaposlenih

Upravljavec obdeluje tudi občutljive oziroma sodne podatke svojih zaposlenih za namene večjega javnega interesa za vzpostavljanje in upravljanje delovnih razmerij vseh vrst.
Takšna vrsta obravnave vključuje obravnavo za namene ugotavljanja izpolnjevanja določenih pogojev, predvidenih za dostop do specifičnih služb, izpolnjevanje pogojev za prekinitev ali prenehanje zaposlitve oziroma službe, za izpolnjevanje obveznosti, povezanih z opredelitvijo pravnega ali ekonomskega statusa zaposlenih ter v zvezi s povezanimi plačnimi, davčnimi in računovodskimi obveznostmi, ki se nanašajo na osebje v delovnem razmerju oziroma upokojeno osebje.
V skladu z veljavnimi predpisi upravljavec sprejme vse varnostne ukrepe pri obdelavi osebnih podatkov o svojih zaposlenih, ki razkrivajo njihovo zdravstveno stanje, njihove spolne navade, politično, sindikalno, versko in filozofsko prepričanje oziroma druga prepričanja in rasni ali etnični izvor.
Obdelava občutljivih podatkov o zaposlenem mora s strani delodajalca potekati ob upoštevanju načel potrebnosti in nujnosti, zaradi katerih mora biti obravnava zmanjšana na najmanjši obseg uporabe osebnih podatkov, če pa je uporaba sodnih in občutljivih podatkov nujna, lahko obdeluje samo tiste

podatke, za katere se izkaže, da so nujni za vodenje delovnega razmerja.
Objava seznama najbolje uvrščenih kandidatov za izbiro osebja oziroma za dodelitev, izplačilo, spremembo ali prenehanje veljavnosti bonitet, olajšav, dodeljevanja sredstev mora biti izvedena po natančnem preverjanju, da vsebovane navedbe ne vključujejo posredovanja podatkov, s katerimi se razkrije njihovo zdravstveno stanje z uporabo splošnih poimenovanj oziroma številčnih šifer.
Tako, razen v zakonsko predvidenih primerih, ni mogoče razkrivati obvestil, povezanih z boleznimi oziroma osebnimi ali družinskimi ovirami, zaradi katerih lahko pride do izostanka z dela, ter elementov za ocenjevanje in obvestil, povezanih z delovnim razmerjem med zaposlenim in organom uprave, s katerimi se razkrivajo določene občutljive informacije.
Upravljavec je pri obdelavi občutljivih podatkov, povezanih z zdravjem zaposlenih, dolžan upoštevati načela potrebnosti in nujnosti.
Upravljavec deluje usklajeno s smernicami varuha osebnih podatkov na področju obdelave osebnih podatkov zaposlenih za vodenje delovnega razmerja na javnem področju.

Člen 15 Pomen preglednic/tabel, ki določajo tipe občutljivih in sodnih podatkov, za katere je dovoljenja obdelava

Ob nespremenjeni veljavi dejstva, da predstavljajo pravno osnovo za obdelavo občutljivih in sodnih podatkov določila člena 9, odstavka 1 GDPR in zlasti seznam iz člena 2-sexies Zakonika, preglednice z navedbo tipov občutljivih in sodnih podatkov, ki se še nadalje izvajajo tako, da se predložijo temu pravilniku:

a) morajo biti osebno izročene zadolženim osebam po posameznih področjih pristojnosti, na katere se nanašajo,
b) v zvezi z njimi se izvaja izobraževanje,
c) takšne vrste podatkov se spremlja in preverja njihovo uporabo.

Člen 16 Evidenca obdelave in kategorije obdelave

Upravljavec uvede pisno evidenco dejavnosti obdelave in kategorije obdelave, ki se izvajajo v okviru njegove odgovornosti.
Evidenca mora biti nenehno posodabljana in biti na razpolago nadzornim organom.
Navedena evidenca vsebuje naslednje informacije:

- ime in kontaktne podatke upravljavca, obdelovalca, odgovornega za zaščito podatkov, odgovornih in zadolženih oseb,
- namene, za katere se osebni podatki obdelujejo,
- opis kategorij posameznikov in kategorij osebnih podatkov,
- kategorije izvedene obdelave,
- kategorije uporabnikov, katerim so bili ali bodo sporočeni osebni podatki,
- navedbo posebnih previdnostnih ukrepov, ki jih dolžan izvajati vsak obdelovalec na ustrezen način glede na obdelavo, za katero je odgovoren,
- morebitno možnost prenosa podatkov v tujino,
- splošni opis občih in specifičnih varnostnih ukrepov, kot so urejeni z novimi predpisi na področju varstva osebnih podatkov,
- navedbo skrajnih rokov, predvidenih za brisanje določenih kategorij obdelanih podatkov.

Obdelovalec vodi evidenco vseh kategorij dejavnosti, povezanih z obdelavo, opravljenih za račun upravljavca. Navedena evidenca vsebuje:

a) ime in kontaktne podatke obdelovalca oziroma obdelovalcev, vsakega upravljavca, za račun katerega opravlja delo obdelovalec, zastopnika upravljavca oziroma obdelovalca in če se nanaša, odgovornega za varstvo podatkov,

b) kategorije obdelave, izvedene za račun katerega koli drugega upravljavca,

c) če se nanaša, prenose osebnih podatkov v tretjo državo oziroma mednarodni organizaciji, vključno z opredelitvijo tretje države in mednarodne organizacije ter za prenose po drugem odstavku člena 49 dokumentacijo za ustrezna jamstva,

d) če je možno, splošni opis tehničnih in organizacijskih varnostnih ukrepov iz člena 32, odstavka 1 GDPR.

Evidence se vodijo v pisni obliki, tudi elektronsko.

Na zahtevo upravljavec oziroma obdelovalec data evidenco na razpolago varuhu osebnih podatkov.

RAZDELEK IV - PRAVICE POSAMEZNIKOV

Člen 17 Objava in posredovanje osebnih podatkov, vsebovanih v upravnih aktih in odločbah

Upravljavec pred objavo in posredovanjem osebnih podatkov, vsebovanih v upravnih aktih in odločbah, na elektronski oglasni deski oziroma preko mreže za dostop s strani občanov z izvajanjem potrebnih tehničnih in organizacijskih ukrepov, zagotavlja spoštovanje naslednjih načel:

a) varnosti
b) popolnosti
c) točnosti
d) dostopnosti
e) zakonitosti in skladnosti z načeli pripadnosti, nepreseganja, začasnosti in nujnosti glede na zasledovanje cilje.

