1. Radionica LEDAER mreže Hrvatske, 2018.

Priprema i provedba obveza LAG-ova preuzetih Ugovorom i Sporazumom o suradnji sa Agencijom za plaćanja i Priloga I, Sporazum o povjerljivosti (uključujući ZOP/GDPR i ZOI)

Luka, 08.-11.05.2018.

Pravni temelj – obveznici LAG-ovi

Zakonom o udrugama i Sporazumom o suradnji s APPRRR – LAG-ovi su obveznici provedbe:

- Zakona o zaštiti osobnih podataka (NN103/03, 118/06, 41/08, 130/11, 106/12)
- Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (NN 105/2004)
- **Uredbe (EU) 2016/679 Europskog Parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) – GDPR**
- Zakona o pravu na pristup informacijama (NN 25/13, 85/15)

Zašto?

- Uloga LAG-ova je rad za opće dobro (za to su financirani iz javnih izvora), širenje informacija, edukacija i animacija ljudi za razvoj lokalne zajednice, poduzetništva, međusobne suradnje……LAG-ovi su i udruge i upravljaju javnim financijskim sredstvima
- Kako bi ispunili svoju svrhu te dokazali svoje aktivnosti, moraju ih prikazati putem podataka/prikaza uključenih sudionika ili ciljanih skupina
- LAG-ovi prikupljaju, obrađuju, objavljuju podatke i vizualne zapise o:
  - Svojim članovima i njihovim predstavnicima putem kojih djeluju u radu LAG-a
  - Imaju zaposlene osobe, volontere i suradnike/stručnjake
  - Provode informativno-edukativno-animacijske aktivnosti
  - Međusobno surađuju
  - Provode odlučivanje o dodjeli javnih sredstava
  - Nadziru provedbu projekata putem kojih ostvaruju svoje razvojne ciljeve……

Što je GDPR (*General Data Protection Regulation*)

- Novi pravni okvir zaštite osobnih podataka na razini EU – Opća uredba o zaštititi osobnih podataka (stupila na snagu 24.05.2016.) – **obvezna za primjenu u svim zemljama članicama od 25.05.2018**
- **Direktno se primjenjuje u državama članicama bez potrebe za implementacijom u nacionalno zakonodavstvo.** *Za razliku od direktiva EU-a, uredbe se ne moraju naknadno ratificirati u parlamentu, ali je u RH u pripremi* ***Zakon o provedbi Opće uredbe o zaštiti podataka*** *kojim se dodatno reguliraju obaveze i kazne.*
- **AZOP**- **ovlaštena za primjenu Uredbe** i osiguranje sukladnosti s njenim odredbama
- **Ciljevi** GDPR:
  - usklađivanje zakona o zaštiti podataka u cijeloj EU,
  - zaštita i osnaživanje osobnih podataka svih građana EU,
  - promjena načina pristupa zaštiti podataka u organizacijama
- **Kazne**:
  - novčane kazne u iznosu do €20 milijuna ili 4% ukupnog godišnjeg prometa (ovisno što je veće)
- **Obveznici:**
  - svi gospodarski subjekti koji barataju s podacima korisnika koji žive na području EU, neovisno o lokaciji gospodarskog subjekta

Što možete nakon 25.05.2018.

- Želite vidjeti kako kartičarska kuća koristi vaše podatke o kupnji?
- Želite saznati tko točno u MUP-u pristupa podacima o vašoj registraciji automobila, boravištu i podacima s osobne iskaznice?
- Želite da od banke dobijete popis svih osoba koje su unatrag mjesec dana pristupale vašim financijskim podacima?
- Želite zatražiti osobne podatke koje o vama prikuplja bilo koja mobilna aplikacija poput vaših GPS lokacija i IMEI broja?
- Moći ćete zatražiti i informaciju o tome koje podatke o vama prikuplja svaka web stranica koja vas je zatražila da prihvatite njen cookie
- Možete tražiti Agenciju za plaćanja ili Ministarstvo poljoprivrede gdje, kome, kada i zašto je dostavilo podatke o vama
- Možete tražiti vlasnike web stranica da uklone vaše podatke ili fotografije i dr.
- **Jednako tako – bilo tko čije podatke/audio - vizualni prikaz prikuplja ili obrađuje LAG – može isto tražiti od vas**

No…koji su to osobni podaci koji zahtjevaju pažljivu obradu (GDPR)

