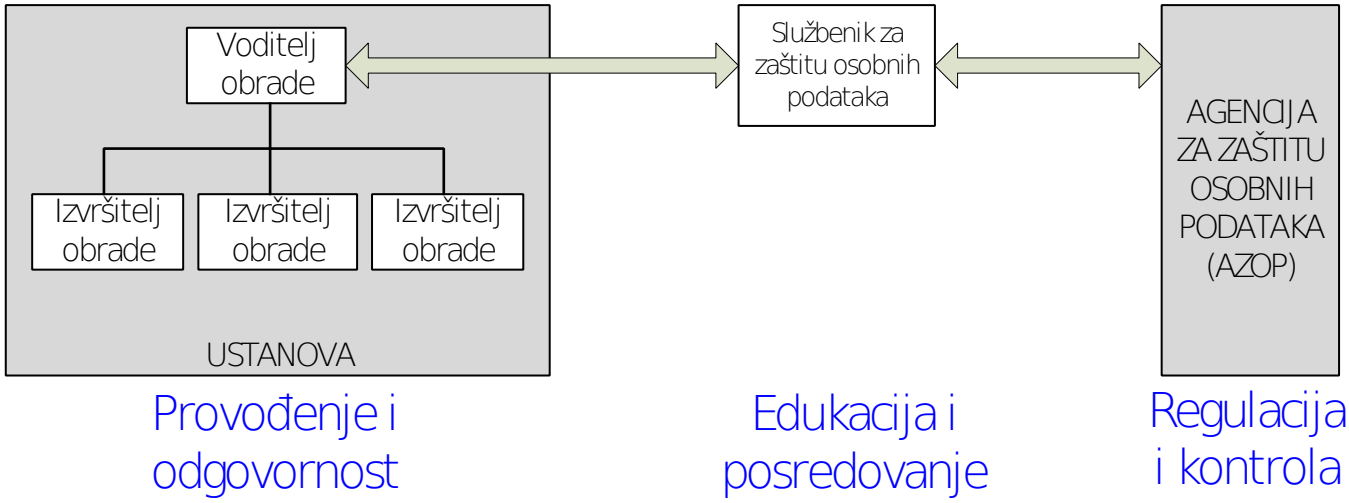
GDPR – ŠTO I KAKO?

Otkud se stvorio taj GDPR?

GRPR je akronim od Anglo-Saksonskog izraza: General Data Protection Regulation, kod nas prevedena kao: *Uredba (EU) 2016/679 Europskog parlamenta i vijeća o zaštiti pojedinca u vezi s obradom osobnih podataka.*
U daljem tekstu ćemo se na istu referirati terminima: Uredba ili GDPR..

Za provođenje Uredbe u Hrvatskoj je Sabor donio: *Zakon o provedbi Opće uredbe o zaštiti podataka*. Isti je na snazi od 25.05.2018.

Uloga Zakona je da osigura provođenje Uredbe u Hrvatskoj. Zakonom je osnovana *Agencija za zaštitu osobnih podataka* (u daljnjem tekstu: AZOP). AZOP je samostalno tijelo odgovorno Saboru.
Osnovna uloga AZOP-a je praćenje postupanja organizacije sa svojim podacima i kontrola usklađenosti tih postupaka s Uredbom.
Odgovorna osoba za provođenje Uredbe u organizaciji je Voditelj obrade. To je ravnatelj ustanove. Suodgovorni su Izvršitelji obrada u mjeri u kojoj Voditelj obrade Pravilnikom na njih prenese odgovarajuće odgovornosti.
Da bi AZOP imao uvid u postupanje organizacije, Zakon je obvezao organizaciju imenovati Službenika za zaštitu podataka. On je spona između organizacije i AZOP-a.
Isto ilustrira donja shema[1]:



Čemu odjednom taj GDPR?

Službenik za zaštitu podataka?

Na shemi s prve stanice smo vidjeli da je Službenik za zaštitu podataka spona između ustanove i AZOP-a. osnovni zadatci Službenika za zaštitu podataka su:

- praćenje poštovanja Uredbe od strane ustanove[2],
- praćenje politika voditelja obrade ili izvršitelja obrade i usklađenost tih politika s Uredbom,
- praćenje raspodjele odgovornosti za provođenje Uredbe unutar ustanove,

[1] Umjesto širokog pojma: organizacija u daljem tekstu ćemo razmatranje suziti na ustanove.
[2] U izvornom obliku navodi se: organizacija.