Če dokumenti, podatki ali informacije, ki so predmet obvezne objave za namen preglednosti, vsebujejo osebne podatke, je te treba prikriti, razen izjem, predvidenih s posebnimi določili.

Če zakon ne določa drugače, upravljavec zagotavlja zaupnost občutljivih podatkov pri objavi na spletni oglasni deski oziroma v mreži za dostop s strani občanov na tak način, da ni mogoče identificirati oseb, na katere se navedeni podatki nanašajo in sprejme ustrezne ukrepe pri pripravi samih aktov ter njihovih prilog. V ta namen upravljavec sprejme in izvaja ustrezne organizacijske ukrepe za vodenje dokumentacije in izobraževanje.

V vsakem primeru morajo biti dokumenti, ki se objavijo in vsebujejo občutljive ali sodne informacije o posamezniku, anonimizirani z ustreznimi tehnikami anonimizacije.

Za občutljive in sodne podatke se ne izvajata indeksacija in sledljivost z zunanjimi spletnimi iskalniki in se ne uporabljajo ponovno.

Upravljavec skrbi za usklajenost s smernicami varuha osebnih podatkov s področja objave in posredovanja osebnih podatkov, vsebovanih v upravnih aktih in odločbah.

Člen 18 Pravica do dostopanja do dokumentacije, pravica do dostopa za občane in varstvo osebnih podatkov

Pogoji, načini in omejitve za uveljavljanje pravice do dostopanja do upravnih dokumentov in pravice do navadnega ali posplošenega dostopanja za občane do upravnih dokumentov, ki vsebujejo osebne podatke ter s tem povezano sodno varstvo, so še naprej urejeni na podlagi predpisov s področja dostopanja do listin in dostopanja za občane, tudi glede tipov občutljivih in sodnih podatkov ter postopkov obdelave, ki se izvajajo na podlagi zahteve za dostop.

Šteje se, da so dejavnosti, namenjene izvajanju obravnavane ureditve, v pomembnejšem interesu javnosti.

Upravljavec deluje usklajeno s smernicami varuha osebnih podatkov na področju odnosov, ki se nanašajo na dostopanje do dokumentacije, pravico do dostopa za občane in zaščito osebnih podatkov.

Člen 19 Pravice posameznika

Upravljavec izvaja in spoštuje organizacijske, upravne, postopkovne in dokumentarne ukrepe, potrebne za lažje uveljavljanje v nadaljevanju navedenih pravic posameznika skladno z ureditvijo GDPR in Zakonika.

20. člen - Pravica do dostopa

Ta pravilnik upošteva ureditev po GDPR s področja pravice do dostopanja, po katerih je posameznik upravičen od upravljavca pridobiti potrditev, ali poteka kakšna obdelava osebnih podatkov, ki se nanj nanaša in v takšnem primeru pridobiti dostop do osebnih podatkov oziroma do naslednjih informacij:

a) cilj obdelave,
b) kategorije obravnavanih osebnih podatkov,
c) uporabniki oziroma kategorije uporabnikov, katerim so bili ali bodo podatki sporočeni, zlasti če gre za uporabnike iz tretjih držav ali mednarodne organizacije,
d) če je možno, predviden čas hrambe osebnih podatkov oziroma če to ni možno, merila, uporabljena za določanje takšnega časa,
e) obstoj pravice posameznika, da od upravljavca zahteva popravek oziroma izbris osebnih podatkov oziroma omejitev obdelave osebnih podatkov, ki se nanj nanašajo oziroma da nasprotuje navedeni obdelavi,
f) pravica do vložitve ugovora nadzornem organu,
g) če podatki niso zbrani pri posamezniku, vse razpoložljive informacije v zvezi z njihovim izvorom,
h) obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov v skladu s členom 22, odstavkoma 1 in 4 GDPR ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

Če se podatki posredujejo v tretjo državo ali mednarodni organizaciji, je posameznik upravičen, da se ga obvesti o obstoju ustreznih zagotovil.

Upravljavec posreduje izvod osebnih podatkov, ki so predmet obdelave. V primeru, da posameznih zahteva nadaljnje izvode, mu upravljavec lahko zaračuna razumen prispevek k stroškom, ki temelji na administrativnih stroških.

Če posameznik posreduje zahtevo v elektronski obliki in če ne navede drugače, se informacije

posredujejo v elektronski obliki v splošni rabi.
Pravica do pridobitve izvoda ne sme kršiti pravic in svoboščin drugih oseb.

Člen 21 Pravica do popravka in izbrisa

Ta pravilnik upošteva ureditev iz GDPR na področju pravice do popravka in izbrisa (»pravica do pozabe«), kot je opisano v nadaljevanju.
Glede pravice do popravka je posameznik upravičen od upravljavca pridobiti popravek netočnih osebnih podatkov, ki se nanj nanašajo, brez neupravičenega odlašanja. Ob upoštevanju ciljev obdelave je posameznik upravičen doseči dopolnitev nepopolnih podatkov, tudi s predložitvijo dopolnitvene izjave.
Upravljavec sporoči morebitne popravke vsakemu uporabniku, kateremu so bili posredovani osebni podatki, razen če je to nemogoče ali če to terja nesorazmeren napor.
Glede pravice »do pozabe«, ki jo predstavlja pravica, da se pri upravljavcu doseže izbris osebnih podatkov, ki se na posameznika nanašajo, brez nepotrebnega odlašanja, se takšna pravica ne more uveljavljati, če je obdelava potrebna:

- za uveljavljanje pravice do svobode izražanja in obveščanja,
- za izpolnjevanje pravne obveznosti obdelave na podlagi prava Unije ali prava države članice, ki velja za upravljavca, ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je bila dodeljena upravljavcu,
- iz razlogov javnega interesa na področju javnega zdravja v skladu s točkama (h) in (i) člena 9(2) ter členom 9(3) GDPR,
- za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene v skladu s členom 89(1) GDPR, kolikor bi pravica iz odstavka 1 lahko onemogočila ali resno ovirala uresničevanje namenov te obdelave, ali
- za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Člen 22 Pravica do omejitve obdelave