- GDPR se **primjenjuje samo na osobne podatke**. Ostali podaci koji se ne smatraju osobnima zaštićeni su nacionalnim zakonodavstvom država članica. GDPR **se ne primjenjuje** na anonimizirane podatke.
- **Podaci se smatraju osobnima ako se iz njih s velikom vjerojatnošću može otkriti identitet pojedinca**:
  - Osnovni podaci – ime i prezime, broj osobne iskaznice, lokacijski podaci; zatim:
  - podaci s kreditnih kartica
  - zdravstveni karton (invalidnost, povijest bolesti i sl.) i biometrijski podaci (sken rožnice, otisci prsta itd.)
  - genetski podaci (DNA i sl.)
  - vjerska i filozofska uvjerenja i etnička pripadnost
  - ekonomsko stanje
  - članstvo u sindikatu
  - seksualna orijentacija i spolni život
  - IP adrese i Osobne poruke e-pošte
  - Kolačići u pregledniku
  - Pseudonimizirani podaci
  - GPS lokacija, IMEI broj mobitela i dr.
  - Audio-vizualni prikaz osobe

GDPR – ostali važni pojmovi

- **Obrada osobnih podataka** je svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne – podatke **obrađuje LAG**
- **Zbirka osobnih podataka** je svaki strukturirani skup osobnih podataka koji je dostupan prema posebnim kriterijima – zbirke podataka **vodi LAG**
- **Voditelj zbirke osobnih podataka** je fizička ili pravna osoba, državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka – u našem slučaju – **to je LAG**
- **Primatelj** je fizička ili pravna osoba, državno ili drugo tijelo kojem se osobni podaci otkrivaju, neovisno o tome je li on ujedno i treća strana ili nije – u našem slučaju **to su sva tijela kojima dostavljamo podatke o: predstavnicima članova LAG-a, zaposlenicima ili sudionicima aktivnosti LAG-a**
- **Korisnik ili ispitanik** – osoba čije podatke ili audio-vizualni prikaz LAG obrađuje

Obrada osobnih podataka

- Osobni podaci smiju se prikupljati i dalje obrađivati:
  - uz privolu ispitanika
  - u slučajevima određenim zakonom
  - u svrhu izvršavanja zakonskih obveza voditelja zbirke osobnih podataka
  - u svrhu sklapanja i izvršenja ugovora u kojem je ispitanik stranka
  - u svrhu zaštite života ili tjelesnog integriteta ispitanika ili druge osobe u slučaju kada ispitanik fizički ili pravno nije u mogućnosti dati svoj pristanak
  - ako je obrada podataka nužna radi ispunjenja zadataka koji se izvršavaju u javnom interesu ili u izvršavanju javnih ovlasti koje ima voditelj zbirke osobnih podataka
  - ako je obrada nužna u svrhu zakonitog interesa voditelja zbirke ili treće strane osim kada prevladavaju interesi zaštite temeljnih prava i sloboda ispitanika
  - ako je ispitanik sam objavio te podatke

GDPR – Prava korisnika (ispitanika)

- **Pravo na pristup:**
  - Korisnik ima pravo dobiti od voditelja obrade podataka potvrdu obrađuju li se njegovi osobni podaci, zašto se obrađuju i koliko dugo
- **Pravo na ispravljanje pogrešaka**
- **Pravo na zaborav (brisanje podataka):**
  - Korisnik ima pravo od voditelja obrade ishoditi brisanje prikupljenih osobnih podataka koje se na njega odnose kada isti više potrebni voditelju zbirke radi ispunjavanja njegove zadaće
- **Izvješćivanje o povredi osobnih podataka:**
  - U slučaju povrede osobnih podataka voditelj obrade bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi izvješćuje nadzorno tijelo (AZOP) i ispitanika
- „**Jasan i pozitivan pristanak"** na obradu osobnih podataka od strane ispitane osobe
- Pravo da se ograniči upotreba podataka (npr. neželjeno oglašavanje)
- **Pravo na prenosivost podataka:**
  - Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega te ima pravo prenijeti te podatke drugom voditelju obrade
- **Pravila o privatnosti moraju biti objašnjena jasnim i razumljivim jezikom**

GDPR – obveze LAG-a (Voditelja zbirke podataka) prema Korisnicima

- **Voditelj zbirke osobnih podataka (u našem slučaju – LAG) dužan je:**
  - dostaviti potvrdu o tome da li se osobni podaci koji se odnose na njega obrađuju ili ne
  - dati obavijest u razumljivom obliku o podacima koji se odnose na njega
  - omogućiti uvid u evidenciju zbirke osobnih podataka te uvid u osobne podatke sadržane u zbirci osobnih podataka
  - dostaviti izvatke, potvrde ili ispise osobnih podataka sadržanih u zbirci osobnih podataka koji se na njega odnose
  - dostaviti ispis podataka o tome tko je i za koje svrhe i po kojem pravnom temelju dobio na korištenje osobne podatke koji se odnose na njega