- djelovanje kao kontaktna točka za nadzorno tijelo[3] po pitanjima obrade podataka u ustanovi,
- suradnja s nadzornim tijelom.

Službenik za zaštitu podataka prati provedbu i usklađenost procesa ustanove vezanih za obradu podataka i isti je kontaktna točka za AZOP.
Važno je, i u Uredbi naglašeno da isti ne smije biti u sukobu interesa. Razmotrimo značenje ovog zahtjeva:

Jedno od osnovnih pravila organizacije poslovanja je da zaposlenik ili organizacijski dio ne može biti odgovoran za provođenje postupaka i procedura, a ujedno i kontrolirati ispravnost njihove provedbe. Kontrolu kvalitete rada određenog izvršitelja ili organizacijskog dijela može vršiti jedino neovisni organ.

Ukoliko zaposlenik ili organizacijski dio provodi određene zadatke, a ujedno i kontrolira ispravnost provedbe tih zadataka, nastaje situacija poznata kao sukob interesa.

Bilo koji zaposlenik ustanove koji obrađuje određenu skupinu podataka (tajnica, računovođa, pedagog, predmetni nastavnik, logoped, ...)[4] ne može sam ocjenjivati kvalitetu svog postupanja s podacima i usklađenost tih postupanja s Uredbom. To bi bilo: „Kadija te tuži, kadija ti sudi“.

Po istom principu, ni rukovoditelj ustanove (organizator poslova) ne može sam donositi ocjenu o kvaliteti svog rada.
Prvi uvjet kod odlučivanja o imenovanju Službenika za zaštitu podataka je isključivanje osoba koje bi mogle biti u sukobu interesa.

Odredivši koje osobe iz ustanove neće biti u sukobu interesa, pogledajmo što se od Službenika za zaštitu podataka očekuje i koji su mu osnovni zadaci:

- poznavanje Uredbe,
- poznavanje poslovnih procesa ustanove,
- pomoć u utvrđivanju načela obrade osobnih podataka,
- suradnja u analizi organizacijskih i tehničkih aspekata zaštite osobnih podataka,
- uspostavljanje evidenciji aktivnosti obrade,
- procjena sigurnost obrade,
- zaštiti prava osoba nezadovoljnih načinom na koji se tretiraju njihovi osobni podaci,
- izvještavanje o povredama osobnih podataka.

Imajući u vidu gornja očekivanja, izgleda da je najprihvatljivije rješenje da bi Službenik za zaštitu podataka trebala biti osoba s informatičkim znanjima koja dobro poznaje Uredbu, a da istovremeno nije u sukobu interesa.

Logično rješenje je da to bude vanjski suradnik koji, ako je moguće, dobro poznaje informacijski sustav ustanove[5].

Terminologija

U daljem upoznavanju s Uredbom, odnosno s prijevodom *General Data Protection Regulation* s engleskog na hrvatski jezik pojavljuju se određeni termini koje bi možda, radi jasnoće trebalo komentirati.

[3] AZOP
[4] Osim navedenog, to po principu zapovjedne odgovornosti ne može biti ni rukovoditelj (organizator) tih poslova.
[5] Poznavanje informacijskog sustava ustanova koje koriste trajnu Konzalting uslugu je navelo AP-Split d.o.o. da se pripremi i obrazuje u sferi GDPR-a.

Anglo-saksonska imenica**:** ***consent*** se prevodi sa: ***privola****.* Termin: *privola* nije nov, nalazimo ga i u Drvodelićevom Hrvatsko-Engleskom rječniku iz 1953., gdje se: *privola* prevodi kao: *assent; consent; approbation; sanction.*

Istovremeno je imenica*: suglasnost* prevedena s *consonance; harmony; conformity; concordance; agreement; consent; accord.*

Obzirom da je jedno od značenja prijevoda: *privola* i termin: *sanction* (prevedeno = *sankcija)*, izraz: ***suglasnost*** (koji ne implicira i sankciju) izgleda kao jednoznačni prijevod termina *consent,* u odnosu na termin: ***privola*** koji može imati i značenje sankcije.