Ta pravilnik upošteva ureditev iz GDPR na področju pravice do omejitve obdelave, kot je opisano v nadaljevanju.
Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec omeji obdelavo, kadar velja en od naslednjih primerov:

a) posameznik, na katerega se nanašajo osebni podatki, oporeka točnosti podatkov, in sicer za obdobje, ki upravljavcu omogoča preveriti točnost osebnih podatkov,
b) je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe,
c) upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov,
d) je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo v skladu s členom 21(1) GDPR, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Kadar je obdelava osebnih podatkov omejena v skladu z 18. členom, odstavkom 1 GDPR, se taki

osebni podatki z izjemo njihovega shranjevanja obdelujejo le s privolitvijo posameznika, na katerega se ti nanašajo, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali zaradi varstva pravic druge fizične ali pravne osebe ali zaradi pomembnega javnega interesa Unije ali države članice.
Upravljavec, ki je dosegel omejitev obdelave v skladu z odstavkom 1, pred preklicem omejitve obdelave o tem obvesti posameznika, na katerega se nanašajo osebni podatki.
Upravljavec vsakemu uporabniku, ki so mu bili osebni podatki razkriti, sporoči morebitne omejitve obdelave, razen če se to izkaže za nemogoče ali vključuje nesorazmeren napor. Upravljavec o teh uporabnikih obvesti posameznika, na katerega se nanašajo osebni podatki, če ta posameznik tako zahteva.

Člen 23 Pravica do prenosljivosti podatkov
Ta pravilnik upošteva okoliščino, da se na podlagi ureditve GDPR pravica do prenosljivosti podatkov ne uporablja za obdelavo, potrebno za opravljanje naloge, ki se izvajajo v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu.

Člen 24 Pravica do ugovora in avtomatizirano sprejemanje posameznih odločitev
Posameznik ima na podlagi razlogov, povezanih z njegovim posebnim položajem, pravico, da kadar koli ugovarja obdelavi osebnih podatkov v zvezi z njim, ki temelji na točki (e) ali (f) člena 6(1) GDPR, vključno z oblikovanjem profilov na podlagi teh določb.
Upravljavec preneha obdelovati osebne podatke, razen če dokaže nujne legitimne razloge za obdelavo, ki prevladajo nad interesi, pravicami in svoboščinami posameznika, na katerega se nanašajo osebni podatki, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov. Posameznika, na katerega se nanašajo osebni podatki, se na pravico iz odstavkov 1 in 2, člena 21 GDPR izrecno opozori najpozneje ob prvem komuniciranju z njim in se mu to pravico predstavi jasno in ločeno od vseh drugih informacij.
V okviru uporabe storitev informacijske družbe in ob nespremenjeni veljavi Direktive 2002/58/ES lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja pravico do ugovora z avtomatiziranimi sredstvi z uporabo tehničnih specifikacij. Kadar se osebni podatki obdelujejo v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene v skladu s členom 89(1) GDPR, ima posameznik, na katerega se ti podatki nanašajo, pravico, da iz razlogov, povezanih z njegovim posebnim položajem, ugovarja obdelavi osebnih podatkov v zvezi z njim, razen če je obdelava potrebna za opravljanje naloge, ki se izvaja zaradi razlogov javnega interesa.

Člen 25 Način uresničevanja pravic posameznika
Za uresničevanje pravic posameznika do dostopanja do osebnih podatkov in njihove obdelave se upoštevajo določila GDPR, Zakonika in tega pravilnika.
Zahtevo za uveljavljanje pravic lahko vloži:

- neposredno posameznik, tudi s pomočjo osebe, ki ji zaupa, s predložitvijo identifikacijskega osebnega dokumenta oziroma s predložitvijo kopije oziroma na druge ustrezne načine oziroma če so podane okoliščine, v katerih je mogoče izkazati osebno identiteto posameznika, kot na primer z osebnim znanstvom,
- druga fizična oseba ali združenje, ki ga je posameznik pisno zadolžil ali pooblastil. V takšnem

primeru je oseba, ki nastopa po pooblastilu posameznika, dolžna predložiti izvod pooblastila oziroma zadolžitve in neoverjeno fotokopijo osebnega dokumenta podpisnika,

- kdor izvaja starševsko ali skrbniško pravico za mladoletne in opravilno nesposobne,
- za pokojne, kdor ima pri tem lastni interes oziroma deluje v zaščito posameznika oziroma iz družinskih razlogov, zaradi katerih je zaščita upravičena,
- fizična oseba, ki je za navedeno pooblaščena po ustreznih statutih ali pravilnikih, če je posameznik pravna oseba, organizacija ali združenje.

Posameznik lahko predloži ali pošlje zahtevo za uveljavljanje pravic:

- upravljavcu ali obdelovalcu, ki hrani osebne podatke posameznika in z njimi upravlja,
- splošnemu vložišču nosilca oziroma službi za odnose z javnostjo.

Zahtevo za uveljavljanje pravice do dostopanja do osebnih podatkov lahko posameznik uveljavlja le glede:

- informacij, ki se nanj nanašajo in ne glede osebnih podatkov, ki se nanašajo na tretje osebe, katere so lahko navedene v dokumentih, ki se nanašajo na posameznika.

Ob nespremenjeni pravici do dostopanja do osebnih podatkov, vodstveni delavec/OP odobri razkritje listin posamezniku, če so izpolnjeni pogoji za dostopanje.

Pristojni osebi za oceno vloge sta:

- pristojni vodstveni delavec/OP,

ki odločata o upravičenosti zahteve za dostop in načinu dostopanja do podatkov.

Odgovor na vlogo mora biti podan v 30 dneh od datuma njenega prejema.

Rok se lahko podaljša za nadaljnjih 30 dni od datuma prejema, po predhodnem takojšnjem obvestilu posameznika, če je vloga, ki jo je posredoval prosilec, posebej kompleksna oziroma če je podan upravičen razlog.

Dostop posameznika do njegovih osebnih podatkov:

- se lahko odloži samo za nujno potreben čas, v katerem se navedeni podatki obravnavajo izključno za izvajanje poizvedb za namene zagovora oziroma za zaščito potreb po zaupnosti upravljavca. V vsakem primeru je dovoljen dostop do ostalih osebnih podatkov posameznika, ki ne vplivajo na razloge, povezane z varstvom na podlagi odložitve.

Upravljavec skrbi za usklajenost s smernicami varuha osebnih podatkov s področja uveljavljanja pravic posameznika.

Člen 26 Poizvedbe za namene priprave zagovora

Za namene poizvedb, ki se opravijo tekom kazenskega postopka, je zagovornik v skladu z Zakonom št. 397 z dne 7. decembra 2000 in člena 391-quater Zakonika o kazenskem postopku upravičen zahtevati dokumente, s katerimi razpolaga upravljavec in lahko pridobi njihovo kopijo, tudi če vsebujejo osebne podatke tretjega posameznika.