Nadzor i kazne

- **AZOP je biti ovlaštena za primjenu Uredbe i osiguranje sukladnosti s njenim odredbama u RH**
  - nadzire provođenje zaštite osobnih podataka,
  - ukazuje na uočene zloupotrebe prikupljanja osobnih podataka,
  - sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuće uređenu zaštitu osobnih podataka,
  - rješava povodom zahtjeva za utvrđivanje povrede prava zajamčenih ovim Zakonom,
  - vodi središnji registar zbirki podataka i voditelja istih
- **Voditelji zbirki podataka dužni su, unutar 72 sata, AZOP-u prijaviti neovlašteni pristup podacima**
- **KAZNE:**
  - Upozorenje u pisanom obliku u slučaju prve pogreške i bez namjernog nepoštivanja Uredbe
  - Ravnatelj agencije, zamjenik ravnatelja, zaposlenici stručne službe te voditelji zbirki odgovaraju kaznama od 20.000 do 40.000 kn
  - Voditelji zbirki (u našem slučaju – LAG) ovisno o veličini i vrsti pogreške mogu biti kažnjeni s 4% ukupnog godišnjeg prometa ili 20 milijuna eura
  - Visina ovih novčanih kazni praktički osigurava da će privatnost podataka biti jedna od ključnih tema u radu svih gospodarskih subjekata

Kako se uskladiti s GDPR-om - transparetnost i privola Ispitanika

- **Transparetnost:**
  - Ispitanike morate na vrijeme informirati o njihovim pravima i načinu na koji ih mogu ostvariti. U tu je svrhu potrebno:
    - U izjavi o privatnosti temeljito navesti sva prava koja ispitanicima pripadaju
    - izjavu o privatnosti smjestiti na vidljivo mjesto na web-stranici ili objasniti prije potpisa Ispitanika
    - izjavu napisati jednostavnim i lako razumljivim jezikom
    - prevesti izjavu na sve jezike na kojima poslujete
    - upoznati ispitanike s izjavom o kolačićima.

- **Privola je važna!**
  - Premda je privola samo jedna od nekoliko zakonskih osnova za obradu podataka, jedna je od važnijih. Ako obradu temeljite na privoli, dužni ste učiniti sljedeće:
    - ispitaniku pružiti izjavu o privoli prilikom prikupljanja podataka
    - zahtijevati privolu za korištenje podataka (potpis, označavanje potvrdnog okvira i sl.)
    - omogućiti povlačenje privole na jednostavan način
    - tražiti izričitu privolu ako prikupljate posebne kategorije osobnih podataka

Kako se uskladiti s GDPR-om - rješavanje zahtjeva ispitanika

- Nije dovoljno samo informirati ispitanike o njihovim pravima. Morate se i potruditi pomoći im u njihovu ostvarivanju. Stoga njihove zahtjeve morate rješavati na blagovremen način. Od vas mogu zahtijevati sljedeće:
  - informiranje o tome posjedujete li njihove podatke
  - pravo pristupa svojim osobnim podacima koje posjedujete
  - tražiti kopiju osobnih podataka u vašem posjedu, u interoperabilnom formatu
  - ispravak netočnih podataka u vašem posjedu (uz prilaganje točnih informacija)
  - prijenos osobnih podataka drugom voditelju obrade
  - prestanak obrade podataka u svrhu izravnog marketinga
  - uputiti prigovor na automatizirano donošenje odluka
  - **brisanje svih podataka u vašem posjedu koji ih se tiču**
- Imajte na umu da svaki zahtjev za brisanjem, ispravkom ili prestankom obrade podataka morate proslijediti trećim stranama s kojima ste podijelili te podatke, kako bi i oni mogli postupiti prema zahtjevu.

Kako se uskladiti s GDPR-om - načela obrade osobnih podataka

- GDPR navodi nekolicinu načela koja se tiču obrade osobnih podataka. Njih trebate imati na umu prilikom svake obrade podataka jer predstavljaju **najključniji dio GDPR-a**, čije se kršenje kažnjava najvećim mogućim kaznama. Ta načela su:
  - podaci se smiju obrađivati samo na valjanoj zakonskoj osnovi, na pošten i prema ispitaniku transparentan način
  - obavezno navođenje svih svrha obrade u koje se podaci prikupljaju
  - prikupljati smijete samo podatke koji su relevantni i potrebni za ispunjavanje svrhe u koju se obrađuju
  - podaci trebaju biti točni i ažurirani
  - podatke ne smijete pohranjivati duže od razdoblja potrebnog za ispunjavanje svrhe u koju su prikupljeni
  - dužni se osobne podatke zaštititi od nezakonite i nedozvoljene obrade, slučajnog gubitka ili uništenja
  - morate biti u stanju dokazati usklađenost s gore navedenim načelima

Kako se uskladiti s GDPR-om - interne politike i ugovori s „trećim” stranama, mjere zaštite podataka