Daljim istraživanjem pojavilo se i objašnjenje da glagol: *privoljeti* ima značenja:

1. (koga) nagovoriti, navesti koga, pobuditi želju da učini što, da pristane na što
2. (na što) pristati, složiti se, suglasiti se s čim
3. (se komu) prići na čiju stranu, opredijeliti se.

Očekujući da ***consent*** treba biti dobrovoljan, bilo bi dobro izbjeći glagol koji uključuje i: *(koga) nagovoriti; navesti koga; pobuditi želju da učini što*. Radi toga bi možda bilo ispravnije koristiti termin ***suglasnost*** umjesto zacrtanog termina: ***privola***.

Drugi neobičan termin bi bio: ***ispitanik***. Termin koji je u engleskom originalu: ***data subject;*** njemački: ***betroffene Person;*** fancuski: ***la personne concernée***; talijaski: ***il soggetto dei dati.***

U spomenutom Drvodelićevom Hrvatsko-Engleskom rječniku iz 1953 ne nalazimo riječ: *ispitanik*. Uspoređujući prijevode termina: ***data subject*** na navedena tri jezika, čini se da bi prijevod na hrvatski jezik: ***naznačena osoba*** ili ***subjekt podataka*** bio bliži izvornom značenju.

Podaci

Najvažniji segment u dosadašnjem razmatranju: a to su podaci, je preskočen. Da bi osobni podaci bili sigurni, mora biti sigurno i okruženje u kome se isti nalaze. Osobni podaci su dio podataka ustanove. Ukoliko nije osigurana sigurnost podataka, nema govora o sigurnosti osobnih podataka.

Voditelj obrade je odgovoran za sigurnost osobnih podataka, pa posljedično i za sigurnost podataka. Ne treba sumnjati da bi samo mali broj Voditelja obrade (ravnatelj ustanove) mogao odgovoriti na donja tri pitanja:

1. Gdje se nalaze podaci ustanove?
2. Koji podaci ustanove sadrže osobne podatke?
3. Tko sve može pristupiti podacima ustanove?

Detaljnija pitanja će vjerojatno izazvati dodatnu nervozu i nesigurnost:

- Gdje se, van ustanove, nalaze serveri (računala na kojima se nalaze baze podataka) na kojima su pohranjeni osobni podaci ustanove?
- Koja računala u ustanovi služe kao serveri?
- Prenose li se podaci sa servera u čitljive formate (Excel, PDF) bez prikrivanja subjekta podataka?
- Tko vodi kataloge podataka pojedinih baza, kako bi se ustanovilo gdje se nalaze osobni podaci?
- Tko sve posjeduje prava pristupa pojedinim bazama ustanove, i u koju svrhu mu je dato odobrenje?
- Postoji li automatska evidencija pristupa bazama podataka s osobnim podacima?
- Tko dodjeljuje lozinke (prava pristupa) pojedinim bazama podataka?
- Postojj li sustav master-lozinki, u slučaju da izvršitelj obrade istu zaboravi ili sabotira?
- Kako se uništavaju papirnati dokumenti, CD-ovi i je li uopće predviđen način zaštite osobnih podataka na odbačenim papirnim ili digitalnim medijima?

Od koga tražiti odgovore na gornja pitanja? Prema Uredbi, za sve što PRAVILNIKOM O ZAŠTITI PODATAKA Voditelj obrade (Ravnatelj) ne prenese na druge osobe, je on osobno odgovoran.

Izvršitelji obrada su stručni za servisiranje problemskog aspekta područja koje obrađuju, a ne posjeduju specijalizirana znanja potrebna za odgovor na gornja pitanja. Stoga ni odgovore na gornja pitanja ne možemo od njih očekivati. Te odgovore bi mogla dati jedino osoba informatičke struke, kad bi bila zadužena za isto.

Kako GDPR može pomoći?