Pred izdajo se preveri, da je zagovarjana pravica podana vsaj v enakem obsegu kot pravica posameznika in sicer, da gre za osebnostno pravico oziroma drugo temeljno in nekršljivo pravico ali temeljno svoboščino, medtem ko se za vse ostale dodatne vidike upošteva ureditev po pravilniku upravljavca o pravici do dostopanja.

Upravljavec skrbi za usklajenost s smernicami varuha osebnih podatkov s področja poizvedb za pripravo zagovora.

Avv. Nadia Corà
Avv. Guido Paratico

RAZDELEK V - OSEBE

Člen 27 Upravljavec in soupravljavci

Upravljavec je Občina XXX, ki jo zastopa župan kot zakoniti zastopnik upravljavca, s sedežem v ulici xxx, št. xxx, xxx.

Upravljavec:

- opredeli strateške cilje za varstvo osebnih podatkov pri obdelavi ter zagotovi, da se takšni strateški cilji vnesejo v enotni programski načrt (DUP) in v ostale programske dokumente ter načrte upravljavca,
- izvaja tehnične in organizacijske ukrepe, s katerimi se zagotovi skladnost obdelave z Zakonikom, GDPR in tem pravilnikom,
- pooblasti oziroma z aktom imenuje vodstvene delavce/OP po posameznih delovnih nalogah in funkcijah ter pooblastilih glede na procese, postopke in izpolnjevanje, povezano z obdelavo osebnih podatkov, varnostjo ter izobraževanjem in jim posreduje potrebna navodila glede obveščanja posameznikov v povezavi z vrsto podatkov, ki se obdelujejo, pogoji, predvidenimi za obdelavo podatkov po predpisih, glede načinov zbiranja, sporočanja in posredovanja podatkov, izvajanja pravic posameznikov, sprejemanja varnostnih ukrepov za hrambo, zaščito in varstvo podatkov, glede morebitne uporabe naprav za video nadzor,
- sestavi in posodablja seznam pooblaščenih ali imenovanih vodstvenih delavcev/OP in ga objavlja na uradni spletni strani upravljavca,
- z aktom imenuje odgovorno osebo za varstvo osebnih podatkov,
- zagotavlja redno preverjanje upoštevanja danih navodil, tudi glede varnosti podatkov in izobraževanja zaposlenih,
- spodbuja sprejemanje kodeksov ravnanja, ki jih izdelajo reprezentančna panožna združenja in organi,
- spodbuja uvedbo mehanizmov za certificiranje,
- izpolnjuje obveznosti v razmerju do varuha osebnih podatkov v primerih, predvidenih po veljavni zakonodaji.

Upravljavec je soupravljavec skupaj z drugimi upravljavci, če navedeni skupaj določajo cilje in sredstva obdelave.

Soupravljavci so dolžni z internim dogovorom na pregleden način določiti posamezne odgovornosti pri spoštovanju obveznosti na podlagi GDPR in tega pravilnika, zlasti pri uveljavljanju pravic posameznika in funkcij posredovanja informacij v skladu s členoma 13 in 14 GDPR, razen če takšne odgovornosti niso določene po pravu Evropske unije oziroma države članice, ki velja za upravljavce in v tolikšni meri, kot jih takšna zakonodaja določa. V takšnem dogovoru je lahko navedena kontaktna točka za posameznike. Interni dogovor mora ustrezno odražati posamezne vloge in razmerja soupravljavcev s posamezniki. Osnovna vsebina dogovora mora biti na voljo posamezniku.

Ne glede na določila internega dogovora, lahko posameznik uveljavlja svoje pravice v skladu s tem pravilnikom v razmerju do vsakega upravljavca in zoper njega.

Člen 28 Vodstveni delavci in nosilec organizacijskega položaja - OP

Upravljavec dodeli v nadaljevanju navedene naloge in funkcije z ustreznimi pooblastili s posebno

odločbo o dodelitvi pooblastil oziroma o imenovanju, ki jo sprejme skladno z lastno ureditvijo, za:

- vodstvene delavce/OP.

V navedeni odločbi je upravljavec dolžan vsakega vodstvenega delavca/OP seznaniti z odgovornostmi, ki so mu dodeljene na podlagi določil Zakonika, GDPR in tega pravilnika.

Naloge, funkcije in pooblastila:

- obdelovati osebne podatke samo po navodilu upravljavca,
- zagotavljati, da so se osebe, pooblaščene za obdelavo osebnih podatkov, zavezale k ohranjanju zaupnosti oziroma da so prilagodile pravno obvezo glede zaupnosti,
- takoj in povezano izpolnjevati obveznosti upravljavca, predvidene po Zakoniku, vključno s profilom, ki se nanaša na varnost obdelave, skladno s členom 32 GDPR,
- upoštevati določila tega pravilnika ter izrecna navodila, prejeta od upravljavca,
- sprejeti ustrezne ukrepe za zagotavljanje spoštovanja pravic in temeljnih svoboščin ter dostojanstva posameznikov pri organizaciji storitev in služb ter poklicne tajnosti, ob nespremenjeni veljavi predpisov, določil varuha osebnih podatkov, tistih, vsebovanih v tem pravilniku, zlasti glede vseh posebnih določil, ki kakor koli vplivajo na obdelavo podatkov,
- sodelovati z upravljavcem pri pripravi dokumenta za oceno učinka v zvezi z varstvom podatkov in pri pripravi evidence dejavnosti obdelave ob sodelovanju z upravljavcem sistema in z drugimi pristojnimi službami upravljavca ter za morebitno posodabljanje in prilagajanje navedenega dokumenta,
- skrbeti za obdelavo in zbiranje obrazcev ter obvestil, ki se uporabljajo znotraj organizacije upravljavca za izvajanje Zakonika, GDPR in tega pravilnika,
- kolikor je možno upravljavcu pomagati z ustreznimi tehničnimi in organizacijskimi ukrepi z namenom izpolnjevanja obveznosti nosilca, ki je dolžan odgovoriti na zahteve za uveljavljanje pravic posameznika skladno z veljavnimi predpisi,
- upravljavcu pomagati zagotavljati spoštovanje obveznosti iz členov od 32 do 36 GDPR (varnost obdelave osebnih podatkov, prijava kršitve osebnih podatkov nadzornemu organu, obvestilo o kršenju v zvezi z osebnimi podatki posameznika, ocena učinka v zvezi z varstvom podatkov, predhodno posvetovanje) ob upoštevanju narave obdelave in razpoložljivih informacij,
- upravljavcu zagotoviti vse potrebne informacije za dokazovanje spoštovanja obveznosti po Zakoniku, GDPR in tem pravilniku,
- prispevati k preverjanju spoštovanja Zakonika, GDPR in tega pravilnika, vključno z inšpekcijskimi pregledi, ki jih izvaja upravljavec ali druga oseba po pooblastilu upravljavca,
- poskrbeti za uvedbo in posodabljanje ustreznih arhivov/baz podatkov, kolikor je to v njegovi pristojnosti:
  - seznam soupravljavcev, obdelovalcev, pooblaščencev z ustreznimi kontaktnimi podatki,
  - seznam zbirk/baz podatkov,
- zagotavljati vsaj enkrat letno posodabljanje prepoznavanja obdelave,
- zagotoviti vse ustrezne informacije in nuditi pomoč pooblaščeni osebi za varstvo podatkov (DPO) pri izvajanju njenih funkcij.