- Obavezni ste temeljito provjeriti postojeće dokumente i ugovore koji se tiču upotrebe i dijeljenja osobnih podataka:
  - pregledajte i prema potrebi revidirajte ugovore s izvršiteljima obrade i trećim stranama
  - ako je potrebno, u pisanom dokumentu odredite zastupnika unutar EU-a
  - donesite ili revidirajte unutarnje politike i izjave o privatnosti (npr. tehničke, organizacijske i fizičke mjere sigurnosti)
  - dokumentirajte procedure za rješavanje zahtjeva ispitanika
  - revidirajte procedure za postupanje u slučaju povreda podataka

Mjere zaštite podataka

- Kako bi se očuvala prava i slobode ispitanika, a koje se tiču obrade osobnih podataka, GDPR propisuje korištenje odgovarajućih organizacijskih i tehničkih mjera. To znači da ste dužni:
  - implementirati mjere zaštite podataka (kao što su enkripcija i pseudonimizacija)
  - uvesti **stroge mjere** kontrole pristupa podacima
  - redovito brisati osobne podatke koji više nisu potrebni ili relevantni
  - držati se načela integrirane zaštite privatnosti (*privacy by design*)

No…..kako će se LAG uskladiti s GDPR-om

LAG je VODITELJ ZBIRKI OSOBNIH PODATAKA, ali……što mora učiniti

- **Upoznati se s promjenama** koje vas čekaju i **fokusirati se na one koje će utjecati na vaše poslovanje.**
- **Analizirati moguće rizike** koje obrada podataka predstavlja po prava i slobode pojedinaca i predvidjeti načine zaštite odnosno smanjenja rizika.
- Implementirati promjene kategorizacijom podataka tako što ćete **odrediti na koje se podatke uopće primjenjuje GDPR.**
- **Odredite podatke koji pripadaju posebnim kategorijama i analizirajte tko im sve ima pristup.**
- **Primijeniti tehničke i organizacijske mjere za njihovu zaštitu** - **podatke treba enkriptirati** kad god je moguće, a uređaje s posebnim kategorijama podataka najsigurnije je ne spajati na Internet – pazite na računalnu sigurnost.
- **Dokumentirajte sve procedure**
  - Morate **uspostaviti cjelovitu zbirku osobnih podataka i voditi evidenciju o načinu korištenja podataka** kako biste u svakom trenutku mogli odgovoriti na upite i zahtjeve nadzornih tijela i ispitanika.
    - To će vam olakšati brisanje, prijenos i pristup podacima jer ćete u svakom trenutku znati gdje su točno smješteni.
    - povremeno pregledajte postojeće izjave i politike te ih prema potrebi dopunite.

No…..kako će se LAG uskladiti s GDPR-om

Mora uspostaviti internu politiku provedbe sukaldnosti i procedure za njezinu implementaciju:

1. Analizirati koje podatke prikuplja i obrađuje te u koje svrhe, i prema tome – definirati zbirke podataka
2. Donijeti opći akt kojim se usklađuje s pravnom regulativom i pokreće okvir za provedbu (Pravilnik)
3. Imenovati osobu/službenika za zaštitu osobnih podataka
4. Definirati sve druge osobe koje uz službenika, smiju imati uvid u osobne podatke koje prikuplja i obrađuje LAG (ovlaštene osobe LAG-a; drugi zaposlenici LAG-a) – svi moraju potpisati Izjave o povjerljivosti i privatnosti)
5. Ispuniti Obrazac evidencije o zbirkama osobnih podataka koje vodi LAG, te
6. Prijaviti LAG kao voditelja zbirki osobnih podataka u Središnji registar AZOP-a - registar.azop.hr
7. Prijaviti službenika za zaštitu osobnih podataka u Registar službenika za zaštitu osobnih podataka
8. Nakon prijave – AZOP dostavlja LAG-u certifikat za pristup aplikaciji evidencije zbirki osobnih podataka za LAG

Za direktan unos podataka u Središnji registar voditelji zbirki osobnih podataka moraju se registrirati u Agenciji za zaštitu osobnih podataka. Za registraciju je potrebno na adresi http://registar.azop.hr popuniti tražene podatke, ispisati ih u dva primjerka, te jedan primjerak ovjeren pečatom i potpisom odgovorne osobe dostaviti u izvorniku Agenciji. Odmah po primitku ovjerenih podataka u Agenciji, voditelju zbirke bit će omogućen unos podataka o zbirkama osobnih podataka koje vodi. Ako je voditelj zbirke naveo e-mail adresu, obavijest o aktivaciji pristupa bit će

Važni i informativni linkovi:

- http://azop.hr/
- https://gdpr-info.eu/
- https://ec.europa.eu/info/law/law-topic/data-protection_en
- https://www.eugdpr.org/
- https://gdprinformer.com/hr
- I dr.