Za razliku od gornjega, Uredba kreće na drugi način, i iz drugog razloga. Ne zanima je jesu li i informacije dio vrijednosti ustanove. Zanimaju je slobode pojedinca i ljudska prava. Stoga je u istoj regulirano postupanje s onim dijelom podataka koji utiču na slobodu pojedinca i na ljudska prava; postupanje s osobnim podacima.

Svrha Uredbe je inicirati, pomoći u uvađanju, pratiti i kontrolirati postupanje s osobnim podacima ustanove, kako bi se zaštitila privatnost pojedinca. Time bi se uveo red i u postupanja sa svim podacima ustanove.

Za ostvarenje ovih poslova Uredba je uvela donju podjelu podataka:
Osobni podaci su dio podataka ustanove. Stoga ustanova mora posebno brinuti o podacima a odvojeno od toga o osobnim podacima. To su dva odvojena zadatka:

1. Uvesti red i propisati način postupanja s podacima ustanove,
2. Zaštititi ljudska prava i slobode pojedinca određivanjem načina postupanja s osobnim podacima.

Da bi se isto postiglo ne remeteći poslovanje ustanove, Uredba osobne podatke dijeli u dvije skupine.

2.1 Osobni podaci koji se koriste u svrhu obavljanja registrirane djelatnosti ustanove,
2.2 Osobni podaci koji se koriste po nahođenju ustanove.

Osobni podaci navedeni pod 2.1. su podaci koji se koriste sukladno:

- *Zakonu koji tretira specifično poslovanje ustanove (predškolski odgoj, odgoj i obrazovanje u osnovnoj i srednjoj školi, muzeji …),*
- *Zakonu o ustanovama i*
- *Zakonu o računovodstvu.*

Uredba ne postavlja restrikcije za osobne podatke koji se koriste u skladu s gornjim zakonima, kako se ne bi poremetilo ili otežalo poslovanje ustanove. Međutim, potrebno je ishoditi posebnu suglasnost[6] od subjekta podataka[7] ukoliko se ti podaci koriste ili objavljuju mimo zakonom određenog načina.

Osobni podaci pod 2.2. su podaci koje ustanova koristi po svom nahođenju. To su uglavnom:

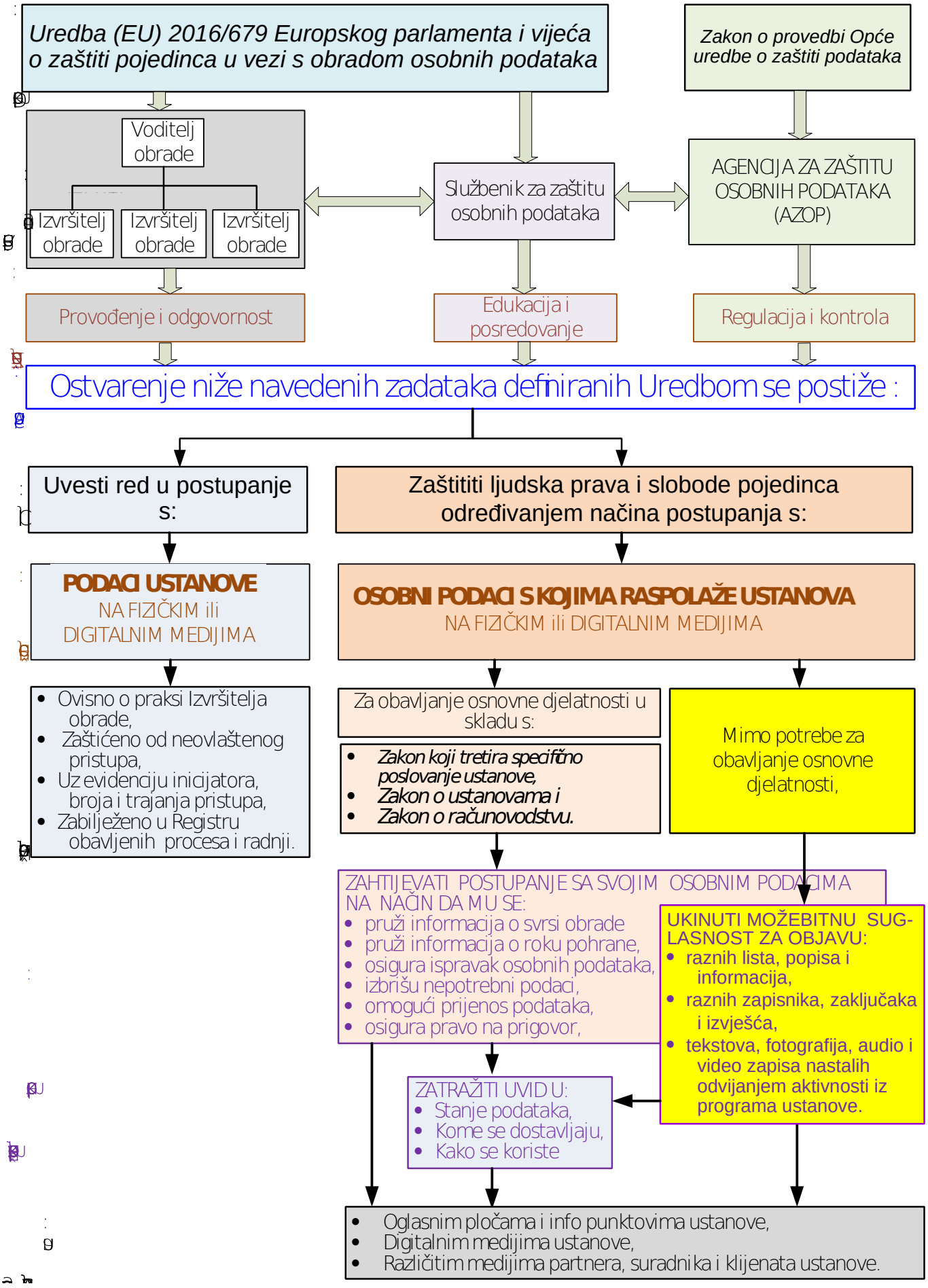
- razne liste, popisi i informacije koje sadrže osobne podatke,
- različiti zapisnici, zaključci i izvješća koja sadrže osobne podatke,
- tekstovi, fotografije, audio i video zapisi nastali tijekom odvijanja aktivnosti iz programa ustanove.

Posebna pažnja se traži za objavljivanje osobnih podataka na oglasnim pločama, info-punktovima i na digitalnim sadržajima a posebna dodatna pažnja je potrebna za objavu osobnih podataka maloljetnika.

Donja shema je pokušaj sinteze: strukture, zaduženja, provođenja, zadataka i postupanja kako bi se uveo red u poslovanje s podacima i osigurala prava subjekata podataka:

[6] U sugeriranoj terminologiji: Privola
[7] U istoj terminologiji: Ispitanik.

Struktura učesnika, zadataka, i svrhe u procesu zaštite osobnih podataka



Tko će sve ovo provesti?

Gore smo naveli svu silu obveza i zadataka. To bi netko trebao i provesti. Pogledajmo na koga se uopće može računati i što su čiji zadaci u izvršenju obveza i poslova određenih Uredbom:

a) **Voditelj obrade**
   Mora poduzeti potrebne organizacijske i tehničke mjere kako bi mogao dokazati da se obrada podataka provodi u skladu s Uredbom, mora omogućiti pristup nepromijenjenim podacima i nakon eventualnog incidenta, te osigurati redovitu provjeru sigurnosti obrade. Ako eventualni incident dovede do povrede osobnih podataka s mogućim ozbiljnim posljedicama po subjekta podataka, voditelj obrade mora bez odgode izvijestiti nositelja podataka i AZOP.

b) **Izvršitelj obrade**
   Dužan je postupati prema uputama voditelja obrade, čuvati povjerljivost osobnih podataka i postupiti u skladu s Uredbom.

c) **Administrator podataka**
   Ova funkcija se ne navodi kao dio procesa obrade osobnih podataka. Ista osigurava ispravno postupanje i sigurnost **svih** podataka u digitalnom obliku, stoga je pretpostavka za bilo kakav rad s digitalnim podacima, pa tako i s .

d) **Službenik za zaštitu osobnih podataka**
   Treba informirati i savjetovati voditelja ili izvršitelja obrade o njihovim obvezama o zaštiti podataka, pratiti provođenje propisa o zaštiti podataka, pratiti poštivanje postupanja s osobnim podacima, te surađivati s nadzornim tijelom.

e) **AZOP**

Zadužen je za praćenje provedbi mjera Uredbe. Istražuje i rješava eventualne pritužbe subjekta podataka. Može privremeno ili konačno ograničavati ili zabraniti obradu podataka, te izreći novčanu kaznu.