Vsak vodstveni delavec/OP pri izvajanju dodeljenih nalog, funkcij in pooblastil oziroma tistih nalog in funkcij, za katere je bil imenovan, z upravljavcem sodeluje z namenom, da:

- ob začetku vsake nove obdelave nemudoma poda obvestilo o prenehanju ali spremembi obdelave v teku ter sporoča vse podatke, pomembne za spoštovanje obveznosti na podlagi členov od 32 do 36 GDPR, povezanih s sprejemanjem tehničnih in organizacijskih ukrepov, namenjenih zagotavljanju nivoja varnosti sorazmerno s tveganjem; prijavlja kršitve osebnih podatkov varuhu osebnih podatkov; sporoča kršitve s področja osebnih podatkov posamezniku; sestavlja oceno učinka v zvezi z varstvom podatkov; zagotavlja predhodno posvetovanje,
- pripravlja predvidena obvestila in preverja njihovo spoštovanje ter posreduje potrebne informacije za posodabljanje evidence o obravnavi,
- imenuje osebe, zadolžene za obdelavo in jim posreduje specifična navodila,
- odgovarja na vloge posameznikov v skladu z določili Zakonika ter določa organizacijske načine za lažje uveljavljanje pravice do dostopa za posameznike in oceno tehtanja prisotnih interesov,
- zagotavlja, da se vsi varnostni ukrepi, povezani s podatki upravljavca, izvajajo znotraj organizacijske strukture slednjega in navzven, če do njih dostopajo tretje osebe kot obdelovalci podatkov,
- upravljavca brez nepotrebnega odlašanja obvešča, če se seznani s kršitvijo osebnih podatkov.

Vsak vodstveni delavec/OP je upravljavcu odgovoren za vsako kršitev ali neizvajanje določil v skladu z veljavnimi predpisi in za neizvajanje varnostnih ukrepov.
Vodstveni delavci/OP se udeležujejo izobraževanj, na katerih se seznanjajo z novostmi.

Člen 29 Obdelovalci in podobdelovalci

Obdelovalec je oseba, ki opravlja naloge za račun upravljavca.
Upravljavec lahko imenuje obdelovalca. Če je to potrebno iz organizacijskih razlogov, se lahko imenuje več obdelovalcev, pri čemer se lahko naloge mednje tudi porazdelijo. Podrobneje se lahko upravljavec za obdelavo podatkov, tudi občutljivih, posluži tudi oseb javnega ali zasebnega prava, ki kot obdelovalci podatkov jamčijo za celovito spoštovanje veljavnih določil s področja obdelave, vključno z varnostnimi vidiki. Če je obdelovalec imenovan, se ga izbere med osebami, ki po svojih izkušnjah, sposobnostih in zanesljivosti predstavljajo ustrezno jamstvo za celovito spoštovanje veljavnih določil s področja obdelave, vključno z vprašanji, povezanimi z varnostjo.
Obdelovalec se ne posluži drugega obdelovalca brez predhodnega izrecnega ali splošnega pisnega pooblastila upravljavca.
Upravljavec lahko glede na kompleksnost in obseg institucionalnih nalog za obdelovalca osebnih podatkov imenuje samo osebe, ki predstavljajo zadostno jamstvo za izvajanje ustreznih tehničnih in organizacijskih ukrepov na tak način, da so pri obdelavi izpolnjeni pogoji, predvideni po tem pravilniku in zagotavlja varstvo pravic posameznika (člen 28 GDPR).
Obdelovalci so dolžni:

- obdelovati podatke na zakonit način, korektno in ob celovitem spoštovanju veljavnih predpisov na obravnavanem področju,
- spoštovati varnostne ukrepe, kot jih določa Zakonik o varstvu osebnih podatkov in sprejemati vse ustrezne ukrepe, da se prepreči in/oziroma izogne posredovanju ali razkrivanju podatkov, tveganju za njihovo uničenje ali izgubo, tudi naključno, za nepooblaščen dostop oziroma nepooblaščeno obdelavo oziroma obdelavo, ki ne bi bila

skladna z nameni zbiranja,

- izmed samih obdelovalcev imenovati osebe, zadolžene za obdelavo,
- zagotavljati, da se z obdelovanimi podatki seznanijo samo osebe, zadolžene za obdelavo,
- obdelovati osebne podatke, tudi občutljive in zdravstvene osebne podatke, izključno za namene, predvidene po pogodbi oziroma dogovoru,
- upoštevati navodila, ki jih prejmejo od upravljavca,
- navajati kraje, kjer se odvija obdelava podatkov in na kakšnih nosilcih poteka,
- obveščati o minimalnih varnostnih ukrepih, sprejetih za zagotavljanje zaupnosti in varstva obdelovanih osebnih podatkov.

Če navedena določila niso upoštevana in v primeru, da upravljavec ni obveščen o imenovanju oseb, zadolženih za obdelavo podatkov, obdelovalec za to neposredno odgovarja upravljavcu.
Upravljavec imenuje obdelovalca z listino, ki se ji priložijo dogovori, sporazumi oziroma pogodbe, s katerimi se določi dodelitev obdelave osebnih podatkov izven upravljavca.
Sprejem imenovanja in prevzem obveznosti spoštovanja določil Zakonika, GDPR in tega pravilnika predstavlja nujen pogoj za vzpostavitev pravnega razmerja med strankami.

Člen 30 Osebe, zadolžene za obdelavo, zaposlene pri upravljavcu

Osebe, zadolžene za obdelavo, so fizične osebe, zaposlene pri upravljavcu, ki jih imenuje vsak vodstveni delavec/OP in so pooblaščene za izvajanje postopkov obdelave osebnih podatkov v svoji pristojnosti z izrecno navedbo nalog, obsega dovoljene obravnave ter načinov.
Za imenovanje osebe, zadolžene za obdelavo osebnih podatkov, je pristojen vodstveni delavec/OP. Imenovanje se izda v pisni obliki in v njem so izrecno navedeni naloge zadolžene osebe in načini, ki jih mora navedeni upoštevati pri izvajanju takšnih nalog ter obseg dovoljene obravnave.
Ne glede na imenovanje, se kot takšen šteje tudi predlog dodelitve z dokazili fizične osebe enoti, za katero je bila ta oseba določena, pri čemer se v pisni obliki določi obseg dovoljene obdelave za zaposlene pri tej enoti. Na podlagi takšnega določila se vsak zaposleni, ki je dodeljen določenemu uradu/službi in je dolžan izvajati postopke obdelave v okviru takšne službe, šteje kot »zadolžena oseba« v skladu s členom 2-quaterdecies Zakonika in v skladu s členom 4, odstavkom 10 in členom 29 GDPR.
Zadolžene osebe morajo v vsakem primeru prejeti ustrezna razdelana navodila, tudi za homogene skupine funkcij, glede dejavnosti, povezanih s podatki, ki so jim dodeljene, ter obveznosti, ki so jih dolžne izpolnjevati.
Zadolžene osebe sodelujejo z upravljavcem in vodstvenim delavcem/OP ter prijavijo morebitna tveganja pri obdelavi podatkov in posredujejo vse potrebne informacije za opravljanje nadzornih funkcij.
Podrobneje so zadolžene osebe dolžne zagotoviti, da so med obravnavo podatki:

- obdelani zakonito, pošteno in na pregleden način v razmerju do posameznika, na katerega se nanašajo osebni podatki,
- zbrani za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni,
- ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo,
- točni in, kadar je to potrebno, posodobljeni; sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju

namenov, za katere se obdelujejo,

- hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo,
- obdelujejo se na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi.

Zadolžene osebe so dolžne varovati zaupnost podatkov, s katerimi se seznanijo pri izvajanju svoje dejavnosti in se obvežejo, da bodo podatke posredovale izključno osebam, ki jih navedeta upravljavec oziroma vodstveni delavec/OP samo v zakonsko predvidenih primerih pri opravljanju institucionalne dejavnosti upravljavca.
Zadolžene osebe, zaposlene pri upravljavcu, se udeležujejo izobraževanj, na katerih se seznanjajo z novostmi.

Člen 31 Osebe, zadolžene za obdelavo, ki niso zaposlene pri upravljavcu

Vse osebe, ki izvajajo dejavnost obdelave podatkov in niso zaposlene pri upravljavcu, kot na primer pripravniki, prostovoljci in osebe, ki začasno delajo v organizacijski strukturi upravljavca oziroma zadolžene osebe, ki jih imenuje zunanji obdelovalec, morajo biti zadolžene za obdelavo s pisno listino o imenovanju.
Slednji so dolžni izpolnjevati enake obveznosti, kot veljajo za zadolžene osebe, ki so zaposlene pri upravljavcu, s čimer se zagotavlja polno spoštovanje na področju zaupnosti podatkov.
Zadolžene osebe, ki niso zaposlene pri upravljavcu, se udeležujejo izobraževanj, na katerih se seznanjajo z novostmi.

Člen 32 Upravitelj sistema

Upravitelj sistema, ki ga določi odgovorni pri Centru za obdelavo podatkov, nadzoruje vodenje in vzdrževanje baz podatkov in celotnega računalniškega sistema, ki je v uporabi pri upravnem organu.
Upravitelj sistema je imenovan po predhodni oceni izkušenj, sposobnosti in zanesljivosti predlaganega kandidata, ki mora zagotoviti ustrezna jamstva za celovito spoštovanje veljavnih določil s področja obdelave in zaupnosti osebnih podatkov. Imenovanje upravitelja sistema je individualno in v njem mora biti razčlenjeno naveden obseg dovoljenih nalog na podlagi dodeljenega profila pooblastil.
Upravitelj sistema opravlja dejavnosti, kot so:

- shranjevanje podatkov, organizacija mrežnih tokov, vodenje nosilcev za shranjevanje podatkov in vzdrževanje računalniške opreme. Upravljavcu predlaga obravnavo dokumenta za ocenjevanje računalniškega tveganja.

Ob upoštevanju predpisov s področja varstva podatkov in varnosti je upravitelj sistema:

- dolžan sprejemati ustrezne sisteme za evidentiranje logičnih dostopov do sistemov za obdelavo in elektronskih zbirk.

  Prijave (access log) morajo biti popolne, nespremenljive in v celoti preverljive ter ustrezne za doseganje cilja preverjanja, zaradi katerega so zahtevane.

Prijave morajo vsebovati časovni sklic in opis dogodka, zaradi katerega so nastale ter se hranijo ustrezno dolgo, najmanj šest mesecev.
V skladu z veljavnimi predpisi je upravljavec dolžan delo upravitelja sistema preverjati letno, s čimer

zagotavlja ustreznost uvedenih tehnično-organizacijskih in varnostnih ukrepov za dejavnost obdelave osebnih podatkov.
Upravitelj sistema izvaja navodila, ki jih prejme od varuha osebnih podatkov na področju predpisanih ukrepov in dejanj za obdelavo, ki poteka z elektronskimi sredstvi, v povezavi z dodelitvijo funkcij upravitelju sistema.
Upravitelj sistema se udeležuje izobraževanj, na katerih se seznanja z novostmi.

Člen 33 Pooblaščena oseba za varstvo podatkov (DPO) - Data Protection Officer

Upravljavec imenuje pooblaščeno osebo za varstvo osebnih podatkov (DPO).
DPO mora:

- ustrezno poznati predpise in prakse upravljanja z osebnimi podatki,
- izpolnjevati svoje funkcije povsem neodvisno in brez navzkrižja interesov,
- biti zaposlen pri upravljavcu oziroma delati po pogodbi o izvajanju storitev.