AZOP je regulatorno tijelo stoga stvarni rad, posao na uvađanju i provođenju Uredbe moraju provesti prva četiri navedena organa.

Nanovo treba napomenuti da Administrator podataka nije dio strukture vezane za postupanje s osobnim podacima, već sa svim podacima u digitalnom obliku.

Zadaci gornjih subjekata, korak po korak su:

1. Ovladati potrebnim informacijama Uredbe,
2. Dobiti snimak postojećeg stanja podataka i osobnih podataka,
3. Pripremiti dokumentaciju koja će usmjeravati Voditelja i Izvršitelje obrada,
4. Definirati radnje potrebne za ustrojavanje obrada
5. Ustrojiti obrade,
6. Testirati sustav.

Da bi lakše pratili radnje i zadatke, pogledajmo prije toga koje je dokumente potrebno kreirati:

1 Uvodna informacija: "GDPR -ŠTO I KAKO?"
2 UPITNIK za Voditelja obrade (i za Administratora podataka)
3 UPITNIK za Izvršitelje obrada
4 SPECIFIKACIJA PODATAKA ustanove
5 POLITIKA USTANOVE U POSTUPANJU S OSOBNIM PODACIMA
6 PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA
7 Postojeći akti (nakon usklađivanja)
8 UPUTE ZA PROVOĐENJE pojedinačnih OBRADA
9 SUGLASNOSI ZA PRIKUPLJANJE I OBRADU OSOBNIH PODATAKA
10 IZJAVA O POVJERLJIVOSTI
11 EVIDENTNI LIST INCIDENATA I PROBOJA SIGURNOSTI
12 ZAHTIJEV SUBJEKATA PODATAKA

Osim navedenih dokumenata treba ustrojiti i registre koji će ažurno pratiti stanje pojedinih dokumenata. To su:

A REGISTAR SUGLASNOSTI
REGISTAR IZJAVA O
B POVJERLJIVOSTI
REGISTAR INCIDENATA I PROBOJA
C PODATAKA
REGISTARA ZAHTIJEVA SUBJEKATA
D PODATAKA.

Prijedloge navedenih dokumenata i registara (isključujući točku 7.), bi trebao kreirati Službenik za zaštitu podataka.

Popis zadataka potrebnih za uvađanje Uredbe

Kreiranje dokumenata je samo početni dio procesa. Dokumenti moraju predstavljati osnovu svakodnevnog poslovanja s osobnim podacima, odnosno moraju se integrirati u poslovni proces ustanove. To je znatno širi zadatak.

Imajući u vidu da se u pitanjima upućenim Službeniku za zaštitu podataka traži odgovor na pitanje: *“Što to ustanova mora napraviti da bi se usuglasila s Uredbom?“* pokušalo se na to pitanje odgovoriti donjim popisom zadataka[8].

Grupe poslova i zadataka koje treba obaviti kako bi se postigla usklađenost poslovnog sustava ustanove s Uredbom su :

1. OVLADAVANJE POTREBNIM INFORMACIJAMA UREDBE,
2. SNIMAK POSTOJEĆEG STANJA,
3. PRIPREMA DOKUMENATA ZA VODITELJA I IZVRŠITELJE OBRADA,
4. DEFINIRANJE RADNJI POTREBNIH ZA USTROJAVANJE OBRADA,
5. USTROJAVANJE I PRAĆENJE OBRADA.

[8] Ponovo treba napomenuti da problem može nastati već na točci 2.1. Veliko je pitanje da li je Voditelj obrade, obzirom na stručnost, može dati odgovore na tražena pitanja. Dodatni problem je koga će opunomoćiti da u daljem radu surađuje s Službenikom za zaštitu podataka nakon što se utvrdi potreba izmjene određenih informatičko-računalnih procedura i praksi.