DPO je v zvezi z izvajanjem svojih nalog zavezan k varovanju tajnosti in zaupnosti podatkov.
Upravljavec da pooblaščeni osebi za varstvo podatkov (DPO) na voljo potrebna sredstva za izvajanje njegovih nalog in dostopanje do osebnih podatkov ter obdelave.
DPO opravlja naslednje naloge:

- obvešča upravljavca in zaposlene, ki izvajajo obdelavo podatkov, v zvezi z veljavnimi obveznostmi s področja varstva podatkov, ter jim svetuje,
- preverja izvajanje in spoštovanje veljavnih predpisov na obravnavanem področju ter politik upravljavca in obdelovalca na področju varstva osebnih podatkov, vključno z dodeljevanjem odgovornosti, seznanjanjem in obveščanjem zaposlenih, ki sodelujejo pri obravnavi in z njo povezanimi revizijami,
- vsakič, ko se to od njega zahteva, poda mnenje o oceni učinka v zvezi z varstvom podatkov in nadzoruje izvajanje obveznosti v zvezi z navedenim,
- nastopa kot kontaktna točka za posameznike glede obdelave njihovih osebnih podatkov in uveljavljanja pravic,
- nastopa kot kontaktna točka z varuhom osebnih podatkov pri vprašanjih, povezanih z obdelavo podatkov, med drugim tudi pri predhodnem posvetovanju.

RAZDELEK VI - VARNOST OSEBNIH PODATKOV

Člen 34 Varnostni ukrepi

Upravljavec pri obdelavi osebnih podatkov zagotavlja izvajanje ustreznih varnostnih ukrepov, ki omogočajo, da se čim bolj zmanjšajo tveganja za uničenje ali izgubo podatkov, tudi naključno, za nedovoljen dostop oziroma nedovoljeno obdelavo oziroma obdelavo, ki ni skladna z namenom zbiranja.
Podrobneje upravljavec izvaja primerne tehnične, organizacijske, upravne, postopkovne in dokumentarne ukrepe za zagotavljanje ustrezne ravni varnosti glede na tveganje. Navedeni ukrepi vključujejo najmanj:

- psevdonimizacijo in šifriranje osebnih podatkov,

- možnost zagotavljanja stalne zaupnosti, celovitosti, dostopnosti in odpornosti sistemov ter storitev za obdelavo,
- načine za pravočasno ponovno vzpostavitev razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta;
- postopek rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnostni obdelave.

Člen 35 Ocena učinka v zvezi z varstvom podatkov - OUZVP

Ocena učinka v zvezi z varstvom podatkov (v nadaljevanju »OUZVP«) je postopek, namenjen opisu obdelave, oceni potrebe in sorazmernosti ter v podporo upravljanju s tveganji za pravice in svoboščine fizičnih oseb, ki izhajajo iz obdelave osebnih podatkov, ob hkratnem ocenjevanju navedenega tveganja in določanju ukrepov za soočanje s takšnimi tveganji.
OUZVP je pomemben instrument za prevzemanje odgovornosti, saj upravljavcem nudi podporo ne le pri upoštevanju zahtev GDPR, temveč tudi pri dokazovanju, da so bili sprejeti ustrezni ukrepi, da se zagotovi spoštovanje uredbe GDPR.
OUZVP je upravljavec dolžan izvajati preden se začne obdelava, če je pri določeni obdelavi glede na naravo, kontekst in namene takšne obdelave lahko prisotna visoka raven tveganja za pravice in svoboščine fizičnih oseb, pri čemer je kot »tveganje« mišljeno stanje, pri katerem so opisani dogodek in njegove posledice, ocenjen glede na resnost in verjetnost takšnega dogodka, kot »upravljanje s tveganji« pa skupek dejavnosti, namenjenih usmerjanju in nadzoru nad tveganji v določeni organizaciji.
Pred OUZVP mora biti:
- izvedeno oziroma posodobljeno prepoznavanje obdelave,
- sprejeta odločitev glede možnosti, da pri obdelavi nastane večje tveganje za pravice in svoboščine posameznikov.

Odločitev glede možnosti, da bi pri obdelavi lahko nastalo večje tveganje za varstvo podatkov fizičnih oseb in torej za obveznost OUZVP, ob nespremenjeni veljavi določil glede seznama obdelav, za katere je OUZVP obvezujoča v skladu s Prilogo 1 k Odločbi varuha osebnih podatkov št. 467 z dne 11. oktobra 2018, se sprejme ob upoštevanju primerov, navedenih v členu 35, odstavku 3 GDPR in pojasnil k merilom, vsebovanih v »Smernicah s področja ocene učinka v zvezi z varstvom podatkov in določanja možnosti, da je pri obdelavi »lahko prisotno večje tveganje« za namene po Uredbi (EU) 2016/679«, ki jih je sprejel varuh osebnih podatkov dne 4. aprila 2017, kot so bile nazadnje spremenjene in sprejete 4. oktobra 2017 (v nadaljevanju imenovane »Smernice«).
Pri izvajanju zgoraj navedenih meril mora biti upoštevano naslednje:

- OUZVP je vedno obvezna, ne glede na to ali izpolnjeno eno ali več od zgoraj navedenih meril in sicer za vse obravnave, vključene v seznam vrst dejanj obdelave, ki ga pripravi in objavi nadzorni organ v skladu s členom 35, točko 4 GDPR in predstavlja Prilogo 1 k Odločbi varuha osebnih podatkov št. 467 z dne 11. oktobra 2018,
- OUZVP je vedno obvezna za obdelavo, vključeno v seznam obdelave občutljivih in sodnih podatkov v skladu s Pravilnikom o obdelavi občutljivih in sodnih podatkov, ki ga organizacija sprejme skladno s tipsko preglednico varuha osebnih podatkov,
- ob nespremenjeni veljavi določila iz smernic, da je za obdelavo, pri kateri sta izpolnjeni vsaj 2 merili, treba izdelati oceno učinka v zvezi z varstvom podatkov, za zagotavljanje boljšega

jamstva za varstvo, predstavlja podanost tudi samo 1 merila zadosten element za nastanek obveznosti izvedbe OUZVP,

- večje kot je število izpolnjenih meril pri obravnavi, bolj verjetno je, da je prisotno veliko tveganje za pravice in svoboščine posameznikov in da je posledično treba izvesti oceno učinka v zvezi z varstvom podatkov,
- če kljub izvajanju zgoraj navedenih meril potreba po izvedbi OUZVP ni jasno podana, gre kljub temu šteti, da obstaja obveznost v skladu s priporočili WP29 - da se OUZVP izvede, saj prispeva k spoštovanju predpisov s področja varstva podatkov s strani upravljavcev.

OUZVP ni zahtevana v naslednjih primerih:

- če na podlagi zgoraj navedenih meril izhaja, da obdelava ne »predstavlja velikega tveganja za pravice in svoboščine fizičnih oseb«,
- če so narava, področje izvajanja, kontekst in nameni obdelave zelo podobni obdelavi, pri kateri je bila izdelana ocena učinka v zvezi z varstvom podatkov. V takšnih primerih se lahko uporabijo rezultati ocene učinka v zvezi z varstvom podatkov,
- če tipe obdelave nadzorni organ preverja pred majem 2018 v posebnih pogojih, ki se niso spremenili,
- kadar je pravna podlaga za obdelavo v skladu s točko (c) ali (e) člena 6(1) GDPR pravo Unije ali pravo države članice, ki velja za upravljavca, ureja zadevno posebno dejanje obdelave ali niz zadevnih dejanj obdelave, in je bila ocena učinka v zvezi z varstvom podatkov že izvedena v okviru splošne ocene učinkov med sprejemanjem te pravne podlage (člen 35, točka 10 GDPR).

OUZVP zajema vsaj:

- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva upravljavec;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti s to uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.

Upravljavec po potrebi opravi pregled, da bi ocenil, ali obdelava poteka v skladu z oceno učinka v zvezi z varstvom podatkov vsaj takrat, ko se spremeni tveganje, ki ga predstavljajo dejanja obdelave.

Za doseganje ciljev zmanjševanja tveganja OUZVP ob upoštevanju ustreznih standardov UNI ISO (31000 in 27001) in usmeritev, vsebovanih v Smernicah ter zlasti v Prilogi 2, poteka po fazah, navedenih v nadaljevanju, predvidenih po členu 35, odstavku 7 GDPR:

- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva upravljavec;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz člena 35, odstavka 1 GDRP,
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti s to

uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.

Upravljavec se pri ocenjevanju posvetuje s pooblaščeno osebo za varstvo podatkov.

Če se pri OUZVP ugotovi prisotnost preostalega velikega tveganja, je upravljavec dolžan zahtevati predhodno posvetovanje z nadzornim organom glede obdelave v skladu s členom 36, odstavkom 1 GDPR.

Člen 36 Objava povzetka ocene učinka - OUZVP

Upravljavec objavi OUZVP oziroma njen povzetek z namenom povečati zaupanje v obdelavo, ki jo izvaja upravljavec ter kot dokaz prevzemanja odgovornosti in preglednosti.

Objavljena OUZVP ne sme vsebovati celotne ocene, če bi utegnila vključevati specifične informacije, povezane s tveganji za varnost upravljavca oziroma če bi razkrivala poslovne tajnosti ali občutljive poslovne podatke. V takšnem primeru lahko objavljena različica vključuje samo povzetek glavnih izsledkov OUZVP oziroma samo izjavo, s katero se ugotovi, da je bila OUZVP izvedena.

Člen 37 Predhodno posvetovanje

Upravljavec se pred obdelavo podatkov preko DPO posvetuje z varuhom osebnih podatkov, če je bilo pri ocenjevanju učinka na varstvo podatkov ugotovljeno, da bi obdelava brez sprejetih ukrepov lahko povzročila večje tveganje.

Člen 38 Obrazci in postopki

Upravljavec z namenom olajševanja in poenostavitve pravilnega ter doslednega izvajanja določil Zakonika, GDPR in tega pravilnika ter vseh smernic in odločb varuha osebnih podatkov:

a) sprejema in stalno posodablja:

- enotne obrazce za obveščanje,
- enotne obrazce in besedila, potrebna za vodenje obdelave podatkov in varnostne ukrepe,

b) obdeluje, sprejema in stalno posodablja:

- ustrezne vodstvene procese, ki so zbrani v ustreznem Priročniku postopkov.

Člen 39 Odgovornost v primeru kršitve določil s področja varstva osebnih podatkov

V primeru nespoštovanja določil s področja zaupnosti osebnih podatkov varuh osebnih podatkov izreka sankcije, predvidene po členu 166 Zakonika in členu 83 Uredbe in disciplinske sankcije.

Upravljavec je odgovoren za škodo, ki se povzroči z njegovo obdelavo, s katero je kršen ta pravilnik.

Obdelovalec je odgovoren za škodo, ki nastane pri obdelavi, samo če ni izpolnil obveznosti, predvidenih po Zakoniku, GDPR in tem pravilniku, ki se izrecno nanašajo nanj oziroma če ni ravnal v skladu ali je ravnal v nasprotju s pravnimi navodili, kot jih je prejel od upravljavca.

Upravljavec in obdelovalec sta prosta odgovornosti, če dokažeta, da za škodni dogodek v nobenem primeru nista odgovorna.

Člen 40 Uradno obvestilo o kršitvi varstva osebnih podatkov

V primeru kršitve varstva osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti varuha osebnih podatkov, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedba razlogov za zamudo.

Obdelovalec po seznanitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja uradno obvesti upravljavca.

Uradno obvestilo vsebuje vsaj:

a) opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;

b) sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;

c) opis verjetnih posledic kršitve varstva osebnih podatkov;

d) opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

Kadar in kolikor informacij ni mogoče zagotoviti istočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja.

Člen 41 Sporočilo o kršitvi varstva osebnih podatkov

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

V sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz odstavka 1 tega člena je v jasnem in preprostem jeziku opisana vrsta kršitve varstva osebnih podatkov ter so vsebovane vsaj informacije in ukrepe iz točk (b), (c) in (d) člena 33(3) GDPR.

Sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz odstavka 1 ni potrebno, če je izpolnjen kateri koli izmed naslednjih pogojev:

a) upravljavec je izvedel ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot je šifriranje;

b) upravljavec je sprejel naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz odstavka 1 verjetno ne bo več udejanjilo;

c) to bi zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

Če upravljavec posameznika, na katerega se nanašajo osebni podatki, še ni obvestil o kršitvi varstva osebnih podatkov, lahko nadzorni organ to od njega zahteva po preučitvi verjetnosti, da bi kršitev varstva osebnih podatkov povzročila veliko tveganje, ali pa lahko odloči, da je izpolnjen kateri koli od pogojev iz odstavka 3.

Člen 42 Končne določbe

Za vse, kar ni predvideno s tem pravilnikom, se uporabljajo določila Zakonika, GDPR, Smernic in odločb varuha osebnih podatkov.

Ta pravilnik je posodobljen na podlagi dodatnih sprememb, veljavnih predpisov s področja zaupnosti in varstva osebnih podatkov.